Bitdefender

GravityZone

РУКОВОДСТВО АДМИНИСТРАТОРА

Bitdefender GravityZone
Руководство администратора

Дата публикации 2021.09.29

Правовое положение

Bitdefender

Содержание

Предисловие

1. Обозначения, используемые в данном руководстве

Типографские обозначения

Это руководство использует несколько текстовых стилей для улучшения читаемости. Узнайте об их аспекте и значении из таблицы ниже.

Виды шрифтов и стилей	Описание
`образец`	Встроенные имена команд и синтаксис, пути и имена файлов, файлы конфигурации, вводимый текст печатается стандартными моноширинными шрифтами.
http://www.bitdefender.com	Ссылки URL на внешние источники (http или ftp серверы).
gravityzone-docs@bitdefender.com	Адреса электронной почты в тексте приводятся в качестве контактной информации.
«Предисловие» (p. viii)	В кавычках приводятся внутренние ссылки на другие материалы в пределах этого документа.
опция	Все параметры продукта выделены **жирным** шрифтом.
ключевое слово	Опции интерфейса, ключевые слова или сочетания клавиш выделены с помощью **bold** шрифта.

Примечания

Примечания — это текстовая информация, выделенная в основном тексте различными средствами, целью которой является привлечение вашего внимания к дополнительной информации, имеющей отношение к содержанию текущего раздела руководства.

Примечание

Примечание – это краткое замечание. Вы можете пропустить его, но в нем может содержаться ценная информация, например определенная особенность или ссылка на источник, имеющий отношение к данному материалу.

Важно

Эта информация требует вашего внимания, и ее не рекомендуется пропускать. Обычно, здесь приводится важная информация о факторах, которые не имеют угрожающего характера для безопасности вашей системы.

Предупреждение

Это критическая информация, к которой следует отнестись с максимальным вниманием. Ничего плохого не случится, если вы будете следовать указаниям. Внимательно прочтите и попытайтесь понять суть предупреждения, поскольку в нем описываются весьма опасные угрозы для безопасности вашей системы.

1. О GRAVITYZONE

GravityZone является решением по безопасности для бизнеса, построенного с нуля для виртуализации и облачных сред, чтобы предоставлять услуги по безопасности для физических конечных точек, виртуальных машин в частном, публичном облаке и почтовых серверов Exchange.

GravityZone это продукт с единой консолью управления доступной в облаке, предоставляемый Bitdefender, или организованный в качестве виртуального устройства установленного локально в компании, что обеспечивает единую точку для развертывания, соблюдения и управления политиками безопасности для любого количества конечных точек, любого типа, в любом месте.

GravityZone обеспечивает несколько уровней безопасности для конечных точек и почтовых серверов Microsoft Exchange: защита от вредоносного ПО с мониторингом поведения, защита от угроз нулевого дня, составление черных списков приложений и изоляция потенциально опасных объектов в ограниченной среде, межсетевой экран, управление устройствами, управление контентом, антифишинг и антиспам.

2. УРОВНИ ЗАЩИТЫ GRAVITYZONE

GravityZone обеспечивает следующие уровни защиты:

- Защита от вредоносного ПО
- Расширенный контроль угроз (Advanced Threat Control)
- Обнаружение гипервизора
- Advanced Anti-Exploit
- Брандмауэр
- Контроль контента
- Управление исправлениями
- Контроль устройств
- Полное шифрование диска
- Security for Exchange
- Sandbox Analyzer
- Обнаружение и отклик конечной точки (EDR)
- Управление Рисками Конечной Точки (ERA)
- Email Security

2.1. Защита от вредоносного ПО

Уровень защиты от вредоносного ПО основан на сканировании сигнатур и эвристическом анализе (B-HAVE, ATC) против: вирусов, червей, троянов, программ-шпионов, рекламного ПО, кейлоггеров, руткитов и других типов вредоносных программ.

Технология сканирования Bitdefender на наличие вредоносного ПО основана на следующих технологиях:

- Во-первых, используется традиционный метод сканирования, когда отсканированное содержимое сравнивается с базой данных сигнатур. В базе данных сигнатур содержатся записи байт-кодов, характерные для известных угроз, которые регулярно обновляются Bitdefender. Этот метод сканирования является эффективным против известных угроз, которые были исследованы и задокументированы. Тем не менее, независимо от того, насколько оперативно база данных обновляет записи, всегда есть окно уязвимости между временем, когда новая угроза обнаружена и когда исправление выпущено.
- Против новых, незарегистрированных угроз, защиту осуществляет второй слой Bitdefender, используя эвристический двигатель **B-HAVE**.

Эвристические алгоритмы обнаруживают вредоносные программы на основе поведенческих характеристик. B-HAVE запускает подозрительные вредоносные программы в виртуальной среде, чтобы проверить их воздействие на систему и удостовериться, что они не представляют никакой угрозы. Если угроза обнаружена, предотвращается запуск программы.

Сканирующие движки

Bitdefender GravityZone может автоматически выбирать антивирусные движки при создании пакетов агентов безопасности в соответствии с конфигурацией конечной точки.

Также администратор может подстроить сканирующий движок, выбирая между несколькими технологиями сканирования:

1. **Локальное сканирование**, когда сканирование выполняется на конечном устройстве. Режим локального сканирования подходит для мощных машин, где все механизмы защиты хранятся локально.
2. **Гибридное сканирование со световыми двигателями (общее облако)**, для средних групп, использует сканирование в облаке и, частично, локальные механизмы защиты. Данный режим сканирования предоставляет лучшее задействование ресурсов, по сравнению с использованием удаленного сканирования.
3. **Централизованное сканирование в общем или частном облаке** с небольшим объемом памяти, требующим Security Server для сканирования. В этом случае механизмы защиты не хранятся локально и сканирование выгружается на Security Server.

   Примечание
   Существует минимальный набор движков, хранящийся локально, необходимый для распаковки сжатых файлы.

4. **Централизованное сканирование (сканирование в частном или публичном облаке с помощью Security Server) с локальным резервом* (Local Scan - при наличии полных движков).**
5. **Централизованное сканирование (сканирование в частном или публичном облаке с помощью Security Server) с резервом* гибридного сканирования (Local Scan - публичное облако с облегченным движками).**

* Когда используются двойные движки сканирования - если первый движок не доступен, резервный движок может быть задействован. Потребление ресурсов и утилизация сети будет зависеть от используемых движков.

2.2. Расширенный контроль угроз (Advanced Threat Control)

Для угроз, которые ускользают даже от эвристического движка, присутствует еще один слой защиты в виде Advanced Threat Control (ATC).

ATC постоянно отслеживает запущенные процессы и оценивает подозрительное поведение, такое как: попытки замаскировать тип процесса, выполнение кода в пространстве памяти процесса (захват памяти для привилегированной эскалации), репликация, перемещение файлов, скрытность в списке технологических процессов и т.д. Каждое подозрительное поведение повышает рейтинг процесса. Когда достигается порог, включается сигнал тревоги.

2.3. Обнаружение гипервизора

Bitdefender HyperDetect - дополнительный уровень безопасности, разработанный специально для обнаружения продвинутых атак и подозрительной активности ещё до выполнения процессов. HyperDetect содержит модели машинного обучения и технологии обнаружения скрытых атак против угроз, таких как: атаки нулевого дня, продвинутые устойчивые угрозы (APT), скрытое вредоносное ПО, безфайловые атаки (злоупотребление PowerShell, инструментарием управления Windows и т. д.), кража учетных данных, целевые кибератаки, специализированное вредоносное ПО, атаки на основе сценариев, эксплойты, инструменты взлома, подозрительный сетевой трафик, потенциально нежелательные приложения (PUA), вымогатели.

2.4. Advanced Anti-Exploit

Основанная на машинном обучении, технология Advanced Anti-Exploit блокирует атаки нулевого дня, использующие трудно-обнаруживаемые эксплойты. Advanced anti-exploit в режиме реального времени отслеживает последние эксплойты и устраняет уязвимости повреждения памяти, которые могут использоваться для обхода существующих решений безопасности. Технология защищает большинство стандартных приложений, таких как браузеры, редакторы Microsoft Office и Adobe Reader и другие. Модуль следит

за системными процессами и защищает от брешей в безопасности и перехватов существующих процессов.

2.5. Брандмауэр

Брандмауэр контролирует доступ приложений к сети и к Интернету. Доступ разрешается автоматически, основываясь на базе данных известных, легитимных приложений. Кроме того, брандмауэр может защитить систему от сканирования портов, ограничивать использование общего доступа к Интернет (ICS) и предупредить, когда новые узлы подключаются по Wi-Fi.

2.6. Контроль контента

Модуль Контентного Контроля помогает обеспечить соблюдение политики компании в отношении разрешенного трафика, веб-доступа, защиты данных и контроля приложений. Администраторы могут задавать параметры сканирования трафика и исключения, составлять график доступа к веб, блокировать или разрешать определенные веб-адреса или категории, настраивать правила защиты данных и устанавливать разрешения для использования конкретных приложений.

2.7. Network Attack Defense

Модуль Network Attack Defense опирается на технологии Bitdefender, нацеленные на распознание сетевых атак, целью которых является получение доступа к конечным точкам при помощи таких средств как: атаки методом перебора, сетевые "эксплоиты", программы для кражи паролей, векторы заражения посредством скрытой загрузки, боты и трояны.

2.8. Управление исправлениями

Полностью интегрированный в GravityZone, модуль управления исправлениями поддерживает последнюю версию операционной системы и приложений, а также обеспечивает полное представление о состоянии исправления в управляемых точках Windows.

Модуль управление исправлениями GravityZone включает несколько особенностей, таких как сканирование патчей по требованию / запланированное, автоматическое / ручное сканирование исправлений или создание отчетов об отсутствующих патчах.

Вы можете узнать больше о продавцах и продуктах управления исправлениями GravityZone из этой статьи базы знаний.

Примечание
Модуль управления исправлениями - это дополнение, доступное при наличии отдельного лицензионного ключа для всех доступных пакетов GravityZone.

2.9. Контроль устройств

Модуль Контроля устройств позволяет предотвратить утечки конфиденциальных данных и проникновение вредоносного ПО через внешние устройства, подключаемые к конечным точкам, применяя блокирующие правила и исключения с помощью политик для широкого спектра устройств (таких, как USB флэш-накопители, устройства Bluetooth, CD/DVD-плееры, устройства хранения, и т.д.).

2.10. Полное шифрование диска

Данный уровень защиты позволяет Вам осуществлять шифрование всего диска на машине, управляя BitLocker для Windows, и FileVault и diskutil для macOS. Вы можете зашифровать и дешифровать загрузочные и обычные тома одним щелчком мыши, т.к. GravityZone обрабатывает весь процесс с минимальным вмешательством со стороны пользователей. Кроме того, GravityZone хранит ключи восстановления, необходимые для разблокировки томов, на тот случай, если пользователь забыл свой пароль.

Примечание
Полное шифрование диска - это дополнение, доступное при наличии отдельного лицензионного ключа для всех доступных пакетов GravityZone.

2.11. Security for Exchange

Bitdefender обеспечивает защиту Security for Exchange от вредоносных программ, антиспам, антифишинг, фильтрацию контента и содержимого писем, полностью интегрирована с серверами Microsoft Exchange, для обеспечения безопасной среды обмена сообщениями и повышения производительности. Используя признанные технологии защиты от вредоносных программ и спама, программа защищает пользователей Exchange от новейших, самых сложных вредоносных программ и от попыток украсть конфиденциальные и ценные данные пользователей.

Важно
Security for Exchange разработан для защиты всей Exchange-организации, к которой принадлежит защищаемый Exchange-сервер. Это означает, что происходит защита всех активных почтовых ящиков, включая user/room/equipment/shared mailboxes.
В дополнение к защите Microsoft Exchange, эта лицензия также покрывает установленные на сервере модули защиты конечных точек.

2.12. Sandbox Analyzer

Bitdefender Sandbox Analyzer обеспечивает мощный уровень защиты от продвинутых угроз путем автоматического и глубокого анализа подозрительных файлов, не подписанных антивирусным движком Bitdefender. Песочница использует обширный набор технологий Bitdefender для размещения потенциально полезных данных в виртуальной среде, предоставленной Bitdefender, анализирует их поведение и сообщает о мельчайших системных изменениях, которые могут свидетельствовать о вирусной и злонамеренной природе файлов.

Sandbox Analyzer автоматически принимает подозрительные файлы, находящиеся на управляемых конечных точках и скрываемые службами защиты от вредоносных программ. Процесс отправки файлов в безопасную среду запускает выделенная эвристическая модель, встроенная в модуль защиты от вредоносных программ из Bitdefender Endpoint Security Tools.

Служба Sandbox Analyzer позволяет предотвратить запуск неизвестных угроз на конечной точке. Он работает в режиме мониторинга или блокировки, разрешая или запрещая доступ к подозрительному файлу до получения окончательного решения. Sandbox Analyzer ведет себя с обнаруженными угрозами автоматически в соответствии с действиями по исправлению, определенными в политике безопасности для зараженных систем.

Кроме того, Sandbox Analyzer разрешает вам вручную принимать подозрительные файлы напрямую из Control Center, позволяя вам самостоятельно решить, что с ними делать.

2.13. Обнаружение и отклик конечной точки (EDR)

Обнаружение в конечной точке и отклик - это компонент корреляции событий, способный выявлять сложные угрозы или активные атаки. В рамках корпоративной интегрированной платформы EDR объединяет возможности всех устройств, работающих в корпоративной сети. Это решение приходит

на помощь в случаях, когда группы немедленного реагирования распознают и отвечают на серьезные угрозы.

Посредством Bitdefender Endpoint Security Tools вы можете активировать защитный модуль EDR Sensor в управлении конечной точки, чтобы объединять данные компьютера и операционной системы. Сбор и обработка метаданных с обеих сторон идет на платформе клиент-сервер.

Этот компонент несет детальную информацию по обнаруженным происшествиям, интерактивной карте происшествий, действиям по исправлению и интеграции с Sandbox Analyzer и HyperDetect.

2.14. Управление Рисками Конечной Точки (ERA)

Управление Рисками Конечной Точки (ERA) определяет, оценивает и исправляет слабые стороны конечных точек Windows с помощью сканирования рисков (по запросу или по расписанию согласно политике), учитывая большое число индикаторов риска. После первого сканирования вашей сети с определенными индикаторами риска, вы получите обзор состояния риска вашей сети в панели **Управление рисками**, доступной из главного меню. Некоторые риски Вы можете разрешить автоматически из Control CenterGravityZone, а также просмотреть рекомендации по снижению ущерба конечной точки.

2.15. Email Security

С помощью Email Security вы можете контролировать доставку электронной почты, фильтровать сообщения и применять политики в масштабах всей компании, чтобы предотвращать нацеленные и сложные угрозы электронной почты, включая Нарушение безопасности деловой почты (BEC) и CEO мошенничество. Email Security требует предоставления учетной записи для доступа к консоли. Для получения дополнительной информации см. Руководство пользователя Bitdefender Email Security.

2.16. Security for Storage

GravityZone Security for Storage предоставляет защиту в реальном времени для ведущих систем обмена файлами и сетей хранения. Система и алгоритмы обнаружения угроз обновляются автоматически - без каких-либо усилий с вашей стороны или создания помех для конечных пользователей.

Два или более GravityZone Security Servers Multi-Platform выполняет роль сервера ICAP выполнять роль сервера ICAP, предоставляющего службы защиты от вредоносных программ для устройств сетевого хранилища (NAS) и систем совместного использования файлов, соответствующих протоколу Internet Content Adaptation Protocol (ICAP, как определено в RFC 3507).

Когда пользователь делает запрос на открытие, чтение, запись или закрытие файла с ноутбука, рабочей станции, мобильного или другого устройства, клиент ICAP (NAS или система обмена файлами) отправляет запрос на сканирование к Security Server и получает результат относительно данного файла. В зависимости от результата клиент ICAP разрешает/запрещает доступ или удаляет файл.

Примечание
Этот модуль - это дополнение, доступное при наличии отдельного лицензионного ключа

2.17. Доступность уровней защиты GravityZone

Уровни защиты GravityZone отличаются в зависимости от операционной системы на конечной точке. Чтобы узнать больше, обратитесь к статье Доступность слоев защиты GravityZone в Базе Знаний.

3. АРХИТЕКТУРА GRAVITYZONE

Решение GravityZone включает в себя следующие компоненты:

- Веб-Консоль (Control Center)
- Security Server
- Агенты безопасности

3.1. Веб-консоль (GravityZone Control Center)

Решения безопасности Bitdefender управляются в рамках GravityZone из единой точки управления, веб-консоли Control Center, которая обеспечивает более легкий доступ и управление настройками общей безопасности, глобальных угроз безопасности, а также контроль над всеми модулями безопасности, защищающими виртуальные или физические настольные компьютеры, серверы и экземпляры облака Amazon. Работая на архитектуре Gravity, Control Center способна удовлетворить потребности даже самых крупных организаций.

Веб-интерфейс Control Center интегрируется с существующими системами управления и мониторинга, чтобы упростить применение защиты для неуправляемых рабочих станций и серверов.

3.2. Security Server

Security Server является специализированной виртуальной машиной, которая дедуплицирует и централизует большую часть функциональностей защиты от вредоносных программ, агентов защиты от вредоносных программ, действуя в качестве сервера сканирования.

Security Server должен быть установлен на одном или нескольких хостах, чтобы соответствовать количеству защищаемых виртуальных машин.

3.3. Агенты безопасности

Чтобы Bitdefender защитил вашу сеть, необходимо установить соответствующих агентов безопасности GravityZone на сетевых конечных точках.

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac

3.3.1. Bitdefender Endpoint Security Tools

GravityZone обеспечивает защиту физических и виртуальных Windows и Linux машин с помощью Bitdefender Endpoint Security Tools - интеллектуального агента, который адаптируется к типу конечной точки. Bitdefender Endpoint Security Tools может быть развернут на любой машине, как физической так и виртуальной, обеспечивая гибкую систему сканирования и являясь идеальным выбором для смешанных сред (физических, виртуальных и облачных).

В дополнение к защите файлов системы,Bitdefender Endpoint Security Tools также включает защиту почтовых серверов Microsoft Exchange.

Bitdefender Endpoint Security Tools использует единый шаблон политики для физических и виртуальных устройств, а также один установочный комплект для любой среды (физической или виртуальной), работающей на Windows.

Слои защиты

Следующие уровни защиты доступны в Bitdefender Endpoint Security Tools:

- Защита от вредоносного ПО
- Расширенный контроль угроз (Advanced Threat Control)
- Обнаружение гипервизора
- Брандмауэр
- Контроль контента
- Network Attack Defense
- Управление исправлениями
- Контроль устройств
- Полное шифрование диска
- Sandbox Analyzer
- Обнаружение и отклик конечной точки (EDR)
- Управление Рисками Конечной Точки (ERA)

Роли конечных точек

- Привилегированный пользователь
- Ретранслятор
- Сервер кэширования патчей
- Защита Exchange

Привилегированный пользователь

Администраторы Центра управления (Control Center) могут предоставлять права привилегированных пользователей обычным пользователям конечных устройств с помощью параметров политики безопасности. Модуль привилегированных пользователей разрешает предоставление администраторских прав уровню пользователей, которые разрешат конечным пользователям получать доступ и изменять настройки безопасности, используя локальную консоль. Control Center будет уведомлена, когда конечная точка находится в режиме привилегированного пользователя и администратор Control Center всегда может переназначить локальные настройки безопасности.

Важно
Этот модуль доступен только для поддерживаемых настольных и серверных операционных систем Windows. Для получения более подробной информации, обратитесь к руководству по установке GravityZone.

Ретранслятор

Агенты конечных точек с ролью Bitdefender Endpoint Security Tools Relay выступают как прокси-сервер и сервер обновлений для других конечных точек в сети. Агенты конечных устройств с ролью ретранслятора особенно необходимы в организациях с изолированными сетями, где весь трафик проходит через единую точку доступа.

В компаниях с большими распределенными сетями, агент-ретранслятор помогает снизить использование полосы пропускания, предотвращая защищаемые конечные устройства и серверы безопасности от прямого взаимодействия с машинами GravityZone.

После того, как агент Bitdefender Endpoint Security Tools Relay установлен в сети, другие конечные точки могут быть сконфигурированы с помощью политик, чтобы общаться с Control Center через агента ретрансляции.

Агенты Bitdefender Endpoint Security Tools Relay служат для следующих целей:

- Обнаружение всех незащищенных конечных точек в сети.

  Эта функциональность имеет важное значение для развертывания агента безопасности в облачной среде GravityZone.
- Развертывание агентов конечных точек внутри локальной сети.
- Обновление защищаемых конечных точек в сети.

- Обеспечение связи между Control Center и подключенными конечными точками.
- Выступать в качестве прокси-сервера для защищаемых конечных точек.
- Оптимизации сетевого трафика во время обновления, развертывания, сканирования и других ресурсоемких задач.

Сервер кэширования патчей

Конечные точки с ролью ретранслятора также могут выступать в качестве сервера кэширования исправлений. При включении этой роли ретрансляторы служат для хранения исправлений программного обеспечения, загружаемых с веб-сайтов поставщиков, и их распространения на конечные точки сети. Всякий раз, когда подключенная конечная точка имеет программное обеспечение с отсутствующими исправлениями, она берет их с сервера, а не с веб-сайта поставщика, таким образом оптимизируя генерируемый трафик и нагрузку на пропускную способность сети.

Важно
Эта дополнительная роль доступна с зарегистрированной надстройкой Patch Management.

Защита Exchange

Bitdefender Endpoint Security Tools с ролью защитника Exchange может быть установлен на сервере Microsoft Exchange с целью защиты пользователей Exchange от угроз передаваемых по электронной почте.

Bitdefender Endpoint Security Tools с ролью защитника Exchange защищает как сам сервер, так и сервисы Microsoft Exchange.

3.3.2. Endpoint Security for Mac

Endpoint Security for Mac - это агент безопасности, предназначенный для защиты рабочих станций Macintosh и ноутбуков с процессорами Intel или Apple M1. В качестве технологии сканирования доступно **Локальное сканирование**, с локально расположенными механизмами защиты.

Слои защиты

Следующие уровни защиты доступны в Endpoint Security for Mac:

- Защита от вредоносного ПО

- Расширенный контроль угроз (Advanced Threat Control)
- Контроль контента
- Контроль устройств
- Полное шифрование диска
- Обнаружение и отклик конечной точки (EDR)

3.4. Sandbox Analyzer Архитектура

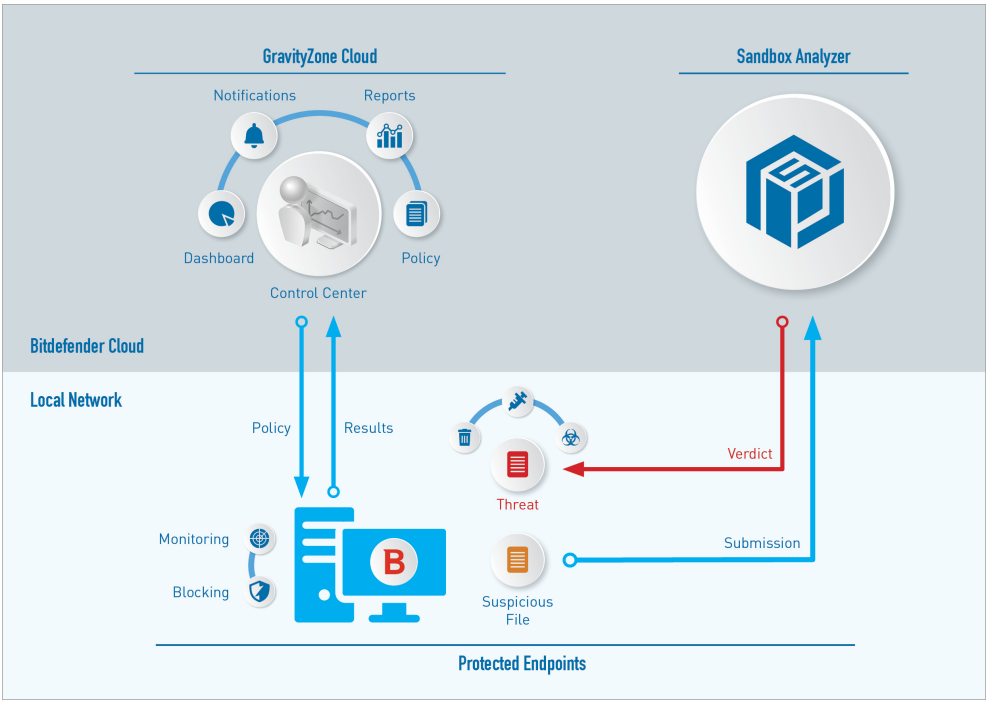
Bitdefender Sandbox Analyzer обеспечивает мощный уровень защиты от новейших угроз путем автоматического и глубокого анализа подозрительных файлов, не подписанных антивирусными ядрами Bitdefender.

Sandbox Analyzer содержит следующие компоненты:

- **Sandbox Analyzer Portal**. Этот компонент - это размещенный сервер связи, используемый для передачи запросов между конечными точками и кластером безопасной среды Bitdefender.
- **Sandbox Analyzer Cluster**. Этот компонент - это размещенная инфраструктура песочницы, в которой происходит анализ поведения объектов. На этом уровне отправленные файлы проверяются на виртуальных машинах под управлением Windows 7.

GravityZone Control Center – функционирует как консоль управления и отчетов, где вы настраиваете политики безопасности, просматриваете отчеты анализа и уведомления.

Bitdefender Endpoint Security Tools (BEST) - агент безопасности, установленный на конечных точках, действует как датчик подачи данных в Sandbox Analyzer.



Архитектура Sandbox Analyzer

Как только сервис Sandbox Analyzer активирован с Control Center на конечных точках:

1. Агент безопасности Bitdefender начинает отправлять в безопасную среду подозрительные файлы в соответствии с установленными правилами защиты.
2. После анализа файла ответ отправляется обратно на Портал и далее в конечную точку.
3. Если файл выявлен как опасный, пользователь получает уведомление об этом и принимает меры по исправлению.

Результаты анализа сохраняются хэш-значением файла в базе данных Sandbox Analyzer. Когда ранее проанализированный файлн найден на другой

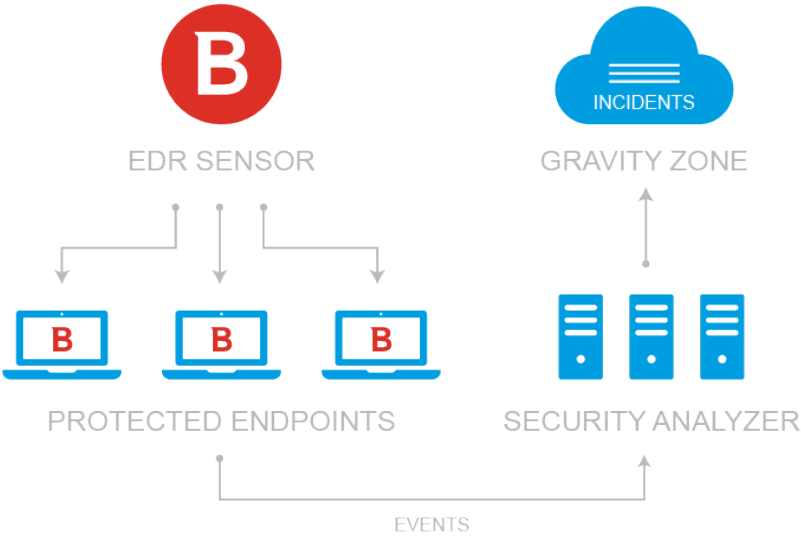
конечной точке, ответ немедленно отправляется обратно, поскольку результаты уже доступны в базе данных.

3.5. Архитектура EDR

Для выявления угроз повышенной сложности и атак в процессе EDR требуются данные об оборудовании и операционной системе. Некоторые новые данные обрабатываются локально: машина выполняет более сложные задачи, одновременно изучая алгоритмы в разделе Аналитика безопасности.

EDR содержит два основных компонента:

- Датчик инцидентов, который собирает данные процесса и сообщает данные о конечной точке и поведении приложения.
- Аналитика безопасности, серверый компонент набора технологий Bitdefender, используемый для интерпретации метаданных, собранных датчиком инцидентов.



EDR передается от конечной точки в Центр Контроля

4. НАЧАЛО РАБОТЫ

4.1. Подключение к Control Center

Доступ к Control Center осуществляется с помощью учетных записей пользователей. Вы получите регистрационную информацию по электронной почте, как только ваш аккаунт будет создан.

Требования к системе:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Рекомендуемое разрешение экрана 1280 x 800 или выше

Предупреждение
Control Center не будет работать должным образом / отображаться в Internet Explorer 9 и выше с включенным режимом совместимости, что эквивалентно использованию неподдерживаемой версии браузера.

Подключение к Control Center:

1. Откройте ваш веб-браузер.
2. Перейдите по следующему адресу: https://gravityzone.bitdefender.com
3. Если вы используете **учетные данные GravityZone**:
   a. Введите адрес электронной почты своей учетной записи и нажмите **Далее**.
   b. Введите пароль своей учетной записи и нажмите **Далее**.
   c. Введите 6-значный код в приложении Authentication как часть двухфакторной идентификации.
   d. Нажмите **Продолжить**, чтобы войти.

   Если вы используете **единый вход**:
   a. При первом входе в систему введите адрес электронной почты своей учетной записи и нажмите **Далее**.

      GravityZone перенаправит вас на страницу аутентификации вашего провайдера идентификации.
   b. Авторизуйтесь у провайдера идентификации.

c. Провайдер идентификации перенаправит вас обратно в GravityZone, и вы автоматически войдете в Control Center.

   В следующий раз вы войдете в Control Center, указав только свой адрес электронной почты.

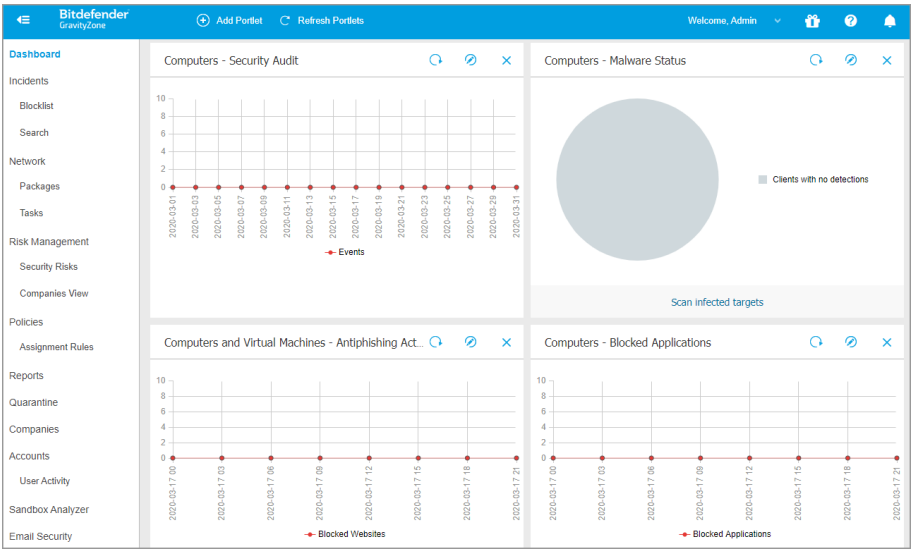
При первом входе в систему вы должны согласиться с Условиями обслуживания Bitdefender. Нажмите **Продолжить**, чтобы начать использовать GravityZone.

Примечание

- Если Вы забыли свой пароль, воспользуйтесь ссылкой восстановления пароля, чтобы получить новый пароль. Вы должны предоставить адрес электронной почты вашей учетной записи.
- Если ваша учетная запись использует единый вход, но GravityZone запрашивает пароль, обратитесь за помощью к администратору. Тем временем войдите под своим предыдущим паролем или воспользуйтесь ссылкой для восстановления пароля, чтобы получить новый пароль.

4.2. Интуитивно понятная Control Center

Control Center организована таким образом, чтобы обеспечить легкий доступ ко всем функциям. Используйте панель меню справа, чтобы перемещаться по консоли. Доступные функции зависят от уровня доступа пользователя к консоли.



Информационная панель

4.2.1. Обзор Control Center

Используйте кнопки **Просмотр меню** в левом верхнем углу чтобы свернуть, скрыть или развернуть меню. Нажмите на клавишу чтобы поочередно изменять вид меню, или нажмите два раза, чтобы пропустить.

В зависимости от Вашей роли, вы можете получить доступ к следующим разделам меню:

Панель управления
Просмотр простых графиков, позволяющих прочитать ключевую информацию о безопасности вашей сети.

События
Просмотр и управление инцидентами безопасности в сети компании.

Сеть
Установка защиты, применение политик для управления настройками безопасности, выполнение удаленных задач и быстрое создание отчетов.

Политики
Создание и управление политиками безопасности.

Отчеты
Получение отчетов о безопасности по управляемым клиентам.

Карантин
Удаленное управление файлами в карантине.

Учетные записи
Управление доступом к Control Center для других сотрудников компании.

В этом меню вы также можете найти страницу **Активность пользователя** , которая позволяет получить доступ к журналам активности пользователей.

Примечание
Это меню доступно только пользователям с **Управление пользователями** .

Конфигурация
Настройте параметры Инвентаризации сети Control Center, включая запланированные правила для автоматического удаления неиспользуемых виртуальных машин.

Примечание
Это меню доступно только пользователям с правом **Управление сетями**.

В левом нижнем углу Control Center, раздел инструментов **Tools** позволяет вам использовать больше ресурсов GravityZone, таких как ручная подача файлов в Sandbox Analyzer.

При нажатии на имя пользователя в правом верхнем углу консоли, доступны следующие опции:

- **Моя учетная запись**. Выберите этот параметр, чтобы управлять своими реквизитами пользователя и настройками.
- **My Company** (Моя компания). Нажмите эту опцию для управления учетной записью вашей компании и настройками.
- **Диспетчер учетных данных**. Выберите этот параметр для добавления и управления учетными данными, необходимыми для задач удаленной установки.
- **Помощь & Поддержка**. Выберите данную опцию, чтобы получить информацию о помощи и поддержке.

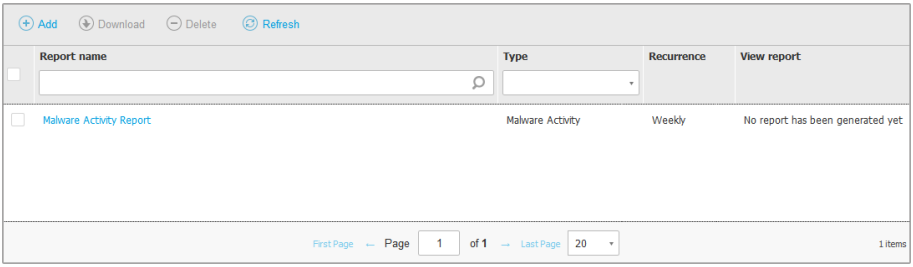
- **Обратная связь**. Нажмите эту опцию, чтобы отобразить форму, позволяющую редактировать и отправлять сообщения обратной связи относительно вашей работы с GravityZone.
- **Выход**. Выход из учетной записи.

Кроме того, в верхнем правом углу консоли вы можете найти:

- Значок **Режим справки** , который активизирует расширяемые всплывающие подсказки, помещенные на элементы Control Center. Здесь вы легко сможете найти полезную информацию, касающуюся функций Control Center.
- Значок **Уведомления** обеспечивает легкий доступ к сообщениям уведомлений, а также к странице **Уведомления**.

4.2.2. Таблица данных

Таблицы часто используются на консоли для организации данных в легко понятном формате.



Страница отчетов

Навигация по Страницам

Таблицы с более чем 20 записями размещаются на нескольких страницах. По умолчанию, только 20 записей отображаются на одной странице. Для перемещения по страницам используйте кнопки навигации в нижней части таблицы. Вы можете изменить количество записей, отображаемые на странице, выбрав другую опцию в меню рядом с кнопками навигации.

Поиск конкретных записей

Чтобы легко найти конкретные записи, используйте окна поиска доступные под заголовками столбцов.

Введите слово для поиска в соответствующем поле. Соответствующие элементы отобразятся в таблице, по мере ввода запроса. Чтобы сбросить содержимое таблицы, очистите поля поиска.

Сортировка данных

Для сортировки данных по определенному столбцу, щелкните заголовок столбца. Нажмите на заголовок столбца еще раз, чтобы вернуть порядок сортировки.

Обновление данных таблицы

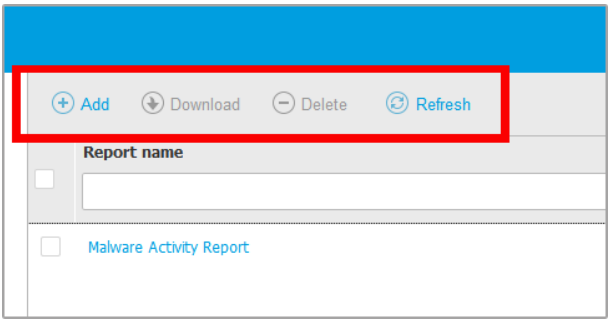
Чтобы убедиться, что консоль отображает последнюю информацию, нажмите кнопку **Обновить** в верхней части таблицы.

Данная функция может быть полезной, если вы длительное время находитесь на странице.

4.2.3. Панели инструментов

Панели инструментов в Control Center позволяют выполнять определенные операции, относящиеся к разделу, в котором вы находитесь. Каждая панель инструментов содержит набор иконок, которые обычно расположены вверху таблицы. Например, панель инструментов в разделе **Отчеты** позволяет вам выполнить следующие действия:

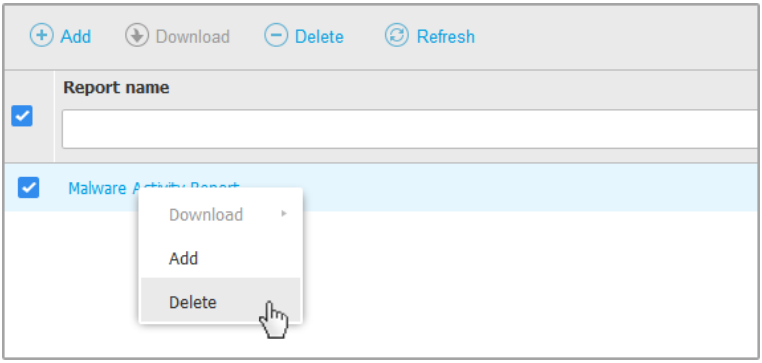
- Создать новый отчет.
- Загрузить отчет по расписанию.
- Удалить отчет по расписанию.



Страница отчетов - Панель Инструментов.

4.2.4. Контекстное меню

Также команды панели инструментов доступны из контекстного меню. При нажатии правой кнопки мыши в разделе Control Center, в котором вы находитесь, вы можете выбрать необходимую команду из предложенного списка.

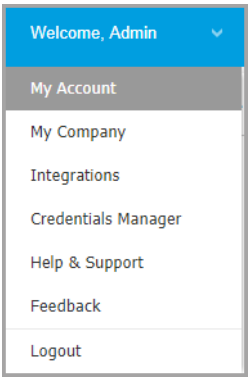


Страница отчетов - Контекстное меню

4.3. Управление вашей учетной записью

Чтобы проверить или изменить данные и настройки вашей учетной записи:

1. Нажмите на ваше имя пользователя в правом верхнем углу консоли и выберите **Мой аккаунт**.



Меню учетных записей

2. **Подробности аккаунта**, позволяет исправить или обновить данные учетной записи.
   - **Полное имя.** Введите свое полное имя.
   - **Эл. почта.** Это ваш логин и контактный адрес электронной почты. Отчеты и важные уведомления безопасности будут отправляться на этот адрес. Уведомления по электронной почте рассылаются автоматически всякий раз при обнаружении значимых угроз в сети.
   - Ссылка **Изменить пароль** позволяет изменить пароль для входа.
3. **Настройки** позволяет настроить параметры учетной записи в соответствии с вашими предпочтениями.
   - **Часовой пояс.** Выберите в меню часовой пояс для вашего аккаунта. Консоль будет отображать информацию о времени в соответствии с выбранным часовым поясом.
   - **Язык.** Выберите из меню язык отображения консоли.
   - **Временной интервал сеанса.** Выберите временной интервал до завершения вашего сеанса в результате бездействия.
4. В разделе **Login Security** настройте двухфакторную аутентификацию и проверьте состояние политик, доступных для защиты Вашей учетной записи GravityZone. Общекорпоративные политики доступны только для чтения

   Чтобы включить двухфакторную аутентификацию:

a. **Двухфакторная аутентификация.** Двухфакторная идентификация добавляет дополнительный слой защиты доя Вашего аккаунта GravityZone, требуя код аутентификации помимо Вашего статуса / полномочий Control Center.

   При первом входе в свою учетную запись GravityZone Вам будет предложено загрузить и установить Аутентификатор Google Authenticator, Microsoft Authenticator или любой двухфакторный TOTP (Time-Based One-Time Password Algorithm), совместимый со стандартным RFC6238 на мобильном устройстве, связать его с Впшей учетной записью GravityZone, а затем использовать его с каждым входом в систему Control Center. Приложение аутентификации генерирует шестизначный код каждые 30 секунд. Для завершения входа в систему Control Center после ввода пароля Вам необходимо будет ввести шестизначный код, сгенерированный приложением.

   Примечание
   Вы можете пропустить этот этап 3 раза, затем вам будет недоступен вход без двухфакторной аутентификации.

   Чтобы включить двухфакторную аутентификацию:

   i. Нажмите на **Включено** кнопку, расположенную под **Двухфакторная аутентификация** сообщением.

   ii. В диалоговом окне нажмите соответствующую ссылку, чтобы загрузить и установить выбранное приложение-аутентификатор на свое мобильное устройство.

   iii. Откройте приложение на Вашем мобильном устройстве.

   iv. На экране **Доавить аккаунт** отсканируйте QR-код, чтобы связать приложение с вашим аккаунтом GravityZone.

   Вы также можете ввести секретный ключ вручную.

   Произвести это действие требуется единожды, чтобы включить активировать функцию в GravityZone.

   Важно
   Убедитесь, что скопировали и сохранили в надежном месте ваш секретный ключ. Нажмите **Напечатать резервную копию**, чтобы создать PDF файл с QR-кодом и секретным ключом. Если мобильное устройство, используемое для активации двухфакторной

аутентификации, потеряно или заменено, Вам необходимо будет установить выбранное приложение autheticator на новое устройство и предоставить секретный ключ, чтобы связать его с Вашей учетной записью GravityZone.

v. Введите 6-значный код в поле **Код аутентификации**.

vi. Нажмите **Включить**, чтобы завершить активацию данной функции.

Примечание
Администратор вашей компании может сделать двухфакторую аутентификацию обязательной для всех аккаунтов GravityZone. В этом случае вам будет предложено при входе настроить ваш 2FA. В то же время, вы не сможете деактивировать 2FA для своей учетной записи, если эта функция применяется администратором вашей компании.
Имейте ввиду, что если для вашей учетной записи отключен 2FA, то секретный ключ не будет действительным.

b. **Политика истечения срока действия пароля.** Регулярные изменения Вашего пароля обеспечивают дополнительный уровень защиты от несанкционированного использования паролей или ограничивают продолжительность несанкционированного использования. При включении функции GravityZone требуется изменить пароль не позднее чем через 90 дней.

c. **Политика блокировки учетной записи.** Эта политика запрещает доступ к Вшей учетной записи после пяти последовательных неудачных попыток входа в систему. Эта мера используется с целью защиты от зловредных действий.

Чтобы разблокировать свою учетную запись, Вам нужно сбросить пароль со страницы входа в систему или обратиться к другому администратору GravityZone.

5. Нажмите **Сохранить**, чтобы сохранить изменения.

Примечание
Вы не можете удалить собственную учетную запись.

4.4. Изменение пароля для входа в систему

После того, как ваша учетная запись будет создана, вы получите письмо с учетными данными для входа.

Рекомендуется выполнить следующие действия:

- Изменить пароль по умолчанию, который вы в первый раз использовали при доступе к Control Center.
- Периодически менять пароль для входа.

Чтобы изменить пароль для входа:

1. Нажмите на ваше имя пользователя в правом верхнем углу консоли и выберите **Мой аккаунт**.
2. В **Account Details** нажмите **Change password**.
3. Введите текущий пароль и новый пароль в соответствующие поля.
4. Нажмите **Сохранить**, чтобы сохранить изменения.

4.5. Управление Вашей Компанией

Как **пользователь**, управляющей компанией, Вы можете проверять или изменять сведения о компании и настройки лицензии, а также управлять настройками проверки подлинности, такими как единый вход в систему и идентификация.

4.5.1. Детали и настройки лицензии

Чтобы проверить или изменить информацию о вашей компании и параметры лицензии:

1. Нажмите на ваше имя пользователя в правом верхнем углу консоли и выберите **My Company**.
2. В разделе **Company Details** заполните информацию о вашей компании, такую как название компании, адрес и телефон.

   Вы можете изменить логотип, отображаемый в Control Center, а также в отчетах вашей компании и уведомлениях по электронной почте следующим образом:

   - Нажмите **Change**, чтобы найти изображение логотипа на вашем компьютере. Формат файла изображения должен быть .png или .jpg, а размер изображения должен быть 200x30 пикселей.

- Нажмите **Default**, чтобы удалить изображение и сбросить его на изображение, предоставленное Bitdefender.

3. По умолчанию, ваша компания может управляться другими учетными записями партнеров, у которых ваша компания перечисленна в их Bitdefender Control Center. Вы можете блокировать доступ этих компаний к сети, отключив опцию **Allow your partner to assist with the security management of this company** (Разрешить вашему партнеру помогать управлять безопасностью этой компании). В результате ваша сеть не будет видна в Control Center других компаний, но они смогут управлять вашими подписками.
4. В разделе **Лицензия** вы можете просматривать и изменять свои данные о лицензии, также вы можете ввести дополнительный ключ.
   - Чтобы добавить новый лицензионный ключ:
     a. Из меню **Type menu** выберите типа подписки **License**.
     b. Введите ключ в поле **Лицензионный ключ**.
     c. Нажмите кнопку **Check** и подождите пока Control Center не получит информацию о введенном лицензионном ключе.
   - Для проверки данных лицензионного ключа, посмотрите информацию, отображаемую ниже лицензионного ключа:
     – **Expiry date**: дата, до которой лицензионный ключ может быть использован.
     – **Used**: количество использованных мест от общего количества мест лицензионного ключа. Лицензия на рабочее место считается использованной, когда клиент Bitdefender был установлен на конечной точке в сети под вашим руководством.
     – **Общее количество**: общее количество мест, доступных для вашего лицензионного ключа или вашей подписки.

     Кроме того, если вы используете ежемесячную подписку, вы можете сгенерировать отчет **Monthly License Usage** за текущий месяц. Для получения более подробной информации, обратитесь к **Ежемесячное использование лицензии** .
   - Чтобы ввести дополнительный ключ:
     – Заполните поле **Дополнительный ключ**.

– Нажмите кнопку **Добавить** и дождитесь пока GravityZone проверит дополнительный ключ. Если он действителен, Control Center получает следующую информацию о добавлении: тип, ключ и возможность его удаления.

Примечание
Поле **Добавочный ключ** не отображается, если у вас пробная или месячная лицензия.

5. В разделе **Bitdefender Partner** Вы можете найти информацию о Вашей компании-поставщике услуг.

   Чтобы изменить вашего поставщика услуг:

   a. Нажмите кнопку **Change**.

   b. Введите идентификационный код компании-партнера в поле **Partner ID**.

   Примечание
   Каждая компания может найти свой идентификатор на странице **My Company**. После того как вы заключили соглашение с компанией-партнером, его представитель должен предоставить вам свой ID Control Center (ID Центра Управления).

   c. Нажмите **Сохранить**.

   В результате ваша компания автоматически переместится от предыдущего партнера к новому партнеру в Control Center.

6. Нажмите **Сохранить**, чтобы сохранить изменения.

4.5.2. Настройки проверки подлинности

GravityZone предоставляет дополнительные опции для безопасной аутентификации пользователя в Центре управления, такие как:

- Двухфакторная аутентификация
- Срок действия пароля истекает
- Блокировка аккаунта
- Единый вход

Как администратор компании Вы можете активировать без проблем меры безопасности данного входа в систему для всей Вашей компании:

1. Перейдите к **Конфигурации > Настройки идентификации** страницы.
2. Выберите иди создайте опции, которые Вам необходимы.

   Более подробную информацию о каждом варианте можно найти в следующих разделах.
3. Нажмите **Сохранить**, чтобы применить следующее.

Принудительная двухфакторная аутентификация

Двухфакторная аутентификация (2FA) подтверждает, что лицо, пытающееся войти в Control Center, является предполагаемым пользователем. 2FA запрашивает код аутентификации в дополнение к учетным данным Control Center при каждом входе в систему. В GravityZone используются Google Authenticator, Microsoft Authenticator или любой двухфакторный TOTP (Time-Based One-Time Password Algorithm) аутентификатор, совместимый со стандартом RFC6238.

В GravityZone принудительная двухфакторная аутентификация включается по умолчанию для всей компании. Это означает, что все пользователи GravityZone должны настроить и использовать 2FA со своими учетными записями.

Отказ от этого параметра приведет к деактивации принудительного исполнения 2FA. Вам нужно будет подтвердить эти действия. В результате пользователи по-прежнему будут обладать доступным 2FA, но они смогут отключить его в настройках своей учетной записи.

Примечание

- Вы можете просмотреть статус двухфакторной аутентификации для учетной записи на странице **Учетные записи**.
- Если пользователь с включенным 2FA не может войти в систему GravityZone (из-за нового устройства или потерянного секретного ключа для приложения Authenticator), Вы можете сбросить его активацию двухфакторной аутентификации из настроек своей учетной записи на странице **Учетные записи**. Дополнительные сведения см. в разделе «Управление двухфакторной аутентификацией» (p. 42).

Установить максимальный срок действия пароля в 90 дней.

Этот параметр включает политику истечения срока действия пароля. Пользователи должны изменить свои пароли раньше указанного срока. В противном случае, у них не будет возможности входить в GravityZone еще.

После пяти попыток введения неверного пароля аккаунт будет заблокирован

Этот параметр ограничивает количество последовательных недействительных паролей для предотвращения атак. Когда счетчик достигает порогового значения, учетная запись блокируется, и пользователю необходимо сбросить свой пароль.

Политика будет применима к аккаунтам, созданным в GravityZone.

Настройте единый вход в систему при помощи SAML

GravityZone поддерживает единый вход (SSO), инициированный поставщиком услуг в качестве простой и безопасной альтернативы классическому входу в систему с именем пользователя и паролем.

Этот метод требует интеграции со сторонними поставщиками удостоверений (IdP), использующими SAML 2.0, такими как AD FS, Okta и Azure AD, которые аутентифицируют пользователей GravityZone и предоставляют им доступ к Control Center.

Это принцип, по которому GravityZone SSO работает:

1. Пользователи вводят адрес электродной почты GravityZone при входе на страницу:
2. GravityZone создает запрос SAML и направляет его вместе с пользователями поставщику удостоверений.
3. Пользователи должны пройти аутентификацию у провайдера идентификаций.
4. После аутентификации поставщик удостоверений отправляет ответ в GravityZone в виде XML-документа, подтверждённого сертификатом X. 509. Также поставщик удостоверений перенаправляет пользователей на GravityZone.

5. GravityZone извлекает ответ, проверяет его с помощью отпечатка пальца на сертификате и позволяет пользователям входить в Control Center без какого-либо другого взаимодействия с ними.

Пользователи продолжают автоматически входить в Control Center до тех пор, пока их сеанс с поставщиком удостоверений активен.

Чтобы сделать SSO доступным, Вам необходимо предпринять следующее:

1. Сконфигурируйте провайдера идентификации для использования GravityZone в качестве поставщика услуг. Дополнительные сведения о поддерживаемых поставщиках удостоверений и конфигурации ищите в статье this KB article.
2. Включите SSO для вашей компании:
   a. В разделе **Настройка единого входа с использованием SAML** введите URL-адрес метаданных провайдера идентификации в соответствующем поле и нажмите**Сохранить**.
   b. Нажмите **Сохранить**.
3. Настройте пользователей в Вашей компании для проверки подлинности с помощью своего поставщика удостоверений. Дополнительные сведения см. в разделе «Управление методами аутентификации пользователя» (p. 41).

Важно
Являясь администратором GravityZone, Вы имеете право настроить единый вход для пользователей в Вашей компании, но не для Вашей собственной учетной записи из соображений безопасности.

Чтобы отключить единый вход для вашей компании:

1. Удалите URL-адрес метаданных провайдера идентификации.
2. Нажмите **Сохранить** и подтвердите действие.

При отключении единого входа для вашей компании пользователи автоматически переключаются на вход с учетными данными GravityZone. Пользователи могут получить новые пароли, нажав ссылку **Забыли пароль?** на странице входа Control Center и следуя инструкциям.

При повторном включении единого входа для вашей компании пользователи продолжат входить в Control Center с учетными данными GravityZone. Вам

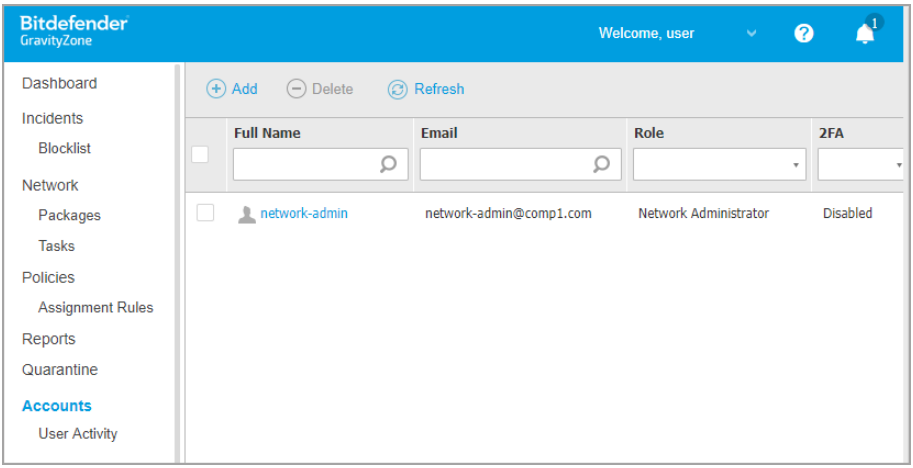
необходимо вручную настроить каждую учетную запись для повторного использования единого входа.

5. УЧЕТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ

Вы можете настроить и управлять GravityZone из Control Center, используя учетную запись, полученную после подписки на услугу.

Вот, что вам нужно знать об учетных записях GravityZone:

- Чтобы разрешить другим сотрудникам компании доступ к Control Center, вы можете создавать внутренние аккаунты для пользователей. Вы можете назначить учетные записи с разными ролями, в соответствии с их уровнем доступа в компании.
- Для каждой учетной записи пользователя, вы можете настроить доступ к функциям GravityZone или к определенным частям сети, к которой он принадлежит.
- Вы можете управлять только учетными записями с равными или меньшими правами.



Страница учетных записей

Существующие учетные записи будут отображаться в таблице. Для каждой учетной записи пользователя, вы можете просмотреть следующее:

- Имя пользователя учетной записи.

- Адрес электронной почты учетной записи (используется для входа в Control Center). Отчеты и важные уведомления безопасности будут отправляться на этот адрес. Уведомления по электронной почте рассылаются автоматически всякий раз при обнаружении значимых угроз в сети.
- Роль пользователя (администратор компании / сетевой администратор / специалист по безопасности / пользовательская).
- Статус двухфакторной аутентификации, который позволяет быстро проверить, включена ли у пользователя двухфакторная аутентификация.
- Метод проверки подлинности, который указывает, входит ли пользователь с учетными данными GravityZone или с помощью поставщика идентификации для единого входа (SSO).

5.1. Роли пользователей

Роль пользователя состоит из определенных комбинаций прав пользователей. При создании учетной записи пользователя, вы можете выбрать одну из предопределенных ролей или вы можете создать собственную роль, выбрав только определенные права пользователя.

Примечание
Вы можете управлять только аккаунтами с равными правами, как у вашего аккаунта, или ниже.

Доступны следующие роли пользователей:

1. **Company Administrator** - Подходит для менеджеров компаний-клиентов, которые приобрели лицензию GravityZone у партнера. Администратор компании управляет лицензией, профилем компании и полным развертыванием GravityZone в сети, позволяя осуществлять высокоуровневый контроль над всеми параметрами безопасности (если параметры не были изменены учетной записью его родительского партнера на сценарий поставщика услуг безопасности). Администраторы компании могут частично или полностью делегировать свои оперативные обязанности подчиненным администраторам и специалисту по безопасности учетных записей пользователей.
2. **Администратор сети** - Несколько аккаунтов могут быть созданы в компании с ролями Сетевого администратора, с административными

привилегиями по развертыванию агентов безопасности во всей компании или по определенным группам конечных точек, включая управление пользователями. Сетевые администраторы отвечают за активное управление настройками безопасности сети.

3. **Специалист по безопасности** - учетные записи специалиста по безопасности доступны только для чтения. Они разрешают доступ только к данным, отчетам и журналам,связанным с безопасностью. Такие учетные записи могут быть созданы для персонала, отвечающего за мониторинг безопасности или для других сотрудников, которые должны отслеживать статус безопасности.
4. **Пользователь** - Предопределенные роли пользователей, включающие определенную комбинацию прав пользователей. Если предопределенная роль пользователя не соответствует вашим требованиям, вы можете создать собственный аккаунт, назначив ему те права, в которых вы заинтересованы.

В следующей таблице приведена взаимосвязь различных ролей аккаунта и их прав. Для получения дополнительной информации перейдите к «Права пользователя» (p. 38).

Роль аккаунта	Разрешения дочерних учетных записей	Права пользователя
Администратор компании	Администратор компании, Сетевой администратор, Специалист по безопасности	Управление компанией Управление пользователями Управление сетями Просмотреть и проанализировать данные
Сетевой администратор	Сетевой администратор, аналитик по безопасности	Управление пользователями Управление сетями Просмотреть и проанализировать данные
Аналитик по безопасности	-	Просмотреть и проанализировать данные

5.2. Права пользователя

Вы можете назначить следующие права доступа учетным записям GravityZone:

- **Управление пользователями**. Создание, редактирование или удаление учетных записей пользователей.
- **Управление компанией**. Пользователи могут управлять своим собственным лицензионным ключом GravityZone и редактировать параметры профиля компании. Эти права только для учетных записей администраторов компании.
- **Управление сетями**. Обеспечивает административные права по настройкам сетевой безопасности (инвентаризация сети, политики, задачи, инсталляционные пакеты, карантин). Эти права только для учетных записей сетевых администраторов.
- **Просмотреть и проанализировать данные**. Просмотр события и журналы безопасности, управление отчетами и приборная панель.

5.3. Управление учетными записями пользователей

Перед тем как создать учетную запись пользователя, убедитесь, что у вас под рукой есть требуемый адрес электронной почты. Этот адрес является обязательным для создания учетной записи пользователя GravityZone. Пользователи получат свои учетные данные GravityZone на указанный адрес электронной почты.

5.3.1. Индивидуальное управление учетными записями пользователей

В Control Center вы можете персонально создавать, редактировать и удалять учетные записи пользователей.

Индивидуальное создание учетных записей пользователей

Чтобы добавить учетную запись пользователя в Control Center:

1. Перейдите на страницу **Аккаунты**.
2. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Появится окно конфигурации.
3. В разделе **Подробная информация** укажите следующее:

- – **Имя пользователя** для локальной учетной записи. Отключите **Импорт из Active Directory** и введите имя пользователя.
  - – **Email**. Введите адрес электронной почты пользователя.

    Адрес электронной почты должен быть уникальным. Вы не можете создать другую учетную запись пользователя с одним и тем же адресом электронной почты.

    GravityZone использует данный адрес электронной почты для отправки уведомлений.
  - – **Полное имя**. Введите полное имя пользователя.

4. В разделе **Настройки и привилегии**, настройте следующие параметры:
   - **Часовой пояс**. Выберите в меню часовой пояс для учетной записи. Консоль будет отображать информацию о времени в соответствии с выбранным часовым поясом.
   - **Язык**. Выберите в меню консоли язык отображения.
   - **Метод аутентификации**. Этот параметр доступен для учетных записей в компании с включенной единой регистрацией. Выберите в меню учетную запись для входа в систему с использованием учетных данных GravityZone или поставщика идентификации. Для получения подробной информации о доступных методах аутентификации см. «Управление методами аутентификации пользователя» (p. 41).
   - **Роль**. Выберите роль пользователя. Для получения подробной информации относительно ролей пользователей, обратитесь к «Роли пользователей» (p. 36).
   - **Права**. Каждая предопределенная роль пользователя имеет определенную конфигурацию прав. Тем не менее, вы можете выбрать те права, которые вам нужны. В этом случае, роль пользователя изменится на **Пользователь**. Для получения подробной информации относительно прав пользователей, обратитесь к «Права пользователя» (p. 38).
   - **Выбрать цель**. Выберите группы сетей, к которым пользователь будет иметь доступ.
5. Нажмите **Save**, чтобы добавить пользователя. Новая учетная запись появится в списке учетных записей пользователей.

Примечание
Пароль для каждой учетной записи автоматически генерируется при ее создании и отправляется пользователю на адрес электронной почты вместе с другими данными аккаунта.
Вы можете изменить пароль после того, как учетная запись создана. Нажмите на имя учетной записи в разделе **Accounts**, чтобы изменить свой пароль. После изменения пароля, пользователь немедленно уведомляется по электронной почте.
Пользователи могут изменять свой пароль для входа из Control Center, на странице **My Account**.

Индивидуальное редактирование учетных записей пользователей

Чтобы добавить учетную запись пользователя в Control Center:

1. Войдите в Control Center.
2. Перейдите на страницу **Аккаунты**.
3. Нажмите на имя пользователя.
4. Измените данные учетной записи и настройки при необходимости.
5. Нажмите **Сохранить**, чтобы сохранить изменения.

Примечание
Все аккаунты с правами **Управление пользователями** могут создавать, редактировать и удалять учетные записи других пользователей. Вы можете управлять только аккаунтами с равными правами, как у вашего аккаунта, или ниже.

Индивидуальное удаление учетных записей пользователей

Чтобы удалить учетную запись пользователя в Control Center:

1. Войдите в Control Center.
2. Перейдите на страницу **Аккаунты**.
3. Выберите учетную запись пользователя из списка.
4. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы.
   Нажмите **Да** для подтверждения.

5.4. Управление методами аутентификации пользователя

При создании или редактировании учетной записи пользователя в компании с включенным единым входом (SSO) можно настроить ее способ входа в Control Center.

В разделе **Настройки и привилегии** доступны следующие параметры:

- **Войдите в систему, используя учетные данные GravityZone**. Выберите эту опцию для этой учетной записи, чтобы войти в Control Center с именем пользователя и паролем.
- **Вход в систему с помощью вашего провайдера удостоверений**. Выберете данную опцию для этого аккаунта, чтобы воспользоваться единым входом (SSO).

Вы можете настроить метод идентификации для GravityZone, считающий пользователей одного за другим.

GravityZone поддерживает различные методы идентификации для пользователей в одной и той же компании. Таким образом, некоторые учетные записи могут входить в систему с именем пользователя и паролем, в то время как другие могут проходить аутентификацию у поставщика удостоверений.

Подробнее о том, как включить единый вход для вашей компании, см. «Настройте единый вход в систему при помощи SAML» (p. 32).

Важно

- Являясь администратором GravityZone, Вы имеете право настроить единый вход для пользователей в Вашей компании, но не для Вашей собственной учетной записи из соображений безопасности.
- Для единого входа пользователи должны иметь в GravityZone те же адреса электронной почты, что и у поставщика удостоверений. Адреса электронной почты чувствительны к регистру при SSO GravityZone. Например, **username@company.domain** отличается от**UserName@company.domain** и **USERNAME@company.domain**.
- Bitdefender управляет двумя облачными экземплярами GravityZone. В некоторых случаях пользователям может потребоваться выбрать один экземпляр при первом входе в систему.

Чтобы проверить изменения, связанные с единым входом для пользователей GravityZone, перейдите на страницу **учетные записи > активность пользователя** и отфильтруйте журналы активности в области > настройки аутентификации.

5.5. Сброс паролей входа

Акаунты владельцев, которые забыли свой пароль, можно сбросить с помощью восстановления пароля, использовав ссылку на странице входа. Вы также можете сбросить забытый пароль, отредактировав соответствующий аккаунт из консоли.

Чтобы сбросить пароль пользователя для входа:

1. Войдите в Control Center.
2. Перейдите на страницу **Аккаунты**.
3. Нажмите на имя пользователя.
4. Введите новый пароль в соответствующих полях (в **Подробности**).
5. Нажмите **Сохранить**, чтобы сохранить изменения. Владелец аккаунта получит письмо с новым паролем.

5.6. Управление двухфакторной аутентификацией

Выбрав учетную запись пользователя, вы сможете просматривать статус его двухфакторной аутентификации (вкл или выкл) в разделе **Двухфакторная аутентификация**. Вы можете предпринять следующие действия:

- **Сбросить или отключить двухфакторную аутентификацию пользователя**. Если пользователь с двухфакторной аутентификацией изменил или стер мобильное устройство и потерял секретный ключ:

  1. Введите пароль GravityZone в поле доступа.
  2. Нажмите **Сбросить** (когда двухфакторная аутентификация включена) or **Отключить** (когда двухфакторная аутентификация выключена).
  3. Сообщение с подтверждением информирует вас о том, что двухфакторная аутентификация была сброшена / отключена для текущего пользователя.

     После отключения двухфакторной аутентификации, когда эта функция включена, при входе в учетную запись окно конфигурации предложит

пользователю заново настроить двухфакторную аутентификацию с новым секретным ключом.

- Если у пользователя отключена двухфакторная аутентификация, и вы хотите ее активировать, вам будет необходимо попросить пользователя включить эту функцию в настройках его учетной записи.

Примечание
Если у вас есть учетная запись администратора компании, вы можете включить двухфакторную аутентификацию для всех учетных записей GravityZone в вашей компании. Для получения более подробной информации, обратитесь к «Управление Вашей Компанией» (p. 28).

Важно
Приложение аутентификации по выбору (Google Authenticator, Microsoft Authenticator или любой двухфакторный TOTP (Time-Based One-Time Password Algorithm) аутентификатор, совместимый сстандартом RFC6238), объединяет секретный ключ с текущей отметкой времени мобильного устройства для генерации шестизначного кода. Имейте ввиду, что текущая метка времени на мобильном устройстве и устройстве GravityZone должны совпадать, чтобы 6-значный ключ оказался рабочим. Чтобы избежать проблем при синхронизации временных меток, мы рекомендуем включать автоматические настройки времени и даты на мобильном устройстве.

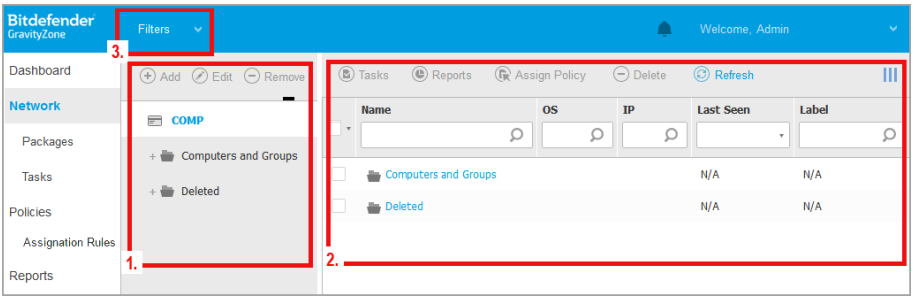
Другой метод проверки изменений двухфакторной аутентификации, связанных с учетными записями пользователей, заключается в том, чтобы получить доступ к странице **Учетные записи > Активность пользователя** и просмотреть журналы активности с помощью следующего фильтра:

- Область > Учетные записи / Компания
- Действие > Изменено

Чтобы получить больше информации о включении двухфакторной аутентификации, оращайтесь к«Управление вашей учетной записью» (p. 24)

6. УПРАВЛЕНИЕ КОНЕЧНЫМИ ТОЧКАМИ

Страница **Network** предоставляет несколько возможностей для просмотра и управления доступными конечными точками. Интерфейс страницы **Сеть** состоит из двух панелей, которые в реальном времени отображают состояние конечных точек:



Раздел - Сеть

1. Левая панель отображает доступную структуру сети в виде дерева.

   Все удаленные конечные точки хранятся в папке **Deleted**. Чтобы узнать больше, обратитесь к «Удаление конечных точек из сетевого содержимого» (p. 122).

   Примечание
   Вы можете просматривать и управлять только группами, на которые у вас есть права администратора.

2. Правая панель отображает содержимое выбранной в дереве сети группы. Эта панель представляет собой сетку, где строки содержат сетевые объекты, а столбцы определенную информацию для каждого типа объекта.

   В этой панели, вы можете сделать следующее:

   - Просмотреть под своей учетной записью подробную информацию о каждом объекте сети. Вы можете просмотреть состояние каждого объекта, проверяя значок рядом с его именем. Нажмите на название объекта, чтобы отобразить окно, содержащее более конкретные детали.

     Каждый тип объекта, например компьютер, виртуальная машина или папка, представлены соответствующей иконкой. Каждый объект сети

может иметь определенный статус, характеризующий состояние управления, проблемы безопасности, связи и так далее. Для получения подробной информации относительно описания каждого значка сетевого объекта и имеющихся статусов, обратитесь к «Типы сетевых объектов и статусы» (p. 508).

- Используйте Панель инструментов в верхней части таблицы, чтобы выполнить определенные операции над каждым сетевым объектом (например, запуск задачи, создание отчетов, назначение политики и удаление) и обновление данных таблицы.

3. Меню **Фильтры**, доступное в верхней части сетевой панели, легко позволяет отображать только определенные сетевые объекты, предоставляя несколько способов фильтрации.

На странице **Сеть** вы также можете управлять пакетами установки и разделом Задачи управляемых вами конечных точек.

Примечание
Чтобы узнать больше об инсталляционных пакетах, обратитесь к руководству по установке GravityZone.

Чтобы отобразить конечные точки под вашей учетной записью, перейдите на страницу **Network** и выберите нужную сетевую группу в левой панели.

Вы можете увидеть доступную структуру сети в левой панели и детальную информацию о каждом конечном устройстве на панели справа.

Все компьютеры и виртуальные машины, обнаруженные в вашей сети, отображаются как неуправляемые (Неуправляемый) и вы можете удаленно произвести установку защиты на них.

Для настройки детальной информации о конечных точках, отображаемых в таблице:

1. Нажмите кнопку **Колонки** справа от Панель действий
2. Выберите столбцы, которые вы хотите отобразить.
3. Нажмите кнопку **Восстановить**, чтобы вернуться к виду столбцов по умолчанию.

На странице **Network** вы можете управлять конечными точками как указано ниже:

- Проверка состояния конечных точек
- Просмотр информации о конечных точках

- Организация конечных точек в группы
- Выполнить сортировку, фильтрацию и поиск
- Управление патчами
- Запустить задачи
- Определение интеграции с Active Directory
- Сформировать быстрые отчеты
- Назначить политики
- Удаление конечных точек из инвентаризации сети

Для просмотра самой актуальной информации, нажмите кнопку **Обновить** в нижнем левом углу таблицы. Данная функция может быть полезной, если вы длительное время находитесь на странице.

6.1. Проверка состояния конечных точек

Каждая конечная точка представлена на странице сети иконкой определенного типа и состояния.

Обратитесь к «Типы сетевых объектов и статусы» (p. 508), чтобы просмотреть список со всеми доступными типами значков и статусов.

Для получения подробной информации о статусе, обратитесь к:

- Состояние управления
- Состояние подключения
- Статус безопасности

6.1.1. Состояние управления

Конечные точки могут иметь следующие статусы управления:

- **Управляемые** - конечные точки, на которых установлен агент безопасности.
- **Ожидают перезагрузки** - конечные точки, которые требуют перезагрузки системы после установки или обновления системы защиты Bitdefender.
- **Неуправляемые** - обнаруженные конечные точки, на которых агенты безопасности еще не были установлены.
- **Удаленные** - конечные точки, которые вы удалили из Control Center. Для получения более подробной информации, обратитесь к «Удаление конечных точек из сетевого содержимого» (p. 122).

6.1.2. Состояние подключения

Статус подключения имеет отношение ко всем виртуальным машинам и только к управляемым компьютерам. Управляемые конечные точки могут быть:

- **Онлайн**. Синий значок означает, что конечная точка находится в состоянии он-лайн.
- **Офлайн**. Серый значок означает, что конечная точка находится в состоянии офф-лайн.

Конечная точка переходит в режим офф-лайн, если агент безопасности неактивен более 5 минут. Возможные причины, по которым конечные точки находятся в режиме офф-лайн:

- Конечная точка выключена, в режиме сна или гибернации.

  Примечание
  Конечная точка остается в режиме он-лайн, даже когда она заблокирована или пользователь отключен.

- Агент безопасности не имеет подключения к Bitdefender Control Center или с назначенным Endpoint Security Relay:
  - Конечная точка может быть отключена от сети.
  - Сетевой брандмауэр или маршрутизатор может блокировать связь между агентом безопасности и Bitdefender Control Center или назначенным Endpoint Security Relay.
  - Конечная точка находится за прокси-сервером и настройки прокси-сервера не были надлежащим образом сконфигурированы в примененной политике.

    Предупреждение
    Для конечных точек, находящихся за прокси-сервером, параметры прокси-сервера должны быть правильно настроены в установочном пакете агента безопасности, в противном случае конечная точка не сможет взаимодействовать с консолью GravityZone и всегда будет отображаться со статусом офф-лайн, даже если политика с корректными настройками прокси-сервера была применена после установки.

- Агент безопасности удален вручную с конечной точки, пока отсутствовала связь конечной точки с Control Center Bitdefender или с закрепленным Endpoint Security Relay. Обычно, когда агент безопасности вручную удален с конечной точки, Control Center уведомляет об этом событии, и конечная точка помечается как неуправляемая.
- Агент безопасности работает ненадлежащим образом.

Чтобы узнать, как долго конечные точки были неактивны:

1. Показать только управляемые конечные точки. Нажмите меню **Фильтры** в верхней части таблицы, выберите все "Управляемые" варианты, которые вам нужны из вкладки **Безопасность**, выберите **Все предметы рекурсивно** из вкладки **Глубина** и нажмите **Сохранить**.
2. Нажмите на заголовок столбца **Last Seen**, чтобы отсортировать конечные точки по периоду бездействия.

Вы можете игнорировать короткие периоды бездействия (минуты, часы), так как они, вероятно, являются результатом временного состояния. Например, конечная точка в настоящее время выключена.

Более длительные периоды бездействия (дни, недели), как правило, указывают на проблемы с конечной точкой.

Примечание
Рекомендуется обновлять данные таблицы сети, время от времени, чтобы обновлять информацию о состоянии конечных точек.

6.1.3. Статус безопасности

Состояние безопасности может отображаться только для управляемых конечных точек. Вы можете определить конечные точки с проблемами безопасности, проверяя значки состояния, отображающие символ предупреждения:

- Компьютер управляется, с проблемами, онлайн.
- Компьютер управляется, с проблемами, офлайн.

Конечные точки могут иметь проблемы с безопасностью, по крайней мере, в одной из следующих ситуаций:

- Защита от вредоносных программ отключена.
- Срок действия лицензии истек.

- Агент безопасности устарел.
- Механизмы защиты устарели.
- Обнаружены вредоносные программы.
- Связь с Bitdefender Cloud Services не может быть установлена из-за следующих возможных причин:
  - Сетевой брандмауэр блокирует соединение с Bitdefender Cloud Services.
  - Порт 443, требующийся для связи с Bitdefender Cloud Services, закрыт.

  В этом случае защита от вредоносных программ полагается исключительно на локальный движок, в то время как сканирование в облаке выключено, это означает, что агент безопасности не может обеспечить полную защиту в режиме реального времени.

Если вы заметили конечную точку с проблемами безопасности, нажмите на ее имя, чтобы отобразить окно **Information**. Вы можете определить проблемы безопасности по значку ! . Убедитесь, что вы проверили информацию о безопасности на всех вкладках информационных страниц. Наведите курсор мыши на значок, чтобы отобразить подсказку, содержащую подробности. Могут потребоваться дальнейшие локальные расслдеования.

Примечание
Рекомендуется обновлять данные таблицы сети, время от времени, чтобы обновлять информацию о состоянии конечных точек.

6.2. Отображение Информации о Конечных точках

Подробные сведения о каждой конечной точке можно получить следующим образом на странице **Сеть**:

- Проверка **Сеть** страница
- Проверка **Информация** окно

6.2.1. Проверка страницы сети

Чтобы получить подробные сведения о конечной точке, проверьте информацию в правой панели таблицы на странице **Сеть**.

Чтобы добавить или удалить столбцы с информацией о конечной точке, нажмите кнопку **Столбцы** в правой верхней части панели.

1. Перейдите в раздел **Сеть**.
2. Выберите желаемую группу в левой панели.

Все доступных конечные точки выбранной группы выводятся в таблице правой панели.

3. Вы можете легко определить состояние конечной точки, проверив соответствующий значок. Для получения дополнительной информации перейдите к «Проверка состояния конечных точек» (p. 46).
4. Проверьте информацию, отображаемую в столбцах для каждой конечной точки.

   Используйте строку заголовка для поиска определенных конечных точек в соответствии с доступными критериями:

   - **Имя**: имя конечной точки.
   - **FQDN**: полное доменное имя, которое включает в себя имя хоста и имя домена.
   - **Версия OS** версия операционной системы, установленной на конечной точке.
   - **OS тип** тип операционной системы, установленной на конечной точке.
   - **IP**: IP-адрес конечной точки.
   - **Последняя активность**: дата и время, когда виртуальная машина была в последний раз онлайн.

     Примечание
     Важно следить за полем **Последняя активность**, так как длительные периоды бездействия могут указывать на проблему связи или отключении компьютера.

   - **Ярлык** : настраиваемая строка с дополнительной информацией о рабочей станции. Можете добавить метку в **Окно** Информации конечной точки, а затем использовать ее в поиске.
   - **Политика**: политика, применяемая к конечной точке, содержит ссылку для просмотра или изменения параметров политики.
   - **Тип конечной**: тип устройства, сервера или рабочей станции.

6.2.2. Проверка информационного окна

В правой боковой панели страницы **Сеть** щелкните имя интересующей вас конечной точки, чтобы отобразить окно **Сведения**. В этом окне отображаются

сгруппированные по нескольким вкладкам данные, доступные только для выбранной конечной точки.

В окне **Информация** приведен полный список сведений в соответствии с типом конечной точки и сведениями о ее безопасности.

Вкладка "Общие"

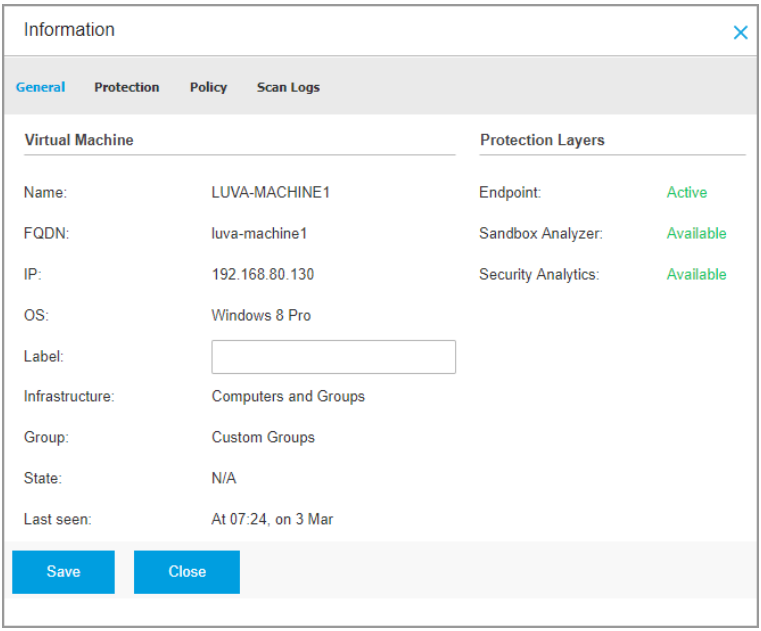
- Общие сведения о конечной точке, например, имя, полное доменное имя, IP-адрес, операционная система, инфраструктура, родительская группа и текущее состояние подключения.

  В этом разделе можно назначить конечную точку с меткой. Вы сможете быстро находить конечные точки с одной и той же меткой и принимать меры по отношению к ним, независимо от их расположения в сети. Для получения дополнительных сведений о фильтрации конечных точек перейдите к «Сортировка, Фильтрация и Поиск Конечных точек» (p. 67).

- Сведения об уровнях защиты, в том числе список технологий безопасности, приобретенных при помощи решения GravityZone, и статус их лицензии, которые могут быть:
  - **Доступен/Активный** - лицензионный ключ для данного уровня защиты активен на конечной точке.
  - **Истек срок действия** — истек срок действия лицензионного ключа для данного уровня защиты.
  - **Ожидание подтверждения** — лицензионный ключ еще не подтвержден.

    Примечание
    Дополнительная информация об уровнях защиты доступна на вкладке **Защита** .

- **Подключение ретрансляции**: имя, IP-адрес и метка ретранслятора, к которому подключена конечная точка.
- Для конечных точек сРолью Интегратора Active Directory: имя домена, дата и время последней синхронизации.



Информационное окно - вкладка «Общие»

Вкладка "Защита"

Эта вкладка содержит сведения о каждом уровне защиты, применимом на конечной точке.

- Сведения об агенте безопасности, такие как название продукта, версия, статус обновления и расположение обновлений, а также конфигурация механизмов сканирования и версии содержимого безопасности. Для изменения защиты, версия антиспама также применима.
- Состояние безопасности для каждого уровня защиты. Этот статус отображается в правой части имени уровня защиты:
  - **Безопасный**, если на конечных точках, применяемых с уровнем защиты, не обнаружены проблемы безопасности.
  - **Уязвимый**, если на конечных точках, применяемых с уровнем защиты, обнаружены проблемы безопасности. Дополнительные сведения см. в разделе «Статус безопасности» (p. 48).

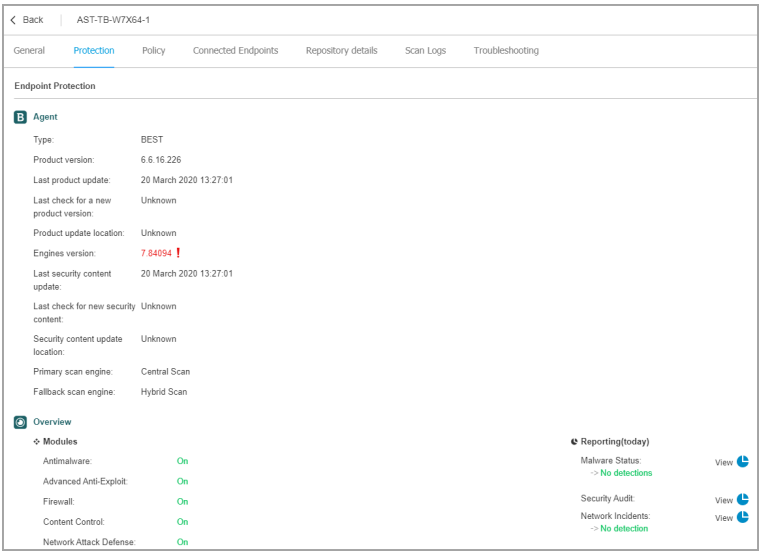
- Связанный Security Server. Каждый назначенный Security Server отображается в случае развертывания без агентов или при сканировании антивирусных механизмов безопасности, настроенных для использования удаленного сканирования. Информация Security Server помогает идентифицировать виртуальное устройство и получить статус его обновления.
- Статусы модулей защиты. Вы можете легко просмотреть, какие модули защиты были установлены на конечной точке, а также статус доступных модулей (**Вкл. / Выкл.**), установленных с помощью применяемой политики.
- Краткий обзор активности модулей и отчетов о вредоносном ПО за текущий день.

  Нажмите ссылку **Просмотр**, чтобы получить доступ к параметрам отчета, а затем Создать отчет. Для получения более подробной информации, обратитесь к «Создание отчетов» (p. 452)
- Информация, касающаяся слоя защиты Sandbox Analyzer:
  - Статус использования Sandbox Analyzer в конечных точках отображается с правой стороны окна:
    - **Активный**: Sandbox Analyzer лицензирован (доступен) и включается, исходя из политики в конечной точке.
    - **Неактивный**:Sandbox Analyzer лицензирован (доступен), но не включен, исходя из политики в конечной точке.
  - Название агента, который действует как датчик подачи.
  - Состояние модуля на конечной точке:
    - **Вкл** - Sandbox Analyzer включен в конечной точке, согласно политике.
    - **Выкл** -Sandbox Analyzer не включен в конечной точке, согласно политике.
  - Чтобы просмотреть угрозы обнаруженные на прошлой неделе, просмотрите отчет перейдя по ссылке **Просмотреть** .
- Дополнительная информация о модуле шифрования, например:
  - Обнаруженные тома (с указанием загрузочного диска).

- Состояние шифрования для каждого тома (**Зашифрован**, **Выполняется шифрование**, **Выполняется дешифрование**, **Незашифрован**, **Заблокирован** или **Приостановлен**).

  Нажмите ссылку **Восстановление** , чтобы получить ключ восстановления для соответствующего зашифрованного тома. Подробнее о получении ключей восстановления см. «Использование Менеджер восстановления (Recovery Manager) для зашифрованных томов» (p. 121).

- Информация об Аналитике безопасности, как часть обнаружения и отклика в конечной точке:
  - Информация о специальном агенте показывает:
    - Поставщик событий - агент безопасности сообщает о конечной точке и состоянии приложения компоненту Аналитики безопасности.
    - Статус взаимодействия - агент безопасности связывается с Аналитикой безопасности.
    - Последнее обновление статуса - самый последний статус.
  - Общая информация о состоянии активации датчика инцидентов.
- Состояние телеметрии безопасности, которое информирует Вас о том, установлено ли и работает ли соединение между конечной точкой и SIEM-сервером, отключено или имеет проблемы.



Информационное окно - вкладка "Защита"

Вкладка "Политика"

Конечная точка может применяться с одной или несколькими политиками, но одна политика может быть активна только с одной конечной точкой. На вкладке **Политика** отображаются сведения о всех политиках, применяемых к конечной точке.

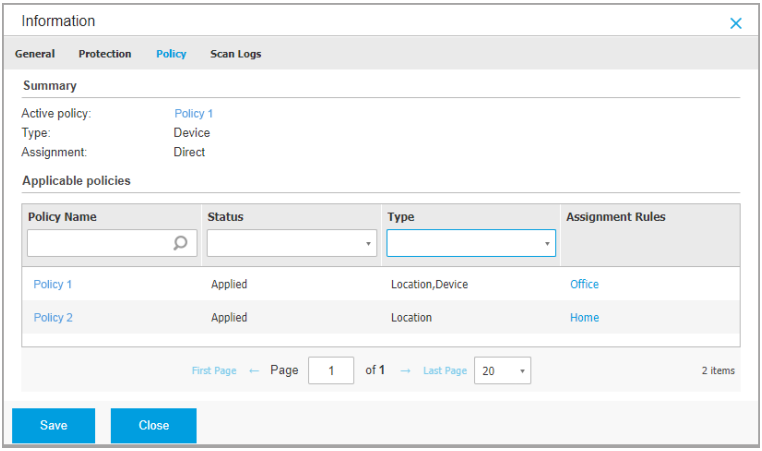
- Имя активной политики. Нажмите на название политики, чтобы открыть шаблон политики и просмотреть ее настройки.
- Тип активной политики, который может быть:
  - **Устройство**: если сетевым администратором вручную назначена политика для конечной точки.
  - **Местоположение**: политика, основываясь на правилах, автоматически назначается конечной точке в том случае, если сетевые настройки конечной точки соответствуют заданным условиям правил назначения .

    Например, ноутбуку назначены две политики по месторасположению: одна называется `Office`, которая становится активной при

подключении к сети компании, и `Roaming`, которая становится активной, когда пользователь работает удаленно и подключается к другим сетям.

  - **Пользователь**: политика, основываясь на правилах, автоматически назначается конечной точке в том случае, если она соответствует цели Active Directory, указанной в правиле назначения.

- Тип назначения активной политики, который может быть:
  - **Прямой**: если политика применяется непосредственно к конечной точке.
  - **Наследственный**: если конечная точка наследует политику родительской группы.
- **Применимые политики**: отображает список политик, связанных с существующими правилами назначения. Эти политики могут применяться к конечной точке, если она соответствует заданным условиям правил назначения.

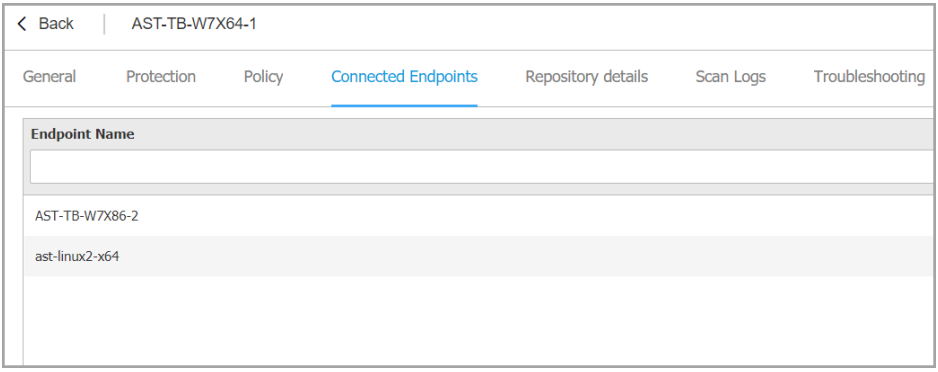


Информационное окно - вкладка «Политика»

Для получения дополнительной информации, касающейся политики, см.«Изменение настроек политики» (p. 144)

Вкладка подключенных конечных точек

Вкладка **Подключенные конечные точки** доступна только для конечных точек с ролью реле. Эта вкладка отображает информацию о конечных точках, подключенных к текущему ретранслятору, такую как имя, IP-адрес и метка.

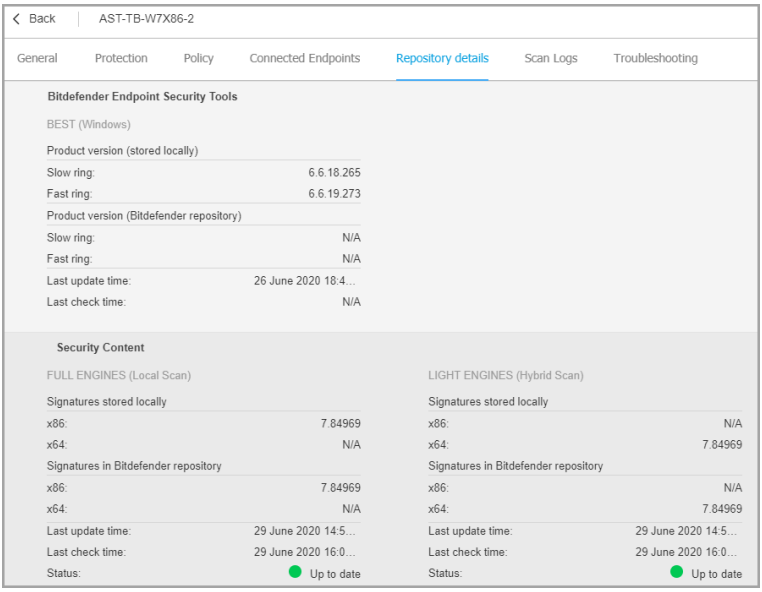


Информационное окно - вкладка подключенных конечных точек

вкладка содержимого репозитория

Вкладка **Сведения о репозитории** доступна только для конечных точек с ролью реле и отображает информацию об обновлениях агента безопасности и содержимом безопасности.

Вкладка содержит сведения о версиях продукта и сигнатур, хранящихся на реле, а также о доступных в официальном репозитории, кольцах обновлений, дате и времени обновления, и о последней проверке на наличие новых версий.



Информационное окно - вкладка содержимого репозитория

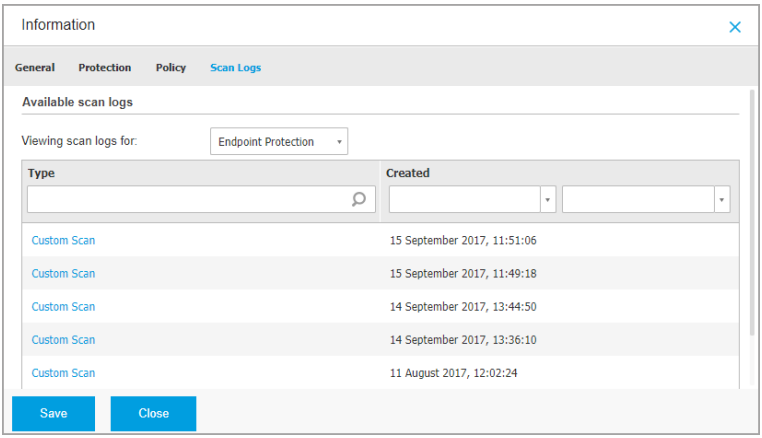
Вкладка "Журналы сканирования"

На вкладке **Сканирование журналов** отображается подробная информация обо всех задачах сканирования, выполняемых на конечной точке.

Журналы сгруппированы по уровню защиты, и вы можете выбрать в выпадающем списке, для какого уровня отображать журналы.

Выберите нужную задачу сканирования, и журнал откроется на новой странице браузера.

Если доступно много журналов сканирования, они могут занимать несколько страниц. Для перемещения по страницам используйте кнопки навигации в нижней части таблицы. Если доступно слишком много записей, вы можете использовать опции фильтрации, доступные в верхней части таблицы.

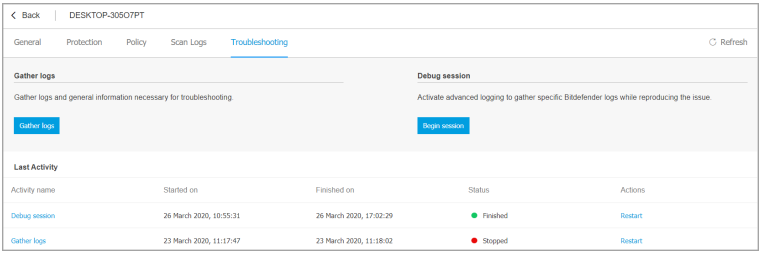


Информационное окно - вкладка «Журналы сканирования»

Вкладка "Устранение неполадок"

Этот раздел посвящен агенту устранения неполадок. Вы можете собирать общие или специальные журналы безопасности с конечных точек, проверять или участвовать в текущих событиях устранения неполадок и просматривать предыдущую активность.

Важно
Устранение неполадок доступно для компьютеров с Windows, Linux, macOS и Security Server на нескольких платформах.



Информационное окно - вкладка "Устранение неполадок"

- **Сбор журналов**

Эта опция помогает собирать журналы безопасности и общую информацию, необходимую для устранения неполадок таких как настройки, активные модули или политика безопасности, конкретная для целевой машины. Все сгенерированные данные сохраняются в архив.

Рекомендуется использовать это опцию когда источник проблемы неясен.

Для начала процесса устранения неполадок:

1. Нажмите кнопку **Сбор журналов**. Появится окно конфигурации.
2. В разделе **Хранилище журналов** выберите место хранения:
   - **Целевой компьютер**: архив журналов сохраняется по указанному локальному пути. Путь не настраивается для серверов безопасности.
   - **Общий сетевой ресурс**: архив журналов сохраняется по указанному пути из общего местоположения.
   - **Облако Bitdefender**: архив журналов сохраняется в хранилище Облака Bitdefender, где команда поддержки предприятия может получить доступ к файлам.

   Вы можете использовать опцию **Сохраняйте журналы также на целевой машине** , чтобы сохранять копию архивов журналов безопасности затронутых машин в качестве резервной копии.
3. Внесите необходимую информацию (локальные пути, параметры доступа к ресурсам сети, путь к общему доступу, идентификатор дела) в зависимости выбранного местоположения.
4. Нажмите кнопку **Сбор журналов**.

Примечание

Если вы выберете **Облако Bitdefender** в качестве опции хранения, учтите следующее:

- Архив журналов сохраняется с одинаковыми именами как в **Облаке Bitdefender**, так и на целевом компьютере. Щелкните событие устранения неполадок, чтобы просмотреть имя архива в окне сведений.
- После того, как архив загружен, пожалуйста, предоставьте службе поддержки Bitdefender Enterprise необходимую информацию (имя целевого компьютера, имя архива), по открытому делу. Откройте новое дело, если ни одного не существует.

- **Сеанс отладки**

  С помощью сеанса отладки вы можете активировать продвинутую регистрацию на целевой машине, чтобы собирать определенные журналы при воспроизведении проблемы.

  Вам следует использовать эту опцию, когда вы обнаружили, какой модуль вызывает проблемы, или по рекомендации службы поддержки Bitdefender. Все сгенерированные данные сохраняются в архив.

  Для начала процесса устранения неполадок:

  1. Нажмите кнопку **Начать сеанс**. Появится окно конфигурации.
  2. В разделе **Тип проблемы** выберите проблему, которая, по вашему мнению, касается компьютера.

     Типы проблем для компьютеров Windows и macOS:

Тип проблемы	Сценарий использования
Защита от вредоносного ПО (при доступе или при запросе)	– Общее снижение производительности конечной точки – Программа или системный ресурс слишком долго отвечает – Процесс сканирования занимает больше времени чем обычно – Нет соединения с ошибкой сервиса безопасности хоста
Ошибки обновления	– Сообщения об ошибке во время обновления продукта или механизмов защиты
Контроль содержимого (сканирование трафика и контроль пользователя)	– Сайт не загружается – Элементы на странице отображаются не полностью
Подключение к Облачным сервисам	– У конечной точки отсутствует соединение с Облачными сервисами Bitdefender

Тип проблемы	Сценарий использования
Общие проблемы продукта (чрезмерно детализированное ведение протокола)	– Воспроизведите общую сообщенную проблему с подробным ведением журнала

Типы проблем для компьютеров Linux:

Тип проблемы	Сценарий использования
Защита от вредоносных программ и обновление	– Процесс сканирования занимает больше времени, чем обычно, и потребляет больше ресурсов – Сообщения об ошибке во время обновления продукта или механизмов защиты – Не удалось установить соединение конечных точек с GravityZone консолью.
Общие проблемы продукта (чрезмерно детализированное ведение протокола)	– Воспроизведите общую сообщенную проблему с подробным ведением журнала

Типы проблем для серверов безопасности:

Тип проблемы	Сценарий использования
Защита от вредоносного ПО (при доступе или при запросе)	Любое непредвиденное поведение Сервера безопасности, в том числе: – Виртуальные машины не защищены должным образом – Задачи сканирования на наличие вредоносных программ не выполняются или занимают больше времени, чем ожидалось – Обновления продукта установлены неправильно

Тип проблемы	Сценарий использования
	– Неисправность общего сервера безопасности (демоны bd не работают)
Связь с Центром управления GravityZone	Любое неожиданное поведение, наблюдаемое из консоли GravityZone: – Виртуальные машины не отображаются должным образом в консоли GravityZone – Вопросы политики (политика не применяется) – Сервер безопасности не может установить соединение с консолью GravityZone **Примечание** Используйте этот метод по рекомендации службы поддержки Bitdefender Enterprise.

3. Для **Продолжительность сеанса отладки** выберите временной интервал после которого сеанс отладки будет автоматически завершен.

   Примечание
   Рекомендуется вручную останавливать сеанс, используя опцию **Завершить сеанс**, сразу после воспроизведения проблемы.

4. В разделе **Хранилище журналов** выберите место хранения:
   - **Целевой компьютер**: архив журналов сохраняется по указанному локальному пути. Путь не настраивается для серверов безопасности.
   - **Общий сетевой ресурс**: архив журналов сохраняется по указанному пути из общего местоположения.
   - **Облако Bitdefender**: архив журналов сохраняется в хранилище Облака Bitdefender, где команда поддержки предприятия может получить доступ к файлам.

   Вы можете использовать опцию **Сохраняйте журналы также на целевой машине** , чтобы сохранять копию архивов журналов безопасности затронутых машин в качестве резервной копии.

5. Внесите необходимую информацию (локальные пути, параметры доступа к ресурсам сети, путь к общему доступу, идентификатор дела) в зависимости выбранного местоположения.
6. Нажмите кнопку **Начать сеанс**.

Важно
Вы можете запустить только один процесс устранения неполадок за раз (**Сбор журналов/Отладка**) на уязвимом компьютере.

- **История устранения неполадок**

  Раздел **Последняя активность** показывает активность устранения неполадок на затронутом компьютере. Сетка отображает только последние 10 событий устранения неполадок в хронологическом обратном порядке и автоматически удаляет активность старше 30 дней.

  Сетка отображает детали каждого процесса устранения неполадок.

  Процесс имеет основной и промежуточный статусы. В зависимости от пользовательских настроек вы можете иметь следующий статус, где вам необходимо принять меры:

  – **Выполняется (готов к воспроизведению вопроса)** - перейдите на затронутую машину вручную или дистанционно и воспроизведите проблему.

  У вас есть несколько опций для остановки процесса устранения неполадок:

  – **Завершить сеанс**: завершает сеанс отладки и процесс сбора на машине, сохраняя все собранные данные в специальное место хранения.

    Рекомендуется использовать эту опцию сразу после воспроизведения проблемы.

  – **Отменить**: эта опция отменяет процесс и журналы безопасности не собираются.

    Используйте эту опцию, если вы не хотите собирать какие-либо журналы с целевой машины.

  – **Принудительно завершить**: принудительно завершает процесс устранения неполадок.

Используйте эту опцию, если отмена сессии занимает слишком много времени или целевая машина не отвечает. Вы сможете начать новую сессию за несколько минут.

Для повторного запуска процесса устранения неполадок:

– **Перезапуск**: эта кнопка, связанная с каждым событием и расположенная в разделе **Действия**, перезапускает выбранное действие по устранению неполадок, сохраняя прежние настройки.

Важно

– Чтобы убедиться, что консоль отображает последнюю информацию используйте кнопку **Обновить** на верхней правой стороне страницы **Устранение неполадок**.

– Для получения подробностей о конкретном событии нажмите на имя события из сетки.

6.3. Организация Конечных точек в Группы

Основным преимуществом этой функции является то, что вы можете использовать групповые политики для удовлетворения различных требований к безопасности.

Вы можете управлять группами конечных точек из левой панели страницы **Сеть** в разделе **Компьютер и группы**.

В группе **Сеть**, принадлежащей вашей компании, вы можете создавать, удалять, переименовывать и перемещать группы компьютеров в пределах созданной структуры дерева.

Примечание

- Группа может содержать как конечные точки, так и другие группы.
- При выборе группы из левой панели, вы можете просмотреть все конечные точки кроме тех, которые помещены в ее подгруппы. Чтобы просмотреть все конечные точки, включенные в группу и ее подгруппы, нажмите на меню **Filters**, расположеное в верхней части таблицы и выберите **All items recursively** в разделе **Depth**.

Создание групп

Прежде чем начать создавать группы, подумайте о причине создания, зачем они вам нужны и продумайте схему группировки. Например, вы можете сгруппировать конечные точки на основе одного или нескольких следующих критериев:

- Организационная структура (продажи, маркетинг, контроль качества, разработка программного обеспечения, управление и т.д.).
- Требования безопасности (настольные компьютеры, ноутбуки, сервера и т.д.).
- Местонахождение (штаб, местные офисы, удаленные сотрудники, домашние офисы и т.д.).

Для организации вашей сети в группы:

1. Выберите папку **Computers and Groups** в левой панели.
2. Нажмите кнопку ⊕ **Добавить группу** в верхней части левой панели.
3. Введите подходящее имя группы и нажмите **OK**.

Переименование групп

Чтобы переименовать группу:

1. Выберите группу в левой панели.
2. Нажмите кнопку ✎ **Редактировать группу** в верхней части левой панели.
3. Введите новое имя в соответствующем поле.
4. Нажмите **OK** для подтверждения.

Перемещение Групп и Конечных точек

Вы можете перемещать объекты из **Custom Groups** в любое место внутри иерархии групп. Для перемещения объекта, перетащите его из правой панели в желаемую группу левой панели.

Примечание

Объект, который перемещается, унаследует параметры политик новой родительской группы, если другая политика не была непосредственно применена к нему. Для получения более подробной информации о наследовании политик, обратитесь к «Политики безопасности (Security Policies)» (p. 134).

Удаление групп

Удаление группы - это окончательное действие. В результате агент безопасности, установленный на целевой конечной точке, будет удален.

Чтобы удалить группу:

1. Нажмите на пустую группу в левой панели раздела **Сеть**.
2. Нажмите кнопку **Удалить группу** в верхней части левой панели. Вы должны будете подтвердить ваши действия, нажав **Да**.

6.4. Сортировка, Фильтрация и Поиск Конечных точек

В зависимости от количества конечных точек, правая панель может занимать несколько страниц (всего 20 записей на каждой странице отображается по умолчанию). Для перемещения по страницам используйте кнопки навигации в нижней части таблицы. Чтобы изменить количество записей отображаемых на странице, введите другое значение в поле рядом с кнопками навигации.

Если записей слишком много, вы можете использовать поля поиска под заголовками столбцов или меню **Фильтры** в верхней части страницы, чтобы отобразить только те объекты, которые вам необходимы. Например, вы можете искать определенную конечную точку или выбрать для просмотра только управляемые конечные точки.

6.4.1. Сортировка Конечных точек

Для сортировки данных по определенному столбцу, щелкните заголовок столбца. Например, если вы хотите отсортировать конечные точки по имени, нажмите на заголовок **Name**. При повторном нажатии на заголовок, конечные точки будут отображаться в обратном порядке.

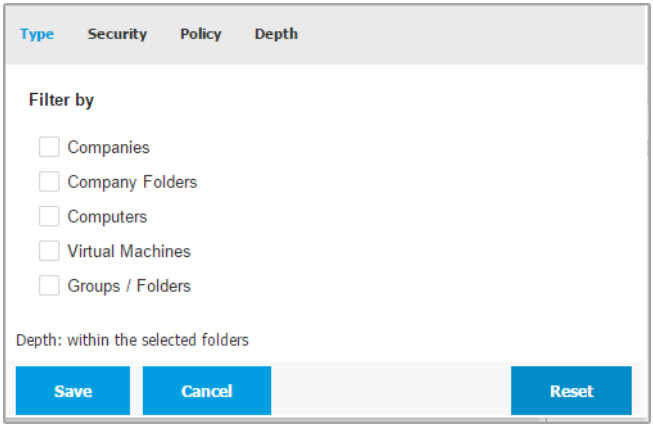
Сортировка компьютеров

6.4.2. Фильтрация Конечных точек

Чтобы отфильтровать ваши сетевые объекты, используйте меню **Фильтры** в правой верхней части сетевой панели.

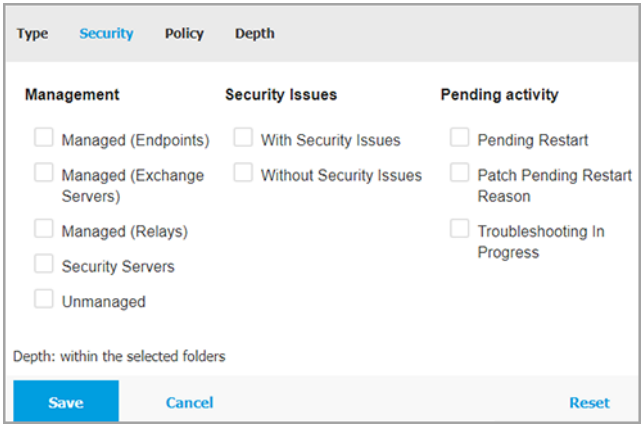
1. Выберите желаемую группу из левой панели.

2. Нажмите меню **фильтры** в правой верхней части сетевой панели.
3. Вы можете использовать следующие критерии фильтрации:
   - **Тип**. Выберите тип объектов, которые будут отображаться (компьютеры, виртуальные машины, папки).



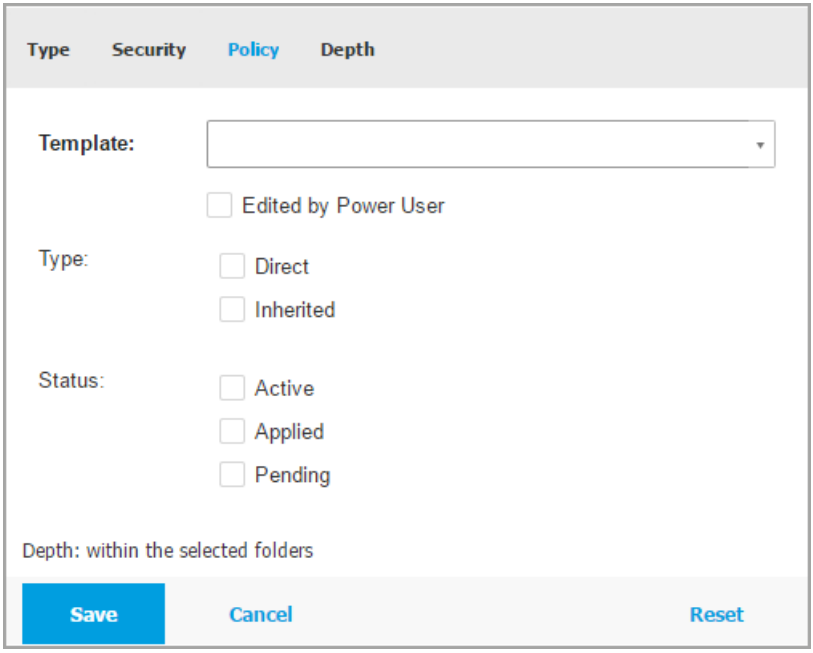
Конечные точки - Фильтрация по Типу

   - **Безопасность**. Выберите отображение конечных точек по управлению защитой, состоянию безопасности и ожиданию.



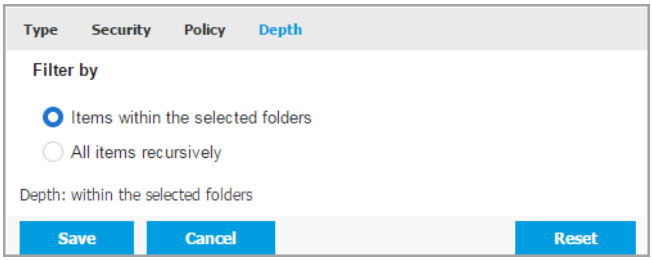
Конечные точки - Фильтрация по Безопасности

- **Политика**. Выберите шаблон политики, для которого нужно фильтровать конечные точки, тип назначения политики (прямой или наследуемый), а также статус назначения политики (активный, применяемый или в ожидании). Вы также можете выбрать для отображения объекты только с политиками, отредактированными привилегированными пользователями.



Конечные точки - Фильтрация по Политикам

- **Глубина**. При управлении древовидной структурой сети, конечные точки размещенные в подгруппах, не отображаются при выборе корневой группы. Выберите **All items recursively**, чтобы просмотреть все конечные точки, входящие в текущую группу и все ее подгруппы.



Конечные точки - Фильтрация по Глубине

При выборе рекурсивного просмотра всех элементов Control Center отображает их в виде простого списка. Чтобы найти местоположение элемента, выберите интересующий вас элемент и нажмите **Перейдите в контейнер** в верхней части таблицы. Вы будете перенаправлены в вышестоящий контейнер выбранного элемента.

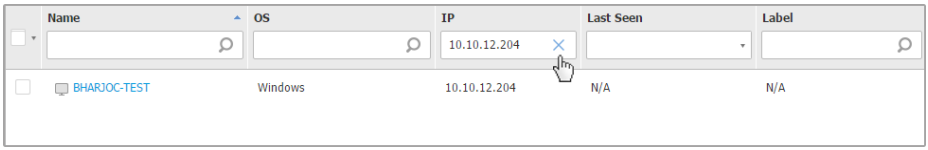
Примечание
Вы можете просмотреть все выбранные критерии фильтрации в нижней части окна **Filters**.
Если вы хотите очистить все фильтры, нажмите кнопку **сбросить**.

4. Нажмите **Save**, чтобы отфильтровать конечные точки по выбранным критериям. Фильтр в разделе **Сеть** остается активным, пока вы не выйдите из раздела или не сбросите фильтр.

6.4.3. Поиск Конечных точек

1. Выберите нужную группу в левой панели.
2. Введите слово для поиска в соответствующем поле под заголовками столбцов в правой панели. Например, введите IP-адрес конечной точки в поле **IP**, которую вы ищете. Только соответствующая конечная точка появится в таблице.

   Очистите окно поиска, чтобы отобразить полный список конечных точек.



Поиск конечных точек

6.5. Инвентаризация патча

GravityZone выясняет, какие патчи требуются вашему ПО посредством задачи **Сканирование патчей** и затем добавляет их в инвентарь.

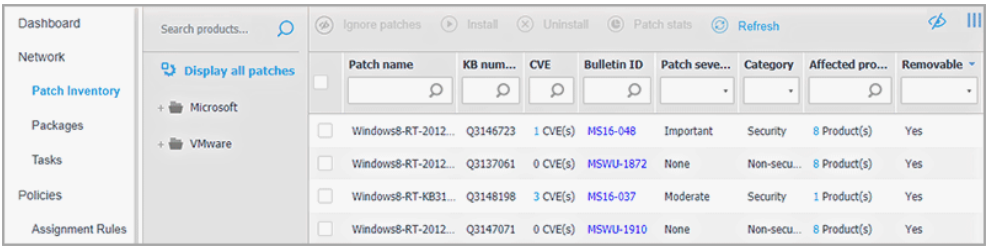
Страница **Patch Inventory** отображает все обнаруженные патчи для ПО, установленные в конечных точках и предлагает несколько действий, которые вы можете предпринять с этими патчами.

Используйте Patch Inventory когда вам это необходимо, чтобы сразу же развернуть определенные патчи. Эта альтернатива позволяет вам легко решать некоторые проблемы, о которые вам известно Например, вы прочитали статью об уязвимости ПО и вы знаете CVE ID. Вы можете найти инвентарь для патчей, подходящий CVE и затем посмотреть, какая конечная точка нуждается в обновлении.

Чтобы перейти в Patch Inventory, выберите опцию **Сеть > Patch Inventory** в основном меню Control Center.

Страница организована в двух панелях:

- Панель слева отображает продукты ПО, установленные в вашей сети, сгруппированные продавцом.
- Панель справа отображает таблицу доступных патчей и информацию о них.



Инвентаризация патча

Далее вы узнаете, как использовать инвентарь. Вы можете выполнить следующие задачи:

- См. детали патчей
- Искать и фильтровать патчи
- Игнорировать патчи
- Устанавливать патчи
- Удалять патчи
- Создавать статистику о патчах

6.5.1. Получение сведений о патчах

Таблица патчей дает информацию, которая помогает вам идентифицировать патчи, оценить их важность, просмотреть статус их установки и объем. Детали описаны здесь:

- **Имя патча.** Это имя запускаемого файла, содержащего патч.
- **KB номер.** Этот номер идентифицирует статью KB, в которой есть информация об освобождении патча.
- **CVE.** Это номер CVE, на которые ссылается патч. Нажимая на номер, вы увидите список CVE IDs.
- **ID бюллетени** Это ID бюллетеня по безопасности, выпускаемый продавцом. Этот ID связан с актуальной статьей, которая описывает патч и дает детали установки.
- **Важность патча.** Этот рейтинг информирует вас о важности патча в отношении ущерба, который он предотвращает.

- **Категория.** В зависимости от типа проблем, которые они решают, патчи группируются на: патчи безопасности и иные. Это поле информирует вас о том, в какой категории находится патч.
- **Затронутые продукты.** Это количество продуктов, для которых выпущен патч. Количество связано со списком этих продуктов ПО.
- **Удаляемые.** Если вам нужно откатить какой-либо патч, вы должны сначала убедиться в том, что его можно удалить. Используйте этот фильтр, чтобы узнать, какие патчи можно удалить (откатить). Для большей информации обратитесь к Uninstall patches.

Чтобы настроить детали, отображенные в таблице:

1. Нажмите кнопку **Колонки** справа от Панель действий
2. Выберите столбцы, которые вы хотите отобразить.
3. Нажмите кнопку **Восстановить**, чтобы вернуться к виду столбцов по умолчанию.

Пока вы находитесь на странице, процессы GravityZone, протекающие фоном, могут повлиять на базы данных. Убедитесь, что вы просматриваете последнюю информацию в таблице, нажимая кнопку **Обновить** в верхней части таблицы.

GravityZone просматривает список доступных исправлений и удаляет те, которые больше не применяются в связи с тем, что связанных приложений или конечных точек больше не существует.

GravityZone также ежедневно просматривает и удаляет патчи, недоступные в списке, хотя они могут присутствовать на некоторых конечных точках.

6.5.2. Поиск и фильтрация патчей

По умолчанию Control Center отображает все доступные исправления для вашего программного обеспечения. GravityZone предоставляет вам несколько вариантов быстрого поиска нужных вам исправлений.

Фильтрация патчей по продукту

1. Расположите продукт в левой панели.

   Это можно сделать, прокрутив список, чтобы найти его поставщика, или введя его имя в поле поиска в верхней части панели.

2. Нажмите на имя поставщика, чтобы развернуть список и просмотреть его продукты.
3. Выберите продукт, чтобы просмотреть доступные исправления, или отмените выбор, чтобы скрыть его исправления.
4. Повторите предыдущие шаги с другими интересующими вас продуктами.

Если вы хотите снова просмотреть исправления для всех продуктов, нажмите кнопку **Показать все исправления** в верхней части левой панели.

Фильтрация патчей по утилите

Исправление становится ненужным, если, например, оно само или более новая версия уже развернуты в конечной точке. Поскольку инвентарь может в какой-то момент содержать такие патчи, GravityZone позволяет вам их игнорировать. Выберите эти исправления, а затем нажмите кнопку **Игнорировать исправления** в верхней части таблицы.

Control Center отображает пропущенные патчи в другом виде. Нажмите кнопку **Управляемый / Пропущенный** справа от Панели инструментов действий, чтобы переключаться между представлениями:

- - чтобы увидеть пропущенные исправления.
- - чтобы увидеть управляемые исправления.

Фильтрация исправлений по деталям

Используйте возможности поиска для фильтрации исправлений по определенным критериям или после известных деталей. Введите условия поиска в поля поиска в верхней части таблицы исправлений. Совпадающие исправления отображаются в таблице по мере ввода или после выбора.

Очистка поля поиска сбрасывает поиск.

6.5.3. Игнорирование исправлений

Возможно, вам придется исключить некоторые исправления из инвентаря исправлений, если вы не планируете устанавливать их на свои конечные точки, с помощью команды **Игнорировать исправления**.

Игнорируемое исправление будет исключено из задач автоматического исправления и отчетов о исправлении и не будет считаться отсутствующим исправлением.

Чтобы игнорировать исправление:

1. НА странице **Инвентарь исправлений** выберите одно или несколько исправлений, которые вы хотите игнорировать.
2. Нажмите кнопку **Игнорировать патчи** в верхней части таблицы.

   Появится окно конфигурации, где вы можете просмотреть сведения о выбранных исправлениях, а также любые подчиненные исправления.
3. Нажмите **Игнорировать**. Исправление будет удалено из списка инвентаря исправлений.

Вы можете найти пропущенные исправления в отдельном формате и выполнить действия над ними:

- Нажмите кнопку **Показать пропущенные исправления** в правой верхней части таблицы. Вы увидите список всех пропущенных исправлений.
- Вы можете получить больше информации об отдельном пропущенном исправлении, сгенерировав статистический отчет исправлений. Выберите нужное вам исправление и нажмите кнопку **Статистика исправлений** в верхней части таблицы. Дополнительные сведения см. в разделе «Создание статистики исправлений» (p. 79)
- Чтобы восстановить пропущенные исправления, выберите их и нажмите кнопку **Восстановить исправления** в верхней части таблицы.

  Появится окно конфигурации, где вы можете просмотреть подробную информацию о выбранных исправлениях.

  Нажмите кнопку **Восстановить** чтобы отправить исправление в инвентарь.

6.5.4. Установка патчей

Чтобы установить исправления из инвентаря:

1. Перейдите в раздел **Сеть> Инвентарь исправлений**.
2. Найдите исправления, которые вы хотите установить. Если необходимо, отфильтруйте их для быстрого поиска
3. Выберите исправления и нажмите кнопку **Установить** в верхней части таблицы. Появится окно конфигурации, где вы можете редактировать детали установки исправления.

   Вы увидите выбранные исправления вместе с любыми подчиненными исправлениями.

- Выберите целевую группу конечных точек.
- **При необходимости перезагрузите конечные точки после установки патча**. Эта опция перезапустит конечные точки сразу после установки исправлений, если потребуется перезагрузка системы. Учтите, что это действие может прервать сеанс пользователя.

  Если этот параметр отключен, это означает, что, если требуется перезагрузка системы на целевых конечных точках, они будут отображать значок состояния ожидающего перезапуска в сетевой инвентаризации GravityZone. В этом случае вам доступны следующие варианты:

  – Отправить задачу **Перезагрузить компьютер** ожидающим конечным точкам перезапуска в любое время по вашему выбору. Дополнительные сведения см. в разделе «Перезагрузка машины» (p. 113).

  – Настроить активную политику, чтобы уведомить пользователя конечной точки о необходимости перезагрузки. Для этого перейдите к активной политике на целевой конечной точке, перейдите в раздел **Общие > Уведомления** и включите параметр **Уведомление о перезапуске конечной точки**. В этом случае пользователь будет получать всплывающее окно каждый раз, когда требуется перезапуск из-за изменений, внесенных указанными компонентами GravityZone (в данном случае, Управление исправлениями). Всплывающее окно предоставляет возможность отложить перезагрузку. Если пользователь выбирает отложить, то уведомления перезагрузки будут периодически появляться на экране до тех пор пока пользователь не перезагрузит систему, или пока не истечет назначенное администратором компании время.

    Дополнительные сведения см. в разделе «Уведомление о перезапуске конечной точки» (p. 153).

4. Щелкните **Установить**.

   Задача установки создается вместе с подзадачами для каждой целевой конечной точки.

Примечание

- Вы также можете установить исправление со страницы **Сеть**, начиная с определенных конечных точек, которыми вы хотите управлять. В этом

случае выберите конечные точки из инвентаризации сети, нажмите **Задачи** нажмите в верхней части таблицы и выберите **Установка исправлений**. Для получения более подробной информации, обратитесь к «Установка патча» (p. 97).

- После установки исправления мы рекомендуем отправить задачу Сканировать исправления конечным точкам. Это действие обновит информацию об исправлении, сохраненную в GravityZone для ваших управляемых сетей.

6.5.5. Удаление патчей

Возможно, вам придется удалить исправления, которые вызвали сбои в работе конечных точек. GravityZone предоставляет функцию отката для исправлений, установленных в вашей сети, которая восстанавливает программное обеспечение до его предыдущего состояния перед применением исправления.

Функция удаления доступна только для сменных исправлений. Инвентаризация исправлений GravityZone включает в себя столбец **Удаляемые**, где вы можете фильтровать исправления по степени их удаляемости.

Примечание
Атрибут съемности зависит от того, каким образом исправление было выпущено производителем или от изменений, внесенных исправлением в программное обеспечение. Для исправлений, которые невозможно удалить, вам может понадобиться переустановить ПО.

Чтобы удалить исправление:

1. Перейдите в раздел **Сеть> Инвентарь исправлений**.
2. Выберите исправление, которое вы хотите удалить. Для поиска определенного исправления используйте фильтры, доступные в столбцах, например номер КБ или CVE. Используйте колонку **Удаляемые** чтобы отобразить только те исправления, которые можно удалить.

Примечание
Вы можете удалить одновременно только одно исправление для одной конечной точки или нескольких сразу.

3. Нажмите кнопку ⊗ **Удалить** в верхней части таблицы. Появится окно конфигурации, в котором вы можете редактировать детали задачи удаления.

   - **Название задачи:**. Вы можете изменить имя по умолчанию для задачи удаления исправления, если хотите. Таким образом, вы легче определите задачу на странице **Задачи** .
   - **Добавить патч в список пропущенных патчей**. Обычно вам больше не понадобится исправление, которое вы хотите удалить. Этот параметр автоматически добавляет исправление в список игнорируемых после удаления исправления.
   - **При необходимости перезагрузите конечные точки после удаления патча**. Эта опция перезапустит конечные точки сразу после удаления исправления, если потребуется перезагрузка системы. Учтите, что это действие может прервать сеанс пользователя.

     Если этот параметр отключен, это означает, что, если требуется перезагрузка системы на целевых конечных точках, они будут отображать значок состояния ожидающего перезапуска в сетевой инвентаризации GravityZone. В этом случае вам доступны следующие варианты:

     – Отправить задачу **Перезагрузить компьютер** ожидающим конечным точкам перезапуска в любое время по вашему выбору. Дополнительные сведения см. в разделе «Перезагрузка машины» (p. 113).

     – Настроить активную политику, чтобы уведомить пользователя конечной точки о необходимости перезагрузки. Для этого перейдите к активной политике на целевой конечной точке, перейдите в раздел **Общие > Уведомления** и включите параметр **Уведомление о перезапуске конечной точки**. В этом случае пользователь будет получать всплывающее окно каждый раз, когда требуется перезапуск из-за изменений, внесенных указанными компонентами GravityZone (в данном случае, Управление исправлениями). Всплывающее окно предоставляет возможность отложить перезагрузку. Если пользователь выбирает отложить, то уведомления перезагрузки будут периодически появляться на экране до тех пор пока пользователь не перезагрузит систему, или пока не истечет назначенное администратором компании время.

Дополнительные сведения см. в разделе «Уведомление о перезапуске конечной точки» (p. 153).

- В таблице **Цели отката** выберите конечные точки, на которых вы хотите удалить исправление.

  Вы можете выбрать одну или несколько конечных точек в вашей сети. Используйте доступные фильтры, чтобы найти конечную точку, которую вы хотите.

  Примечание
  В таблице отображаются только те конечные точки, где установлено выбранное исправление.

4. Нажмите **Подтвердить**. Задача **Удаление исправлений** будет создана и отправлена на целевые конечные точки.

   Отчет **Удаление исправления** автоматически создается для каждой завершенной задачи удаления исправления, предоставляя сведения об исправлении, конечных точках назначения и состоянии задачи удаления исправления.

Примечание
После удаления исправления мы рекомендуем отправлять на целевые конечные точки задачу Сканировать исправления. Это действие обновит информацию об исправлении, сохраненную в GravityZone для ваших управляемых сетей.

6.5.6. Создание статистики исправлений

Если вам нужны подробности о состоянии определенного исправления для всех конечных точек, используйте функцию **Статистика исправлений**, которая генерирует мгновенный отчет для выбранного исправления:

1. На странице **Инвентарь исправления** выберите нужное вам исправление из правой панели.
2. Нажмите кнопку **Статистика исправлений** в верхней части таблицы.

   Отображается отчет о статистике исправлений, предоставляющий различные сведения о состоянии исправлений, в том числе:

   - Круговая диаграмма, показывающая процентное соотношение установленного, неудачного, отсутствующего и ожидающего состояния исправления для конечных точек, сообщивших о исправлении.

- Таблица, отражающая следующую информацию:
  - **Имя**, **полное доменное имя**, **IP** и **ОС** каждой конечной точки, которая сообщила об исправлении.
  - **Последняя проверка**: время, когда исправление проверялось последний раз на конечной точке.
  - **Статус исправления**: установлен, не выполнен, отсутствует или игнорируется.

Примечание
Функциональность статистики исправлений доступна как для управляемых, так и для игнорируемых исправлений.

6.6. Запущенные Задачи

На странице **Network** вы можете удаленно запускать ряд администраторских задач на конечных точках.

Вы можете выполнить следующие задачи:

- «СКАНИРОВАТЬ» (p. 81)
- «Сканирование на наличие IOC» (p. 92)
- «Сканирование рисков» (p. 95)
- «Задачи патчей» (p. 96)
- «Сканирование Exchange» (p. 99)
- «Установить» (p. 103)
- «Удаление клиента» (p. 109)
- «Обновление клиента» (p. 110)
- «Перенастройка клиента» (p. 111)
- «Обслуживание клиента» (p. 113)
- «Перезагрузка машины» (p. 113)
- «Сетевое Обнаружение» (p. 114)
- «Обновление Security Server» (p. 115)

Вы можете создавать задачи отдельно для каждой конечной точки или для групп конечных точек. Например, вы можете удаленно установить агент безопасности группе неуправляемых конечных точек. Позже вы можете создать задачу сканирования для определенной конечной точки в этой группе.

Для каждой конечной точки вы можете запускать только совместимые задачи. Например, если вы выберите неуправляемую конечную точку, то вы

можете выбрать только установку агента безопасности, все другие задачи будут недоступны.

Задача, выбранная для группы, будет создана только для совместимых конечных точек. Если ни одна из конечных точек в группе не совместима с выбранной задачей, вы будете уведомлены, что задача не может быть создана.

После создания задача будет запущена незамедлительно на конечных точках, находящихся он-лайн. Если конечная точка находится в автономном режиме (офф-лайн), задача начнет выполняться, как только она подключится к сети.

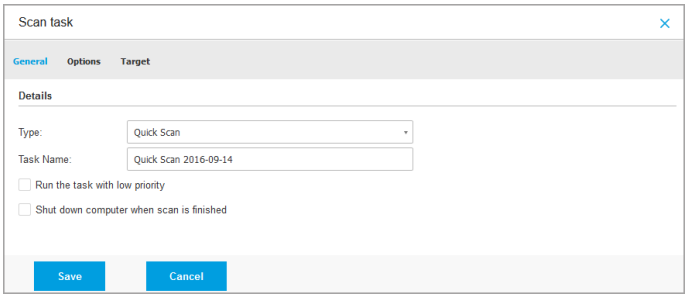
Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к Просмотр и управление задачами.

6.6.1. СКАНИРОВАТЬ

Для удаленного запуска задачи сканирования на одной или нескольких конечных точках:

1. Перейдите в раздел **Сеть**.
2. Выберите желаемый контейнер в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.
3. Отметьте флажками конечные точки или группы, которые вы хотите просканировать.
4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Сканировать**.

   Появится окно настроек.
5. Настройте параметры сканирования:
   - На вкладке **Общее** вы можете выбрать тип сканирования и ввести имя для задачи проверки. Название задачи сканирования предназначено для более простой идентификации соответствующей задачи на странице **Задачи**.



Задача сканирования - Настройка общих параметров

Выберите тип сканирования из меню **Тип**:

- **Быстрое сканирование** использует облачное сканирование для обнаружения вредоносных программ, запущенных в системе. Данный тип сканирования предварительно настроен, чтобы сканировать только критические системные области Windows и Linux. Быстрое сканирование занимает, как правило, менее минуты. Быстрое сканирование использует лишь незначительную часть системных ресурсов, в отличие от процесса стандартного антивирусного сканирования.

  Bitdefender автоматически переходит к обезвреживанию, если обнаружены вредоносные программы или руткиты. Если по какой-либо причине файл нельзя вылечить, он перемещается в карантин. Этот тип сканирования игнорирует подозрительные файлы.

- **Полное сканирование** проверяет всю систему на все типы вредоносных программ, угрожающих безопасности, таких как вирусы, программы-шпионы, рекламное ПО, руткиты и другие.

  Bitdefender автоматически пытается обезвреживать файлы, обнаруженные вредоносными программами. Если вредоносная программа не может быть удалена, она перемещвется в карантин, где она не может навредить. Подозрительные файлы игнорируются. Если вы хотите принять меры и в отношении подозрительных файлов, или если вы хотите выполнить другие действия по умолчанию для зараженных файлов, выберите вариант «Запуск пользовательского сканирования».

- **Memory Scan** проверяет программы, запущенные в памяти конечных точек.
- **Сканирование сети** тип пользовательского сканирования, позволяющий сканировать сетевые диски, используя агента безопасности Bitdefender, установленного на выбранной конечной точке.

  Для выполнения задачи сетевого сканирования:

  - Вам необходимо назначить задачу для одной конечной точки в сети.
  - Для агента безопасности вам необходимо ввести учетные данные пользователя с правами чтения/записи для выбранных сетевых дисков, чтобы иметь возможность получить доступ и выполнить требуемые действия на этих сетевых дисках. Необходимые учетные данные могут быть сконфигурированы на вкладке **Цель** окна задач.
- **Выборочное сканирование** позволяет выбирать места сканирования и настраивать параметры сканирования.

Для выборочного сканирования, сканирования памяти и сети, вы можете выбрать следующие опции:

- **Выполнить задачу с низким приоритетом**. Установите этот флажок для снижения приоритета процесса сканирования, чтобы другие программы смогли работать быстрее. При это может увеличится время, необходимое для завершения процесса сканирования.

  Примечание
  Эта опция применима только к Bitdefender Endpoint Security Tools и Endpoint Security (устаревший агент)

- **Выключить компьютер после завершения сканирования** Установите этот флажок, чтобы выключить машину, если вы не собираетесь использовать ее некоторое время.

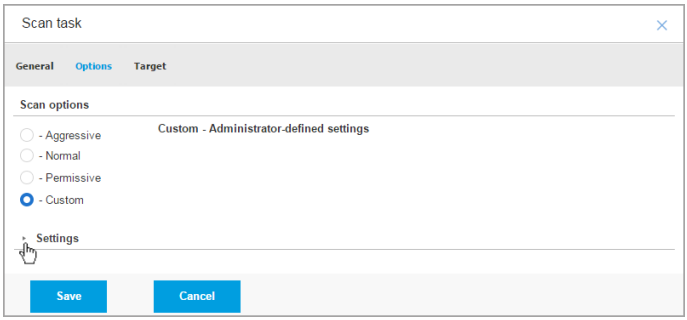
  Примечание
  Эта опция применима к Bitdefender Endpoint Security Tools, Endpoint Security (устаревший агент) и Endpoint Security for Mac.

Примечание
Только два варианта применимы к Bitdefender Endpoint Security Tools и Endpoint Security (устаревший агент).

Для пользовательского сканирования (Custom Scan) настройте следующие параметры:

– Перейдите на вкладку **Опции**, чтобы установить параметры сканирования. Выберите уровень безопасности, который лучше всего соответствует вашим потребностям (Интенсивный, Нормальный или Рекомендуемый). Используйте описания справа от шкалы, которые помогут сделать выбор.

  В зависимости от выбранного профиля, параметры сканирования в разделе **Настройки** будут сконфигурированы автоматически. Тем не менее, при желании, вы можете настроить их более детально. Чтобы сделать это, отметьте чек-бокс **Пользователь** и затем раскройте раздел **Настройки**.



Задача сканирования - Настройка пользовательского режима

Доступны следующие опции:

- **Типы файлов.** Используйте данную настройку, чтобы задать типы файлов, которые вы хотите просканировать. Вы можете указать агенту безопасности просканировать все файлы (независимо от их расширений), только файлы приложений или специфические типы файлов, которые вы считаете потенциально опасными. При сканировании всех файлов обеспечивается

оптимальная защита. Сканируя только приложения, можно повысить скорость сканирования.

Примечание

Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов. Для получения более подробной информации, обратитесь к «Типы файлов приложений» (p. 509).

Если вы хотите просканировать только специфические типы файлов, выберите в меню **Пользовательские расширения** и затем введите желаемые расширения в редактируемом поле, нажимая `войти` после каждого расширения.

Важно

Агенты безопасности Bitdefender устанавливаются в операционных системах Windows и Linux, сканируют большинство .ISO форматов, но не предпринимают никаких действий над ними.

Настройка задач сканирования - Добавление пользовательских расширений

- **Архивы.** Архивы, содержащие инфицированные файлы, не представляют непосредственной угрозы безопасности системы. Вредоносные программы могут повлиять на систему только если зараженный файл извлечен из архива и будет исполнен при выключенной защите в реальном времени. Тем не менее, рекомендуется сканировать архивы для обнаружения и удаления любой потенциальной угрозы, даже не представляющей собой непосредственной угрозы системе.

Важно
Сканирование файлов, сжатых в архив, увеличивает общее время сканирования и занимает больший объем системных ресурсов.

– **Сканирование внутри архивов.** Выберите эту опцию, если вы хотите проверить заархивированные файлы на наличие вредоносных программ. Если вы решили использовать данную опцию, вам необходимо настроить следующие параметры оптимизации:

  - **Ограничение размера архива (Мб).** Вы можете установить максимально допустимый размер архивов для сканирования. Поставьте флажок в соответствующем поле и введите максимальный размер архива (в МБ).
  - **Максимальная глубина архива (уровни).** Отметьте соответствующий флажок и выберите в меню максимальную глубину архива. Для лучшей производительности выберите наименьшее значение, для максимальной защиты выберите наибольшее значение.

– **Сканировать архивы электронной почты.** Выберите данную опцию если хотите разрешить проверку почтовых сообщений и почтовых баз, включая такие форматы файлов как .eml, .msg, .pst, .dbx, .mbx, .tbb и другие.

Важно
Процесс сканирования почтовых архивов является достаточно ресурсоемким и может повлиять на производительность системы.

- **Разное.** Выберите соответствующие флажки, чтобы включить нужные параметры сканирования.

  – **Сканирование загрузочных секторов.** Проверка загрузочных секторов системы. Этот сектор жесткого диска содержит компьютерный код, необходимый для запуска процесса загрузки. Заражение вирусом загрузочного сектора может привести к тому, что диск станет недоступен и вы не сможете загрузить систему и получить доступ к своим данным.

- **Сканирование реестра.** Выберите этот параметр для сканирования ключей реестра. Реестр Windows — это база данных, в которой хранятся настройки и параметры конфигурации для компонентов операционной системы Windows и установленных приложений.
- **Сканирование на наличие руткитов.** Выберите этот параметр для сканирования на наличие руткитов и объектов, скрытых с помощью такого программного обеспечения.
- **Сканирование на наличие клавиатурных шпионов.** Выберите данную опцию для сканирования системы на наличие клавиатурных шпионов.
- **Сканировать общие сетевые ресурсы.** Эта опция сканирует подключенные сетевые диски.

  Для быстрого сканирования эта опция отключена по умолчанию. Для полного сканирования опция активирована по умолчанию. Для сканирования по выбору пользователя, если вы установите уровень безопасности **Интенсивный/Нормальный**, параметр **Сканирование общих сетевых ресурсов** включается автоматически. Если вы установите уровень безопасности **Рекомендуемый**, параметр **Сканирование общих сетевых ресурсов** автоматически отключается.
- **Сканирование памяти.** Выберите этот параметр для сканирования программ, запущенных в системной памяти.
- **Сканирование файлов cookie.** Выберите эту опцию для сканирования cookies-файлов, сохраненных браузерами на компьютере.
- **Сканирование только новых/измененных файлов.** Сканируя только новые и измененные файлы, можно значительно повысить общее быстродействие системы с минимальными потерями в безопасности.
- **Сканирование на наличие потенциально нежелательных приложений (PUA).** Потенциально нежелательные приложения (PUA) это программы, которые могут быть нежелательными для ПК, а иногда и поставляться в комплекте с программным

обеспечением бесплатного. Такие программы могут быть установлены без согласия (также называются рекламными) или включены по умолчанию в комплект экспресс-установки (как дополнение). Потенциальное воздействие этих программ заключается в показе всплывающих окон, установке нежелательных панелей инструментов в браузере по умолчанию или работе нескольких процессов в фоновом режиме, что замедляет производительность компьютера.

- **Сканирование съемных носителей.** Выберите этот параметр для сканирования любых съемных накопителей, подключаемых к конечной точке.

- **Действия.** В зависимости от типа обнаруженного файла автоматически выполняются следующие действия:

  - **Действие при обнаружении зараженного файла.** Bitdefender определяет файлы как зараженные с помощью различных передовых механизмов, которые включают сигнатуры вредоносного ПО, технологии машинного обучения и искусственного интеллекта (ИИ). Агент безопасности Bitdefender может удалить вредоносный код из зараженного файла и воссоздать исходный файл. Эта операция известна как лечение.

    По умолчанию, если зараженный файл обнаружен, агент безопасности Bitdefender автоматически попытается вылечить его. Если файл не удается вылечить, он перемещается в карантин в целях предотвращения распространения вируса.

    Важно
    В случае определенных типов вредоносных программ лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. В таких случаях выполняется удаление зараженного файла с диска.

  - **Действие при обнаружении подозрительного файла.** Для обнаружения подозрительных файлов Bitdefender использует Эвристический анализ и другие технологии . Такой подход обеспечивает высокий уровень обнаружения, но в некоторых

случаях пользователь должен знать о случаях ложных сигналов (чистые файлы, определенные как подозрительные). Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.

По умолчанию, задачи сканирования настроены игнорировать подозрительные файлы. Вы можете изменить действие по умолчанию, чтобы перемещать подозрительные файлы в карантин. Помещенные в карантин файлы отправляются на анализ в лабораторию Bitdefender на регулярной основе. Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит его удалить.

– **Когда найден руткит.** Руткиты представляют собой специализированное программное обеспечение, используемое для того, чтобы скрыть файлы операционной системы. Однако, руткиты часто используются, чтобы скрыть вредоносные программы, либо для сокрытия присутствия злоумышленника в системе.

  Обнаруженные руткиты и скрытые файлы по умолчанию игнорируются.

Хотя это и не рекомендуется, вы можете изменить действие по умолчанию. Можно задать дополнительное действие, которое будет выполнено в случае, если не удалось выполнить первое, а также различные действия для каждой из категорий. Выберите в соответствующих меню первое и второе действие, которые будут выполняться в отношении всех типов обнаруженных файлов. Доступны следующие действия:

Лечить

Удаляет вредоносный код из зараженных файлов. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов.

Перемещение файлов в карантин

Перемещает зараженные файлы из исходного расположения в папку карантина. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице консоли Quarantine.

Удалить
Удаляет обнаруженные файлы с диска без предупреждения. Желательно избегать использование этого действия.

Пропустить
Никаких действий не будет предпринято в отношении обнаруженных файлов. Эти файлы будут отображаться только в журнале сканирования.

– Перейдите на вкладку **Target**, чтобы настроить объекты, которые вы хотите просканировать на конечных точках.

В разделе **Сканирование цели** вы можете добавить новый файл или папку, которые необходимо проверить:

a. Выберите предопределенное месторасположение из выпадающего меню или введите конкретные пути в **конкретные пути**, которые вы хотите просканировать.

b. Укажите путь к объекту для сканирования в поле редактирования.

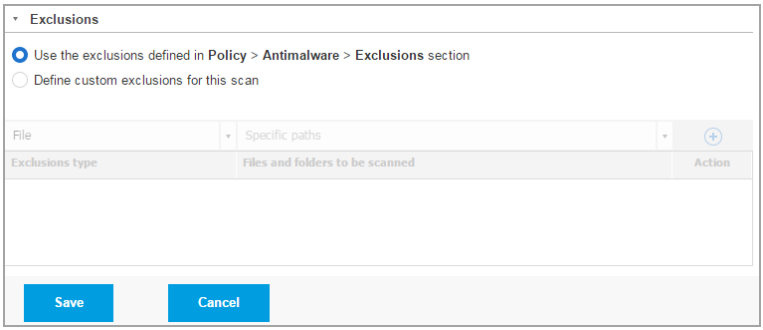
- Если вы выбрали предопределенное место, необходимо корректно завершить путь. Например, для сканирования всей папки `Программные файлы`, достаточно выбрать соответствующее предопределенное место из выпадающего меню. Для сканирования конкретной папки из `Программные файлы`, необходимо завершить путь, добавив обратную косую черту (\) и имя папки.
- Если вы выбрали **Конкретные пути**, введите полный путь к объекту проверки. Желательно использовать системные переменные (в соответствующих случаях), чтобы быть уверенным, что путь действителен для всех нужных компьютеров. Для получения более подробной информации о системных переменных, обратитесь к «Системные переменные» (p. 511).

c. Нажмите соответствующую кнопку ⊕ **Добавить**.

Чтобы изменить существующий путь, нажмите на него. Чтобы удалить папку из списка, нажмите соответствующую кнопку ⊗ **Удалить**.

Для агента безопасности вам необходимо ввести учетные данные пользователя с правами чтения/записи для выбранных сетевых дисков, чтобы иметь возможность получить доступ и выполнить требуемые действия на этих сетевых дисках.

Нажмите на раздел **Исключения**, если вы хотите добавить исключения.



Задача сканирования - Настройка Исключений

Вы можете либо использовать исключения определенные политикой, либо определить явные исключения для текущей задачи сканирования. За более подробной информацией об исключениях, обратитесь к «Исключения» (p. 198).

6. Нажмите **Сохранить**, чтобы создать задачу сканирования. Появится окно подтверждения.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к Просмотр и управление задачами.

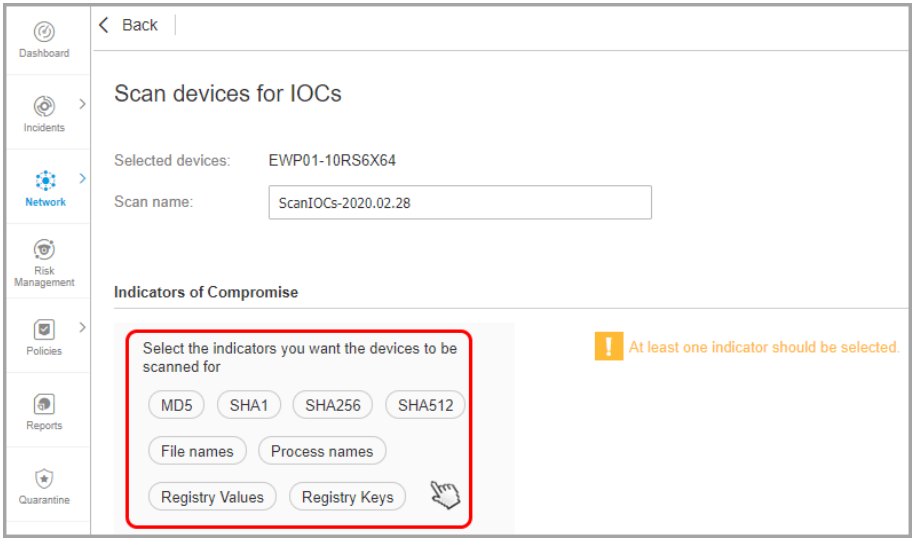
Примечание
Чтобы запланировать задачу сканирования, перейдите на страницу **Политики**, выберите политику, которая будет назначена требуемым компьютерам и добавьте задачу проверки в разделе **Защита от вредоносных программ > По требовнию**. Для получения более подробной информации, обратитесь к «Сканирование по запросу (On-Demand)» (p. 178).

6.6.2. Сканирование на наличие IOC

Вы можете в любое время выбрать запуск сканирования по требованию для известных индикаторов компрометации (IOC) на выбранных конечных точках следующим образом:

1. Перейдите в раздел **Сеть**.
2. Просмотрите контейнеры и выберите конечные точки, которые вы хотите сканировать.
3. Нажмите кнопку **Задачи** и выберите **Сканирование на наличие IOC**.

   Появится окно с настройками, в котором вы сможете выбрать необходимые индикаторы для проверки во время сканирования индикаторов компрометации.



Настроить задачу сканирования на наличие IOC

Примечание
Вы должны выбрать хотя бы один тип индикатора компрометации, чтобы создать правильную задачу.

4. Выберите один или несколько типов индикаторов компроментации (IOC), которые вы хотите учитывать при сканировании, и введите известное имя IOC в новое добавленное поле.

Добавить индикаторы компроментации

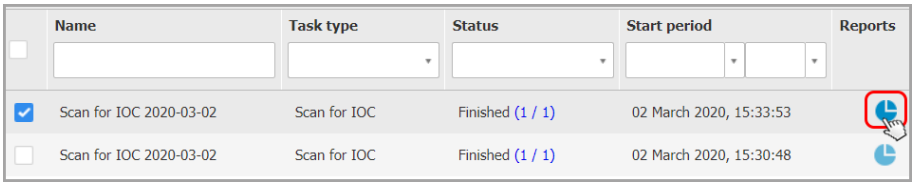
Вы можете выбрать из следующих типов:

- MD5
- Алгоритм криптографического хеширования
- SHA256
- Алгоритм хеширования, который является функцией криптографического алгоритма SHA-2
- Имена файла
- Имена процессов
- Значения реестра
- Ключи системного реестра

Примечание
Содержимое, добавленное в каждое поле, должно быть действительным. В противном случае появятся предупреждение и сообщение.

5. Нажмите **Сохранить**, чтобы создать и запустить задачу **Сканировать на наличие IOC**. Появится окно подтверждения.

   Вы можете проверить ход выполнения задачи на странице **Сеть/Задачи**.



Прогресс задачи

6. После успешного завершения задачи вы можете нажать кнопку **Отчеты**, чтобы прочитать сгенерированный отчет и определить успешность Сканирования на IOC.

Допустимые расширения файлов для IOC, добавленные в задачу, включают: `exe`, `dll`, `com`, `scr`, `jar`, `msi`, `msc`, `bat`, `ps1`, `vbs`, `vbe`, `js`, `jse`, `wsf`, `wsh`, `psc1`, `lnk`, `doc`, `docx`, `docm`, `xls`, `xlsx`, `xlsm`, `ppt`, `pptx`, `pptm`, `eml`, `rtf`, `pdf`, `html`, `ppsx`, `pps`, `ppsm`, `pot`, `potx`, `potm`, `ocx`, `sys`, `fnr`, `fne`, and `pif`.

Задача **Сканировать на IOC** будет сканировать следующие местоположения:

- `%Windows%\System32\Drivers`
- `%Windows%\System32\WindowsPowerShell\v1.0`
- `%Windows%\system32\config\systemprofile\AppData`
- `%Windows%\System32\Tasks`
- `%Windows%\System32\wbem`
- `%Windows%\SysWOW64\WindowsPowerShell\v1.0`
- `%Windows%\SysWOW64\config\systemprofile\AppData`
- `%Windows%\SysWOW64\sysprep`
- `%Windows%\Scripts`
- `%Windows%\System`
- `%Windows%\Web`
- `%Users%`

Важно
Задачи **Сканирование на IOC** не будут запускаться/не будут выполняться на конечных точках в следующих ситуациях:

- На конечной точке нет операционной системы Windows.
- Лицензия агента конечной точки Bitdefender недействительна.
- Модуль **EDR** не установлен в BEST-клиенте, установленном на целевых конечных точках.
- В настоящее время в очереди более 100 задач **Сканирование на IOC**.
- Недопустимые данные вводятся пользователем на странице конфигурации задачи **Сканировать на IOC**.

6.6.3. Сканирование рисков

Вы можете в любое время запустить задачи сканирования рисков по требованию на выбранных конечных точках, выполнив следующие действия:

1. Перейдите в раздел **Сеть**.
2. Просмотрите контейнеры в левой части экрана и выберите конченые точки, которые вы хотите сканировать.
3. Нажмите кнопку **Задачи** и выберите **Сканирование на наличие рисков**.

   Будет появляться сообщение с требованием подтверждения запуска сканирования на наличие рисков.

   Примечание
   Сканирование на наличие рисков будет запущено при всех показателях, которые активируются по умолчанию.

4. После успешного завершения операции Вы можете перейти на вкладкуНеправильная настройка страницы **Рисков безопасности**, проанализировав их, и выбрать показатели, которые следует проигнорировать.

   Оценка всех рисков компании будет пересмотрена в связи с оставленными без внимания индикаторами риска.

   Примечание
   Чтобы просмотреть полный список индикаторов и их описание, см. эту статью Базы Знаний.

Важно
Задачи **Сканирование рисков** не запустятся/не будут выполняться на конечных точках в следующих ситуациях:

- На конечной точке нет операционной системы Windows.
- Лицензия агента конечной точки Bitdefender недействительна.
- Политика, примененная к конечной точке, отключила Модуль управления рисками.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к Просмотр и управление задачами.

6.6.4. Задачи патчей

Рекомендуется регулярно проверять обновления ПО и применять их как можно скорее. GravityZone автоматизирует этот процесс с помощью политик безопасности, но если вам нужно обновить программное обеспечение сразу на определенных конечных точках, выполните следующие задачи в следующем порядке:

1. Сканирование патча
2. Установка патча

Требования к системе

- Агент безопасности с модулем управления исправлениями устанавливается на конечных точках.
- Для успешного выполнения задач сканирования и установки конечные точки Windows должны соответствовать следующим условиям:
  - **Доверенные корневые центры сертификации** хранит **Сертификат корневого ЦС DigiCert Assured ID**.
  - **Промежуточные центры сертификации** включает в себя **центр сертификации подписанного кода DigiCert SHA2**.
  - На конечных точках установлены исправления для Windows 7 и Windows Server 2008 R2, упомянутые в этой статье Microsoft: Рекомендации по безопасности Microsoft 3033929

Сканирование патча

Конечные точки с устаревшим программным обеспечением уязвимы для атак. Рекомендуется регулярно проверять и устанавливать обновление ПО на конечных точках. Чтобы сканировать конечные точки на наличие пропущенных исправлений:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемый контейнер в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.
4. Выберите целевые конечные точки
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Сканировать исправления**. Появится окно подтверждения.
6. Нажмите **Да** чтобы подтвердить задачу сканирования

   Когда задача заканчивается, GravityZone добавляет в Инвентарь исправлений все исправления, необходимые для вашего программного обеспечения. Дополнительные сведения см. в разделе «Инвентаризация патча» (p. 71).

Примечание
Чтобы запланировать сканирование исправлений, измените политики, назначенные целевым конечным точкам, и настройте параметры в разделе **Управление исправлениями**. Для получения более подробной информации, обратитесь к «Управление исправлениями» (p. 246).

Установка патча

Чтобы установить 1 или несколько исправлений на целевой конечной точке:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемый контейнер в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.
4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Установить исправления**.

Появится окно настроек. Здесь вы можете просмотреть все патчи, отсутствующие на целевых конечных точках.

5. При необходимости используйте параметры сортировки и фильтрации в верхней части таблицы, чтобы найти конкретные исправления.
6. Нажмите кнопку **Столбцы** в верхней правой части панели, чтобы просмотреть только соответствующую информацию.
7. Выберите исправления, которое вы хотите установить.

   Некоторые исправления зависят от других В таком случае они автоматически выбираются один раз вместе с исправлением.

   При нажатии на номера **CVE** или **Продукты** отобразится панель с левой стороны. Панель содержит дополнительную информацию, такую как CVE, которые исправляет исправление, или продукты, к которым применяется исправление. Как только прочитаете, нажмите **Закрыть**, чтобы скрыть панель.
8. Выберите **Перезагрузить конечные точки после установки исправления, если необходимо**, чтобы перезапустить конечные точки сразу после установки исправления, если требуется перезагрузка системы. Учтите, что это действие может прервать сеанс пользователя.
9. Щелкните **Установить**.

   Задача установки создается вместе с подзадачами для каждой целевой конечной точки.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Запущенные Задачи» (p. 80).

Примечание

- Чтобы запланировать развертывание исправлений, измените политики, назначенные целевым конечным точкам, и настройте параметры в разделе **Управление исправлениями**. Для получения более подробной информации, обратитесь к «Управление исправлениями» (p. 246).
- Вы также можете установить исправление со страницы **Инвентарь исправлений**, начиная с определенного интересующего вас исправления. В этом случае выберите исправление из списка, нажмите кнопку **Установить** в верхней части таблицы и настройте параметры установки исправления. Дополнительные сведения см. в разделе «Установка патчей» (p. 75).

- После установки исправления мы рекомендуем отправить задачу Сканировать исправления конечным точкам. Это действие обновит информацию об исправлении, сохраненную в GravityZone для ваших управляемых сетей.

Вы можете удалить исправления:

- Удаленно, отправив из GravityZone Задача удаления исправлений.
- Локально на конечной точке В этом случае вам необходимо войти в систему как администратор конечной точки и запустить деинсталлятор вручную.

6.6.5. Сканирование Exchange

Вы можете удаленно сканировать базу данных сервера Exchange, запустив задачу **Exchange Scan**.

Для того, чтобы сканировать базу данных Exchange, необходимо включить сканирование по запросу, указав учетные данные администратора Exchange. Для получения более подробной информации, обратитесь к «Сканирование хранилища Exchange» (p. 267).

Для сканирования базы данных сервера Exchange:

1. Перейдите в раздел **Сеть**.
2. В левой панели, выберите группу, содержащую нужный сервер Exchange. Желаемый сервер вы можете выбрать в правой панели.

   Примечание
   При желании, вы можете использовать фильтры, чтобы быстро найти нужный сервер:
   - Нажмите меню **Фильтры** и выберите следующие параметры: **Управляемый (Exchange Servers)** на вкладке **Безопасность** и **Все пункты рекурсивно** на вкладке **Глубина**.
   - Введите имя сервера или IP-адрес в нужном поле под заголовком соответствующего столбца.

3. Отметьте флажком сервер Exchange, базу данных которого вы хотите проверить.
4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Exchange Scan**. Появится окно настроек.
5. Настройте параметры сканирования:

- **Общее** Введите подходящее имя задачи.

  Для больших баз данных задача сканирования может занимать много времени и может повлиять на производительность сервера. В таких случаях, установите флажок **Остановите сканирование, если это займет больше времени, чем** и выбрать подходящий интервал времени в соответствующем меню.
- **Цель** Выберите контейнеры и объекты, которые будут проверяться. Вы можете выбрать для сканирования: почтовые ящики, общие папки или и то, и другое. Кроме электронной почты, вы можете выбрать для сканирования другие объекты, такие, как **Контакты**, **Задачи**, **Фурнитура** и **Опубликовать элементы**. Кроме того, вы можете установить следующие ограничения на содержимое, которое будет проверяться:
  - Только непрочитанные сообщения
  - Только элементы с вложениями
  - Только новое, полученное в указанный промежуток времени

  Например, вы можете выбрать для сканирования только письма почтовых пользователей, принятые за последние семь дней.

  Выберите флажок **Исключения**, если вы хотите определить исключения при сканировании. Чтобы создать исключение, используйте поля из заголовков таблицы следующим образом:
  a. Выберите тип репозитория из меню.
  b. В зависимости от типа хранилища укажите объекты, которые должны быть исключены:

Тип хранилища	Формат объекта
Почтовый ящик	Адрес электронной почты
Общая папка	Путь к папке, начиная с корня каталога
База данных	Идентификатор базы данных

  Примечание
  Для получения идентификатора базы данных, используйте команду оболочки Exchange:
  `Get-MailboxDatabase | fl name,identity`

Вы можете ввести только одну команду за один раз. Если у вас есть несколько объектов одного типа, вы должны задать столько правил, сколько элементов.

c. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы, чтобы сохранить исключение и добавить его в список.

Чтобы удалить правило исключения из списка, нажмите соответствующую кнопку ⊖ **Удалить**.

- **Параметры** Настройте параметры сканирования для сообщений электронной почты, соответствующих правилу:
  - **Типы отсканированных файлов** Используйте эту опцию, чтобы указать, какие типы файлов вы хотите просканировать. Вы можете сканировать все файлы (независимо от их расширения), только файлы приложений или определенные типы файлов, которые вы считаете опасными. Сканирование всех файлов обеспечивает наилучшую защиту, в то время как сканирование только приложений рекомендуется для быстрого сканирования.

    Примечание
    Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов. Для получения более подробной информации, обратитесь к «Типы файлов приложений» (p. 509).

    Если вы хотите сканировать файлы с определенными расширениями, у вас есть два варианта:
    - **Пользовательские расширения**, где вы должны указать только те расширения, которые будут проверяться.
    - **Все файлы, кроме определенных расширений**, где вы должны ввести только те расширения, которые будут пропущены при сканировании.
  - **Максимальный размер вложения / тела письма (MB).** Установите этот флажок и введите значение в соответствующем поле, чтобы установить максимально допустимый размер прикрепленного файла или тела сообщения электронной почты, которые будут проверяться.
  - **Максимальная глубина архива (уровней).** Установите флажок и выберите максимальную глубину архива из соответствующего поля. Чем ниже уровень глубины, тем выше производительность и ниже степень защиты.
  - **Сканирование на наличие потенциально нежелательных приложений(PUA).** Установите этот флажок, чтобы просканировать

возможность проникновения вредоносных или нежелательных приложений, таких как программы показа рекламы, которые могут установиться на системах без согласия пользователя, изменить поведение различных программных продуктов и снизить производительность системы.

- **Действия** Вы можете указать различные автоматические действия агента безопасности для файлов, в зависимости от типа обнаружения.

  Тип обнаружения делит файлы на три категории:
  - **Зараженных файлов.** Bitdefender определяет файлы как зараженные с помощью различных передовых механизмов, которые включают сигнатуры вредоносного ПО, технологии машинного обучения и искусственного интеллекта (ИИ).
  - **Подозрительные файлы.** Эти файлы опредеояются, как подозрительные с помощью эвристического анализа и других технологий Bitdefender. Такой подход обеспечивает высокий уровень обнаружения, но в некоторых случаях пользователь должен знать о случаях ложных сигналов (чистые файлы, определенные как подозрительные).
  - **Не сканируемые файлы** Эти файлы не могут быть просканированы. Это могут быть файлы защищенные паролем, зашифрованные, перепакованные и другие.

  Для каждого типа обнаружения, вы можете выбрать действия по умолчанию или основные и альтернативные действия, если основные не выполняются. Хотя это и не рекомендуется, можно изменить эти действия в соответствующих меню. Выберите действие, которое будет принято:
  - **Дезинфицировать** Удаляет вредоносный код из инфицированных файлов и восстанавливает исходный файл. В случае определенных типов вредоносных программ лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов. Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.
  - **Отклонить / удалить письмо.** На серверах с ролью пограничного транспорта (Edge Transport), обнаруженная электронная почта будет отклонена с ошибкой SMTP 550. Во всех других случаях электронная почта удаляется без предупреждения. Желательно избегать использование этого действия.

- **Удалить файл** Удаляет проблемные вложения без предупреждения. Желательно избегать использование этого действия.
- **Заменить файл.** удаляет проблемные файлы и вставляет текстовый файл, который уведомляет пользователя о принятых мерах.
- **Переместить файл в карантин.** Перемещает обнаруженные файлы в карантин и вставляет текстовый файл, который уведомляет пользователя о принятых мерах. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице **Карантин**.

  Примечание
  Пожалуйста, обратите внимание, что карантин для серверов Exchange требует дополнительное дисковое пространство на разделе, где установлен агент безопасности. Размер карантина зависит от количества хранящихся элементов и их размера.

- **Не предпринимать никаких действий** Никаких действий не будет предпринято в отношении обнаруженных файлов. Эти файлы будут отображаться только в журнале сканирования. По умолчанию, задачи сканирования настроены игнорировать подозрительные файлы. Вы можете изменить действие по умолчанию, чтобы перемещать подозрительные файлы в карантин.
- По умолчанию, когда почта соответствует одному правилу, она обрабатывается исключительно только им, без проверки любых других оставшихся правил. Если вы хотите продолжить проверку другими правилами, снимите флажок **Если условия правила совпадают, прекратить обработку другими правилами**

6. Нажмите **Сохранить**, чтобы создать задачу сканирования. Появится окно подтверждения.
7. Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к Просмотр и управление задачами.

6.6.6. Установить

Для защиты ваших конечных точек агентом безопасности Bitdefender, необходимо установить его на каждой из них.

После того, как вы установили агент-ретранслятор, он будет автоматически обнаруживать незащищенные конечные точки в этой же сети.

Защита Bitdefender может быть затем установлена на конечных точках удаленно из Control Center.

Удаленная установка выполняется в фоновом режиме, без ведома пользователя.

Предупреждение

Перед установкой, убедитесь, что на компьютере удалено существующее программное обеспечение для защиты от вредоносного ПО и брандмауэр. Установка защиты Bitdefender вместе с другим программным обеспечением безопасности может повлиять на работу и вызвать серьезные проблемы с системой. Защитник Windows и брандмауэр Windows будут отключены автоматически, когда начнется установка.

Если вы хотите развернуть агент безопасности на компьютере с Антивирусом Bitdefender для Mac 5. X, сначала необходимо удалить его вручную. Для инструкции для выполнения смотрите эту статью базы знаний.
При развертывании агента через Linux Relay должны выполняться следующие условия:

- На конечной точке с Relay ролью должен быть установлен пакет Samba (`smbclient`) версии 4.1.0 или выше и `net` binary/command для развертывания агентов на Windows.

  Примечание

  `net` binary/command обычно используется с samba-клиентом и/или стандартными пакетами samba. В некоторых дистрибутивах Linux (например CentOS 7.4) `net` command устанавливается только, когда установлен Samba Samba suite (Common + Client + Server). Убедитесь, что на конечной точке с Relay ролью доступна `net` command.

- Целевые конечные точки Windows должны иметь доступ к ресурсам администрирования и сети.
- В целевых конечных точках Linux и Mac должен быть включен SSH и отключен брандмауэр.

Чтобы запустить задачу удаленной установки:

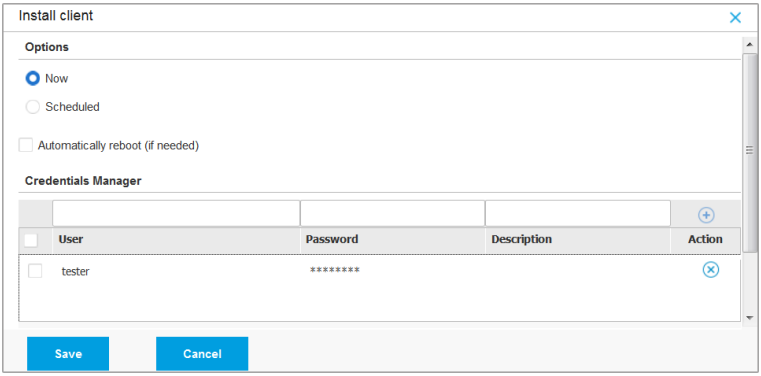
1. Подключитесь и войдите в Control Center.

2. Перейдите в раздел **Сеть**.
3. Выберите нужную группу в левой панели. Объекты, содержащиеся в выбранной группе, будут отображены в таблице правой панели.

> **Примечание**
> При желании, вы можете применять фильтры для отображения только неуправляемых конечных точек. Нажмите меню **Фильтры** и выберите следующие параметры: **Неуправляемые** на вкладке **Безопасность** и **Все предметы рекурсивно** на вкладке **Глубина**.

4. Выберите объекты (конечные точки или группы конечных точек), на которых вы хотите установить защиту.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Установить**.

   Отобразится мастер установки **Install Client**.



Установка Bitdefender Endpoint Security Tools из меню задач

6. В разделе **Опции**, настройте время установки:
   - **Сейчас**, чтобы немедленно начать развертывание.
   - **Запланировано**, настроить интервал повторения развертывания. В этом случае, выберите желаемый интервал времени (ежечасно, ежедневно или еженедельно) и настройте его в соответствии с вашими потребностями.

Примечание
Например, когда некоторые операции требуется выполнить на нужной машине перед установкой клиента (например, удаление другого программного обеспечения и перезагрузки ОС), вы можете запланировать запуск задачи развертывания каждые 2 часа. Задача будет запускаться на каждом компьютере каждые 2 часа до тех пор, пока развертывание не будет завершено.

7. Если вы хотите, чтобы заданные конечные точки перезапустились после завершения установки, выберите **Автоматическая перезагрузка (при необходимости)** .
8. В разделе **Диспетчер учетных задач**, укажите учетные данные администратора, необходимые для удаленной аутентификации на заданных конечных точках. Вы можете добавить учетные данные, набрав имя пользователя и пароль, для каждой выбранной операционной системы.

Важно
Для станций под Windows 8.1, необходимо предоставить учетные данные встроенной учетной записи администратора или учетной записи администратора домена. Для получения подробной информации смотрите эту статью базы знаний.

Чтобы добавить необходимые учетные данные ОС:

a. Введите имя пользователя и пароль учетной записи администратора в соответствующих полях заголовка таблицы.

Если компьютеры находятся в домене, достаточно ввести учетные данные администратора домена.

Используйте правила именования Windows при вводе имени учетной записи:

- Для машин из службы каталогов Active Directory используйте следующий синтаксис: `username@domain.com` и `domain\username`. Чтобы быть уверенным, что введенные учетные данные будут работать, добавьте их в обоих видах (`username@domain.com` и `domain\username`).
- Для машин из рабочей группы достаточно ввести только имя пользователя без имени рабочей группы.

При желании, вы можете добавить описание, которое поможет вам проще определить каждый аккаунт.

b. Нажмите кнопку ⊕ **Добавить**. Учетная запись будет добавлена в список учетных данных.

Примечание
Указанные учетные данные автоматически сохраняются в Менеджере учетных данных, так что вам не придется вводить их в следующий раз. Для доступа к диспетчеру учетных данных, просто укажите ваше имя пользователя в правом верхнем углу консоли.

Важно
Если предоставленные учетные данные являются недействительными, развертывание клиента на соответствующих конечных точках не произойдет. Не забудьте обновить учетные данные введенной ОС в диспетчере учетных данных, если они изменились на конечных точках.

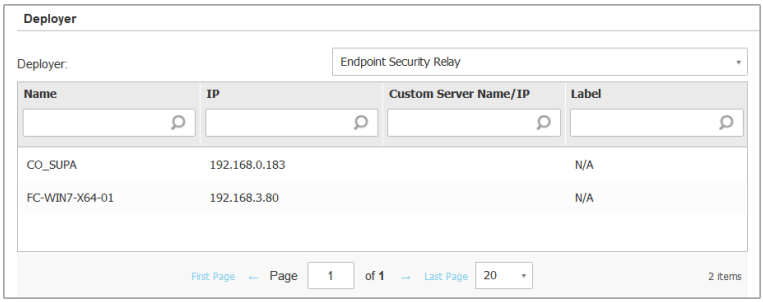
9. Установите флажки на соответствующие аккаунты, которые вы хотите использовать.

Примечание
Предупреждающее сообщение будет отображаться до тех пор, пока вы не выберите какие-нибудь учетные данные. Этот шаг является обязательным для удаленной установки агента безопасности на конечных точках.

10. В разделе **Участник операции** настройте Relay, к которому будут подключаться целевые конечные точки для установки и обновления клиента:

- Все компьютеры с ролью Relay, обнаруженные в сети, будут отображаться в таблице, доступной в разделе **Участник операции**. Каждый новый клиент должен быть подключен в той же сети по меньшей мере к одному Relay, который будет служить в качестве коммуникационного и сервера обновлений. Выберите Relay, к которому вы хотите подключить выбранные конечные точки. Подключенные конечные точки будут сообщаться при помощи Control Center только через выбранный компьютер с ролью ретранслятора.

Важно
При развертывании через агента ретранслятора, должен быть открыт 7074 порт.



11. Вы должны выбрать один установочный пакет для текущего развертывания. Нажмите на список **Использовать пакет** и выберите установочный пакет, который вам нужен. Вы можете найти здесь все инсталляционные пакеты, созданные ранее под вашей учетной записью, а также пакеты установки по умолчанию, доступные в Control Center.
12. При необходимости, вы можете изменить некоторые настройки выбранного пакета установки с помощью кнопки **Настроить**, рядом с полем **Использовать пакет**.

    Настройки инсталляционного пакета появятся ниже и вы сможете сделать необходимые изменения. Чтобы узнать больше о редактировании инсталляционных пакетов, обратитесь к руководству по установке GravityZone.

    Если вы хотите сохранить изменения как новый пакет, выберите опцию **Сохранить как пакет**, расположенную в нижней части списка параметров пакета, и введите имя для нового пакета установки.
13. Нажмите **Сохранить**. Появится окно подтверждения.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**.

Важно
При использовании VMware Horizon View Persona Management рекомендуется настроить групповую политику Active Directory, чтобы исключить следующие процессы Bitdefender (без полного пути):

- bdredline.exe
- epag.exe
- epconsole.exe
- epintegrationservice.exe
- epprotectedservice.exe
- epsecurityservice.exe
- epupdateservice.exe
- epupdateserver.exe

Эти исключения должны применяться до тех пор, пока агент безопасности работает в конечной точке. Подробнее см. на этой странице документации VMware Horizon .

6.6.7. Клиент обновления

Эта задача доступна только тогда, когда агент Endpoint Security установлен и обнаружен в сети. Bitdefender рекомендует выполнить обновление с Endpoint Security до нового Bitdefender Endpoint Security Tools для защиты конечной точки последнего поколения.

Чтобы легко найти клиентов, которые не были обновлены, вы можете создать отчет о состоянии обновления. Для получения информации о том, как создать отчеты см. «Создание отчетов» (p. 452).

6.6.8. Удаление клиента

Для удаленного удаления защиты Bitdefender:

1. Перейдите в раздел **Сеть**.
2. Выберите желаемый контейнер в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.
3. Отметьте флажками конечные точки, с которых вы хотите удалить агента безопасности Bitdefender.
4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Удалить клиента**.
5. Появится окно конфигурации, позволяющее вам выбрать хранение объектов, помещенных в карантин, на клиентской машине.
6. Нажмите **Сохранить**, чтобы создать задачу. Появится окно подтверждения.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к Просмотр и управление задачами.

Примечание
Если вы хотите переустановить защиту, в первую очередь обязательно перезагрузите компьютер.

6.6.9. Обновление клиента

Периодически проверяйте статус управляемых компьютеров. Если вы заметили компьютер с проблемами безопасности, нажмите на его имя, чтобы отобразить страницу **Информация**. Для получения более подробной информации, обратитесь к «Статус безопасности» (p. 48).

Устаревшие клиенты или устаревшие механизмы защиты представляют проблемы безопасности. В этих случаях, вы должны запустить обновление на соответствующем компьютере. Эта задача может быть запущена локально с компьютера, или дистанционно с Control Center.

Для удаленного обновления клиента и механизмов защиты на управляемых компьютерах:

1. Перейдите в раздел **Сеть**.
2. Выберите желаемый контейнер в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.
3. Отметьте флажками конечные точки, на которых вы хотите запустить обновление клиента.
4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обновить**. Появится окно настроек.
5. Вы можете обновить только продукт, только механизмы защиты или всё сразу.
6. Нажмите **Обновить** для запуска задачи. Появится окно подтверждения.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к Просмотр и управление задачами.

6.6.10. Перенастройка клиента

Модули защиты агента безопасности, роли и режимы сканирования изначально заданы в установочном пакете. После того как вы установили агента безопасности в вашей сети, вы можете в любое время изменить исходные настройки, отправив задачу перенастройки **Reconfigure Client** к требуемым управляемым конечным точкам.

Предупреждение
Пожалуйста, обратите внимание, что задача **Reconfigure Client** перезаписывает все параметры установки и ни одна из начальных настроек не сохраняется. Во время использования этой задачи, убедитесь, что перенастроили все настройки установки для требуемых конечных точек.

Примечание
Задача **Перенастроить клиента** удалит все неподдерживаемые модули из существующих установок в устаревшей Windows.

Параметры установки можно изменить в области **Сеть** или в отчете **Статус модулей конечных точек**.

Чтобы изменить настройки установки для одной или нескольких конечных точек:

1. Перейдите в раздел **Сеть**.
2. Выберите желаемую группу в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.
3. Отметьте флажками конечные точки, для которых вы хотите изменить параметры установки.
4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Перенастроить клиента**.
5. Выберите одно из следующих действий:
   - **Добавить**. Добавьте новые модули к существующим.
   - **Удалить**. Удалить определенные модули из существующих.
   - **Список путей**. Подберите модули, установленные по вашему выбору.
6. Выберите модули и роли, которые вы собираетесь установить или удалить на целевых конечных точках.

Предупреждение
Будут установлены только поддерживаемые модули. Например, брандмауэр устанавливается только на поддерживаемые рабочие станции Windows. Дополнительную информацию смотрите в разделе Наличие уровней защиты GravityZone.

7. Выберите **Удалить конкурентов, если это необходимо**, чтобы убедиться, что выбранные модули не будут конфликтовать с другими решениями безопасности, установленными на целевых конечных точках.
8. Выберите один из доступных режимов сканирования:
   - **Автоматически**. Агент безопасности обнаруживает, какие механизмы сканирования подходят для ресурсов конечной точки.
   - **Custom**. Вы напрямую выбираете, какие механизмы сканирования использовать.

     Для получения информации о доступных вариантах обратитесь к разделу Создание инсталляционных пакетов из Руководства по установке.

Примечание
Этот раздел доступен только для **Списка совпадений**.

9. В разделе **Планировщик** выберите время запуска задачи:
   - **Сейчас**, чтобы немедленно начать задачу.
   - **Запланировано**, чтобы настроить интервал повторяемости задачи.

     В этом случае выберите временной интервал (ежечасно, ежедневно или еженедельно) и настройте его в соответствии с вашими потребностями.
10. Нажмите **Сохранить**. Появится окно подтверждения.

    Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к Просмотр и управление задачами.

6.6.11. Обслуживание клиента

Используйте Repair Client task в качестве начальной задачи устранения неполадок для любого количества проблем, связанных с конечными точками. Задача загружает последний установочный пакет на целевую конечную точку, а затем выполняет переустановку агента.

Примечание

- The modules currently configured on the agent will not be changed.
- При задаче восстановления будет сброшен агент безопасности до текущей версии Slow Ring.

Чтобы Repair Client task клиенту на ремонт:

1. Перейдите в раздел **Сеть**.
2. Выберите желаемый контейнер в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.
3. Отметьте флажками конечные точки, на которых Вы хотите запустить исправление клиента.
4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Исправление клиента**. Появится окно подтверждения.
5. Установите флажок **Японимаю и согласен** и нажмите кнопку **Сохранить**, чтобы запустить задачу.

   Примечание
   Для завершения задачи по восстановлению может потребоваться перезапуск клиента

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к Просмотр и управление задачами.

6.6.12. Перезагрузка машины

Вы можете удаленно перезагрузить управляемые конечные точки.

Примечание
Проверьте страницу **Network > Tasks** перед перезапуском определенных конечных точек. Ранее созданные задачи еще могут быть в процессе выполнения на выбранных конечных точках.

1. Перейдите в раздел **Сеть**.
2. Выберите желаемый контейнер в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.
3. Отметьте флажками конечные точки, которые вы хотите перезагрузить.
4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Перезагрузить машину**.
5. Выберите опции перезагрузки по расписанию:
   - Выберите **Restart now**, чтобы немедленно перезагрузить конечные точки.
   - Выберите **Включить перезагрузку** и используйте поля ниже, чтобы запланировать перезагрузку в определенную дату и время.
6. Нажмите **Сохранить**. Появится окно подтверждения.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к Просмотр и управление задачами.

6.6.13. Сетевое Обнаружение

Сетевое обнаружение выполняется автоматически только агентами безопасности с ролями Relay role. Тем не менее, вы можете вручную запустить задачу сетевого обнаружения из Control Center в любое время с любого компьютера, защищенного Bitdefender Endpoint Security Tools.

Чтобы запустить задачу сетевого обнаружения в вашей сети:

1. Перейдите в раздел **Сеть**.
2. Выберите желаемый контейнер в левой панели. Все конечные точки из выбранного контейнера отобразятся в правой панели таблицы.
3. Отметьте флажком конечную точку-ретранслятор, на которой вы хотите запустить задачу сетевого обнаружения.

4. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обнаружение сети**.
5. Появится окно подтверждения. Нажмите **Да**.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к Просмотр и управление задачами.

6.6.14. Обновление Security Server

Если Security Server устарел, вы можете отправить ему задачу обновления:

1. Перейдите в раздел **Сеть**.
2. Выберите группу, где установлен Security Server.

   Чтобы легче найти Security Server, вы можете использовать меню **Фильтры** следующим образом:

   - Перейдите на вкладку **Безопасность** и выберите только **Серверы безопасности**.
   - Перейдите на вкладку **Глубина** и выберите **Все предметы рекурсивно**.
3. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обновить Security Server**. Откроется окно конфигурации.
4. Выберете тип обновления, чтобы представить:

   - **Функции безопасности**для установки новых функций Bitdefender, улучшений и исправлений, а также исправлений безопасности.
   - **Операционная система**, для обновления операционной системы устройства Security Server

   Чтобы узнать, какой вариант выбрать, прочитайте Security Server примечания к выпуску.
5. Кроме того, для обновления операционной системы выберите время и дату запуска обновления. Вы можете запустить его немедленно или запланировать его в удобное время, используя окно обслуживания.
6. Нажмите **OK**, чтобы сохранить задание.

   Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к Просмотр и управление задачами.

6.7. Интеграция со службой каталогов Active Directory

Интеграция позволяет GravityZone импортировать компьютерный инвентарь из Active Directory локально и из Active Directory, размещенной в Microsoft Azure. Таким образом, можно легко развертывать и управлять защитой на конечных точках Active Directory. Интеграция выполняется через управляемую конечную точку, называемую Active Directory Integrator.

Для управления интеграцией с Active Directory можно выполнить следующие действия:

- Настройка Active Directory Integrator
- Удаление Active Directory Integrator
- Удаление интеграции

6.7.1. Настройка Active Directory Integrator

Можно определить несколько интеграторов Active Directory для одного домена, а также для каждого доступного домена.

Требования к системе

Интегратор Active Directory должен соответствовать следующим условиям:

- Он работает под управлением ОС Windows.
- Он подключен в службе каталогов Active Directory.
- Он защищен Bitdefender Endpoint Security Tools.
- Он всегда в сети. Иначе это может повлиять на синхронизацию со службой каталогов Active Directory.

Важно
Рекомендуется, чтобы конечные точки, объединенные в AD, имели политику, назначенную непосредственно им. Все конечные точки, обнаруженные в домене Active Directory, будут перемещены из исходной папки в папку Active Directory. В этом случае, если конечные точки имеют унаследованную политику, они будут назначаться с политикой, установленной по умолчанию.

Настройка Active Directory Integrator

Можно определить несколько интеграторов Active Directory для одного домена, а также для каждого доступного домена.

Чтобы установить конечную точку в качестве Active Directory Integrator:

1. Перейдите в раздел **Сеть**.
2. Перейдите через инвентаризацию сети в группу, в которой находится конечная точка, и выберите ее.

   Примечание
   Если требуется определить несколько интеграторов, необходимо выбрать одну конечную точку.

3. Нажмите кнопку **Интеграция** в верхней части таблицы и выберите команду **Установить как Active Directory Integrator**.
4. Подтвердите ваши действия, нажав **Да**.

   Появится новый значок конечной точки, обозначающий Active Directory Integrator. Через пару минут Вам станет доступен просмотр древовидной схемы **Active Directory** рядом с **Компьютеры и Группы**. Для больших сетей со службой каталогов Active Directory завершение синхронизации может занять больше времени. Конечные точки, объединенные в том же домене, что и Active Directory Integrator, будут перемещены из **Компьютеры и Группы** в контейнер Active Directory.

Синхронизация со службой каталогов Active Directory

GravityZone каждый час автоматически синхронизируется со службой каталогов Active Directory.

GravityZone не может синхронизироваться с доменом Active Directory, если возникают следующие ситуации:

- Все роли Active Directory integrator были удалены
- Соединение между интеграторами Active Directory и GravityZone прервано в течение не менее 2 часов.
- Ни один из интеграторов Active Directory из того же домена не может взаимодействовать с контроллером домена.

В любом из этих случаев проблема, связанная с Active Directory будет инициирована в **Области уведомлений**. Для получения более подробной информации, обратитесь к «Уведомления» (p. 484).

6.7.2. Удаление Active Directory Integrator

Чтобы удалить роль Active Directory Integrator с конечной точки:

1. Перейдите в раздел **Сеть**.
2. Перейдите через инвентаризацию сети в группу, в которой установлен Active Directory Integrator, и выберите его.

> **Примечание**
> Если требуется удалить несколько интеграторов, необходимо выбрать только одну конечную точку.

3. Нажмите кнопку **Интеграция** в верхней части таблицы и выберите команду **Удалить Active Directory Integrator**.
4. Появится окно подтверждения.
   - Если в том же домене нет другой конечной точки с ролью Active Directory Integrator, в подтверждающем сообщении будет указано, что текущий домен больше не будет синхронизироваться с GravityZone.
   - Если конечная точка отключена, роль Active Directory Integrator будет удалена после ее включения.

Можно проверить, был ли удален какой-либо интегратор Active Directory из управляемой сети в разделе **Действия пользователя**, фильтруя журналы пользователей и используя следующие критерии:

- **Область**: Active Directory
- **Действие**: Удаленный интегратор AD

Для получения более подробной информации, обратитесь к «Журнал активности пользователя » (p. 481).

6.7.3. Удаление интеграции Active Directory

Можно выбрать удаление одного или нескольких доменов из папки Active Directory следующим образом:

1. Перейдите в раздел **Сеть**.
2. Под древовидной схемой **Сеть** выберите в левой панели папку **Active Directory**

3. Перейдите к правой панели и выберите папку домена, которую хотите удалить.
4. Нажмите кнопку **Интеграция** в верхней части таблицы и выберите команду **Удалить Active Directory Integration**.
5. Появится окно подтверждения. Опция, доступная с этим сообщением, дает возможность выбрать- удалять неуправляемые конечные точки из Инвентаризации сети или нет. Будьте внимательны, эта опция включена по умолчанию. Нажмите кнопку **Подтвердить**, чтобы продолжить.
6. Все конечные точки в выбранном домене будут помещены в папку **Компьютеры и группы** (или их исходные группы), роль интегратора Active Directory будет удалена из назначенных конечных точек этого домена.

6.8. Формирование быстрых отчетов

Вы можете создавать быстрые отчеты по управляемым конечным точкам, используя страницу **Network**:

1. Перейдите в раздел **Сеть**.
2. Выберите требуемую группу в левой панели. Все конечные точки из выбранной группы отобразятся в правой панели таблицы.

   При желании, вы можете отфильтровать содержимое выбранной группы только по управляемым конечным точкам.
3. Отметьте флажками компьютеры, которые вы хотите включить в отчет.
4. Нажмите кнопку **Отчет** в верхней части таблицы и выберите из меню тип отчета.

   Для получения более подробной информации, обратитесь к «Отчеты по компьютерам и виртуальным машинам» (p. 435).
5. Настройте параметры отчета. Для получения более подробной информации, обратитесь к «Создание отчетов» (p. 452).
6. Нажмите **Создать**. Отчет отобразится немедленно.

   Время, необходимое для формирования отчетов, может сильно изменяться в зависимости от количества выбранных конечных точек.

6.9. Назначение политик

Вы можете управлять настройками безопасности на конечных точках с помощью политик.

На странице **Network** вы можете просматривать, изменять и назначать политики для каждой конечной точки или группы конечных точек.

Примечание
Настройки безопасности доступны только для управляемых конечных точек. Для облегчения просмотра и управления настройками безопасности, вы можете отфильтровать инвентаризацию сети только по управляемым конечным точкам.

Для просмотра политики, назначенной определенной конечной точке:

1. Перейдите в раздел **Сеть**.
2. Выберите желаемую группу в левой панели. Все конечные точки из выбранной группы отобразятся в правой панели таблицы.
3. Нажмите на имя управляемой конечной точки, которая вас интересует. Появится информационное окно.
4. На вкладке **Общее**, в разделе **Политика**, нажмите на название текущей политики, чтобы просмотреть ее настройки.
5. Вы можете изменить настройки безопасности в случае необходимости, при условии, что владелец политики позволил другим пользователям вносить в нее изменения. Пожалуйста, обратите внимание, что любые изменения, которые вы вносите, влияют на все конечные точки, которым назначена данная политика.

   Для получения более подробной информации о настройках политик, обратитесь к «Политики компьютеров и виртуальных машин» (p. 146).

Чтобы назначить политику компьютеру или группе:

1. Перейдите в раздел **Сеть**.
2. Выберите желаемую группу в левой панели. Все конечные точки из выбранной группы отобразятся в правой панели таблицы.
3. Отметьте флажком требуемую конечную точку или группу. Вы можете выбрать один или несколько объектов одного типа, только одного уровня.
4. Нажмите кнопку **Назначить политику** в верхней части таблицы.

5. Сделайте необходимые настройки в окне **Назначение политики**. Для получения более подробной информации, обратитесь к «Назначение политик» (p. 136).

6.10. Использование Менеджер восстановления (Recovery Manager) для зашифрованных томов

Когда пользователи конечных точек забывают свои пароли шифрования и не могут больше получать доступ к зашифрованным томам на своих компьютерах, вы можете помочь им, получив ключи восстановления со страницы **Сеть**.

Чтобы получить ключ восстановления:

1. Перейдите в раздел **Сеть**.
2. Нажмите кнопку **Менеджер восстановления** на панели инструментов действий на панели слева. Появится новое окно.
3. В разделе окна **Идентификатор** введите следующие данные:
   a. Идентификатор ключа восстановления зашифрованного тома. Идентификатор ключа восстановления представляет собой строку цифр и букв, доступных в конечной точке на экране восстановления BitLocker.

      В Windows идентификатор ключа восстановления представляет собой строку цифр и букв, доступных на конечной точке на экране восстановления BitLocker.

      Кроме того, вы можете использовать параметр **Восстановление** на вкладке **Защита** в Сведениях о компьютере для автоматического ввода идентификатора ключа восстановления, для конечных точек как Windows так и macOS.

   b. Пароль вашей учетной записи GravityZone.
4. Нажмите **Открыть** . Окно расширяется.

   В разделе **Информация о томе** представлены следующие данные:

   a. Имя тома
   b. Тип тома (загрузочный или не загрузочный).
   c. Имя конечной точки (как указано в Инвентаризации сети)

d. Ключ восстановления. В Windows ключ восстановления - это пароль, автоматически генерируемый при шифровании тома. На Mac ключ восстановления - это пароль учетной записи пользователя.

5. Отправьте ключ восстановления пользователю конечной точки.

Подробнее о шифровании и дешифровке томов с помощью GravityZone см. «Шифрование» (p. 291).

6.11. Удаление конечных точек из сетевого содержимого

Инвентаризация сети включает, по умолчанию, папку **Удаленные**, предназначенную для хранения конечных точек, которыми вы больше не хотите управлять.

Однако действие **Удалить** оказывает различное влияние на конечные точки в зависимости от папки, в которой они находятся:

- Для конечных точек в **Компьютеры и группы** вкладке:
  - Когда неуправляемые конечные точки удаляются, они перемещаются непосредственно в папку **Удаленные**.
  - Когда управляемые конечные точки удалены:
    - Задача удаления клиента создана.
    - Лицензионное место освобождено.
    - Конечные точки перемещены в папку **Удаленные**.

      Вы можете просмотреть задачу удаления клиента в разделе **Сетевые задачи**. Если конечная точка не получит задачу (поскольку она находится в автономном режиме), задача останется в состоянии ожидания в течение 72 часов, после чего срок ее действия автоматически истечет.

> **Примечание**
>
> - Если вы хотите навсегда исключить определенные конечные точки из управления, вы должны сохранить их в папке **Удаленные**.
> - Если вы удалите конечные точки из папки **Удаленные**, они будут полностью удалены из базы данных GravityZone. Тем не менее исключенные конечные точки, которые находятся в сети, будут обнаружены при следующей задаче обнаружения сети, и они будут отображаться в инвентаризации сети как новые конечные точки.

- Для конечных точек в папке интеграции (Active Directory, Amazon EC2 и т.д.):
  - Конечные точки становятся неуправляемыми и остаются в своих папках (они не перемещаются в папку **Удалено**).
  - Для каждой конечной точки освобождается место для лицензии.

    Если конечная точка находится в сети, она будет лицензирована снова.

Чтобы удалить конечные точки из инвентаризации сети:

1. Перейдите в раздел **Сеть**.
2. На левой панели выберите сетевую группу, которая вас интересует.

   Поочередно используйте меню **Фильтры** и опцию **Глубина > элементы рекурсивно** в верхней части таблицы, чтобы отобразить все объекты в сети.

   Примечание
   Вы можете удалять только конечные точки, отображаемые в **Компьютер и группы**, которые были обнаружены за пределами любой интегрированной сетевой инфраструктуры.

3. Установите в правой панели флажок напротив конечной точки, которую хотите удалить.
4. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы. Подтвердите ваши действия, нажав **Да**.

   В зависимости от конечных точек они либо будут перемещены в папку **Удаленные**, либо станут неуправляемыми.

Вы можете в любое время переместить конечные точки из **удаленной** папки в **компьютер и группы**, используя перетаскивание.

6.12. Просмотр и управление задачами

Страница **Сеть > Задачи** позволяет просматривать и управлять всеми задачами, которые вы создали.

После того как вы создали задачу хотя бы для одного сетевого объекта, вы можете просмотреть ее в таблице задач.

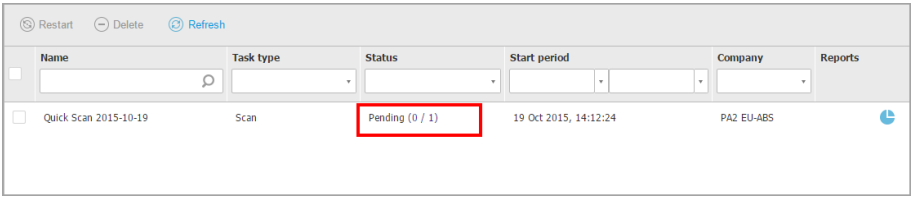
Вы можете выполнить следующие задачи в разделе **Сеть > Задачи**:

- Проверить статус задачи
- Просмотреть отчеты задач
- Перезапустить задачи
- Остановить задачи сканирования Exchange
- Удалить задачи

6.12.1. Проверить статус задачи

Каждый раз, когда вы создаете задачу для одного или нескольких сетевых объектов, вы можете проверить ход выполнения задачи и получить уведомления, когда происходят ошибки.

Перейдите в раздел **Сеть > Задачи** и проверьте колонку **Статус** для каждой интересующей вас задачи. Вы можете проверить статус основной задачи, а также получить подробную информацию о каждой подзадаче.



Страница задач

- **Проверка статуса основной задачи**.

  Основная задача относится к действиям, запущенным на сетевых объектах (например, установка клиента или сканирование) и содержит определенное количество подзадач, по одной для каждого выбранного сетевого объекта. Например, основная задача установки клиента, созданная для восьми компьютеров, содержит восемь подзадач. Цифры в скобках показывают соотношение завершенных задач к общему количеству. Например, (2/8) означает, что две из восьми подзадач закончены.

  Статус основной задачи может быть следующим:
  - **Pending**, если ни одна из подзадач еще не началась.
  - **Выполняется**, когда все подзадачи выполняются. Основная задача будет находится со статусом "Выполняется" пока последняя подзадача не будет выполнена.

- **Завершена**, когда все подзадачи (удачно или неудачно) завершены. В случае неудачного выполнения подзадач, отобразится предупреждающий символ.

- **Проверка статуса подзадач**.

  Перейдите к интересующей вас задаче и нажмите на ссылку в колонке **Статус**, чтобы открыть окно **Статус**. Вы можете просмотреть список сетевых объектов с запущенной главной задачей и статус соответствующих подзадач. Статус подзадачи может быть следующим:

  - **Выполняется,** если подзадача еще выполняется.

    Для Exchange, вы также можете просмотреть статус завершения задач сканирования по запросу.

  - **Завершена**, если подзадача успешно завершена.

  - **Ожидание**, если выполнение подзадачи еще не начато. Это может случится в следующих ситуациях:

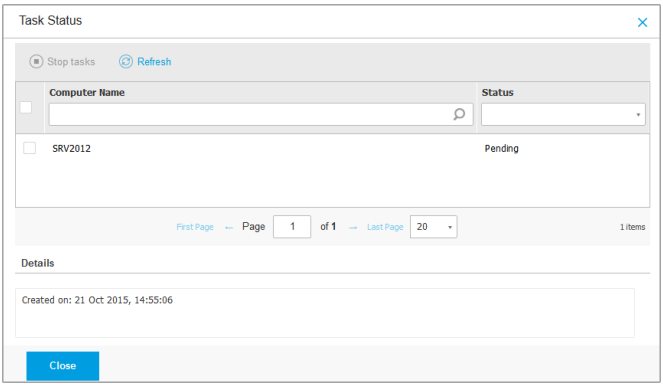
    - Подзадача ожидает очереди.

    - Существует проблема подключения между Control Center и выбранным сетевым объектом.

  - **Провалена**, если подзадача не может быть запущена или она остановлена из-за ошибок, таких как неверные учетные данные для аутентификации и нехватка памяти.

  - **Остановка**, когда сканирование по запросу занимает слишком много времени и вы решили его остановить.

  Для просмотра сведений о каждой подзадаче, выберите ее и проверьте раздел **Подробности** в нижней части таблицы.



Подробная информация о статусах задач

Вы сможете получить следующую информацию:

- Дата и время, когда задача была запущена.
- Дата и время, когда задача была завершена.
- Описание встречающихся ошибок.

6.12.2. Просмотр отчетов задач

На странице **Сеть > Задачи** у вас есть возможность просмотреть отчеты задач быстрого сканирования.

1. Перейдите на страницу **Сеть > Задачи**.
2. Установите флажок на интересующей вас задаче сканирования.
3. Нажмите соответствующую кнопку в колонке **Отчеты**. Дождитесь отображения отчета. Для получения более подробной информации, обратитесь к «Использование отчетов» (p. 434).

6.12.3. Перезапуск задач

По различным причинам задачи установки клиента, удаления или обновления могут быть не завершены. В таких случаях, вы можете перезапустить эти задачи вместо создания новых, выполнив следующие шаги:

1. Перейдите на страницу **Сеть > Задачи**.
2. Установите флажки на требуемых незавершенных задачах.

3. Нажмите кнопку **Перезапуск** в верхней части таблицы. Выбранные задачи будут перезапущены и их статус изменится на **Повторение**.

Примечание
Для задач с несколькими подзадачами, задача **Перезапуск** станет доступна только тогда, когда все подзадачи будут завершены, а перезапущены будут только незавершенные подзадачи.

6.12.4. Остановка задач сканирования Exchange

Сканирование хранилища Exchange может занимать длительное время. Если по каким-либо причинам вы хотите остановить задачу сканирования Exchange по запросу, выполните следующие шаги:

1. Перейдите на страницу **Сеть > Задачи**.
2. Нажмите на ссылку в колонке **Статус**, чтобы открыть окно **Статус задачи**.
3. Установите флажок на соответствующих отложенных или запущенных подзадачах, которые вы хотите остановить.
4. Нажмите кнопку **Остановить задачи** в верхней части таблицы. Вы должны будете подтвердить ваши действия, нажав **Да**.

Примечание
Вы также можете остановить сканирование хранилища Exchange по запросу из области событий Bitdefender Endpoint Security Tools.

6.12.5. Удаление задач

GravityZone автоматически удаляет ожидающие задачи через два дня и завершает задачи через 30 дней. Если у вас по-прежнему много задач, рекомендуется удалить задачи, которые вам больше не нужны, чтобы предотвратить засорение списка.

1. Перейдите на страницу **Сеть > Задачи**.
2. Установите флажок на соответствующей задаче, которую вы хотите удалить.
3. Нажмите кнопку **Удалить** в верхней части таблицы. Вы должны будете подтвердить ваши действия, нажав **Да**.

Предупреждение
Удаление отложенного задания, также отменит и само задание.
Если задача в процессе выполнения, ее удаление отменит и все подзадачи, находящиеся в режиме ожидания. Все завершенные подзадачи отменены быть не могут.

6.13. Настройка параметров сети

На странице **Настройки > Настройки сети** вы можете настроить параметры инвентаризации сети, такие как: сохранение фильтров, сохранение последнего просмотренного местоположения, создание и управление запланированными правилами удаления неиспользуемых виртуальных машин.

Настройки объединены в следующие разделы:

- Настройки инвентаризации сети
- Автономное удаление машин

6.13.1. Настройки инвентаризации сети

В разделе **Настройки инвентаризации сети** доступны следующие параметры:

- **Сохранить фильтры инвентаризации сети**. Установите этот флажок, чтобы сохранить ваши фильтры на странице **Сеть** между сеансами Control Center.
- **Запомнить последнее просмотренное местоположение в инвентаризации сети (Network Inventory), пока я не выйду из системы**. Установите этот флажок, чтобы сохранить последнее местоположение, к которому вы обращались при выходе со страницы **Сеть**. Местоположение между сессиями не сохраняется.
- **Избегайте дублирования клонированных конечных точек**. Выберите эту опцию, чтобы включить новый тип сетевых объектов в GravityZone, называемых золотыми образом. Таким образом, вы можете различать исходные конечные точки от их клонов.

  Для конечных точек, зарегистрированных в Active Directory, используйте следующие параметры:

  – **Применяется к клонированным физическим конечным точкам, объединенным в Active Directory**. Эта опция разрешает проблемы с клонированными жесткими дисками из машин эксплуатации.

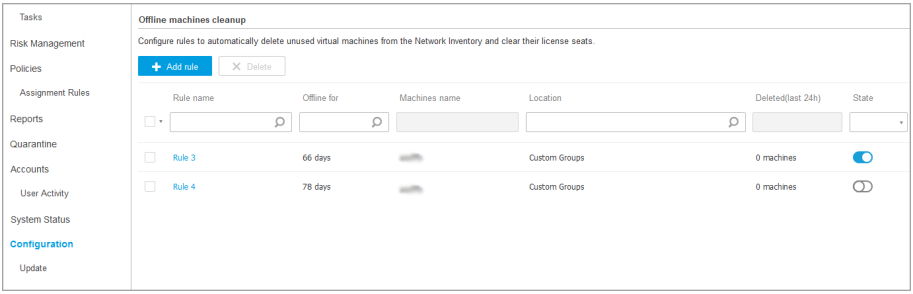
– **Применяется к клонированным виртуплным конечным точкам, объединенным в Active Directory**. Этот параметр разрешает клоны, созданные с помощью VMware Instant Clones.

Далее необходимо пометить каждую конечную точку, которую вы клонируете, следующим образом:

1. Перейдите в раздел **Сеть**.
2. Выберите конечную точку, которую вы хотите клонировать.
3. В контекстном меню выберите **Пометить как Золотое изображение**.

6.13.2. Автономное удаление машин

В разделе **Очистка автономных компьютеров** вы можете запланировать правила автоматического удаления неиспользуемых виртуальных машин из инвентаризации сети.



Настройки - Настройки сети - Автономное удаление машин

Создание правил

Для создания правила удаления:

1. В разделе **Автономная уборка машин** нажмите кнопку **Добавить правило**.
2. На странице конфигурации:
   a. Введите имя правила.
   b. Выберите час для ежедневного удаления.
   c. Определите критерии удаления:

- Количество дней, в течение которых машины были отключены (от 1 до 90).
- Шаблон имени, который может применяться к одной виртуальной машине или к нескольким виртуальным машинам.

  Например, используйте `machine_1`, чтобы удалить машину с этим именем. Либо добавьте `machine_*`, чтобы удалить все машины, имя которых начинается с `machine_`.

  Это поле чувствительно к регистру и принимает только буквы, цифры и специальные символы звездочка (*), подчеркивание (_) и дефис (-). Имя не может начинаться со звездочки (*).

d. Выберите целевые группы конечных точек в Инвентаризации сети, где применить правило.

3. Нажмите **Сохранить**.

Просмотр и управление правилами

В разделе **Настройки сети > Очистка автономных компьютеров** отображаются все созданные вами правила. Выделенная таблица содержит следующую информацию:

- Имя правила.
- Количество дней, прошедших с тех пор, как машины отключились.
- Шаблоны имен машин.
- Расположение в инвентаризации сети.
- Количество удаленных машин за последние 24 часа.
- Состояние: включено, отключено или недействительно.

> **Примечание**
> Правило является недействительным, если цели больше не действительны по определенным причинам. Например, виртуальные машины были удалены или у вас больше нет к ним доступа.

Вновь созданное правило включено по умолчанию. Вы можете в любое время включать и отключать правила, используя переключатель «Вкл/Выкл» в столбце **Состояние**.

При необходимости используйте параметры сортировки и фильтрации в верхней части таблицы, чтобы найти конкретные правила.

Чтобы изменить правило:

1. Нажмите на название правила.
2. На странице конфигурации редактируйте детали правила.
3. Нажмите **Сохранить**.

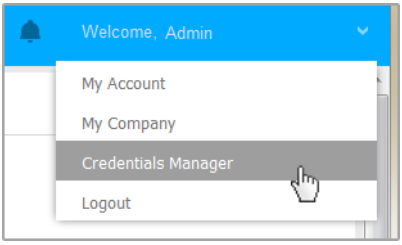
Чтобы удалить одно или несколько правил:

1. Используйте флажки, чтобы выбрать одно или несколько правил.
2. Нажмите кнопку **Удалить** в верхней части таблицы.

6.14. Диспетчер учетных данных (Credentials Manager)

Диспетчер учетных данных позволяет определить необходимые учетные данные для удаленной аутентификации на различных операционных системах в вашей сети.

Чтобы открыть диспетчер учетных данных, нажмите на имя пользователя в правом верхнем углу страницы и выберите **Диспетчер учетных данных**.

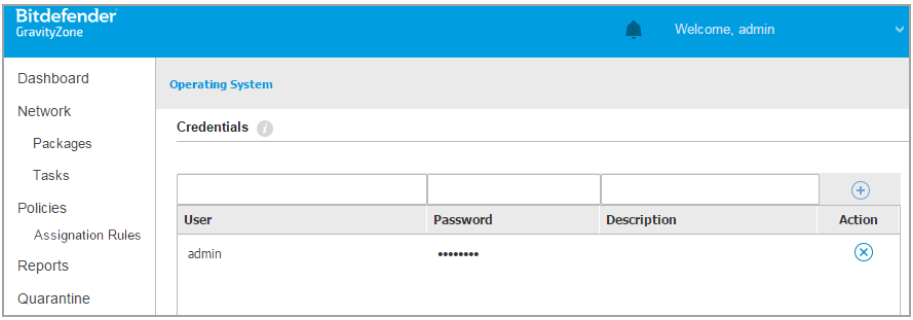


Меню диспетчера учетных данных

6.14.1. Добавление учетных данных в диспетчер учетных данных

С помощью Диспетчера учетных данных можно управлять учетными данными администратора, необходимыми для удаленной аутентификации, во время выполнения задач установки, отправленных на компьютеры и виртуальные машины в вашей сети.

Чтобы добавить набор учетных данных:



Диспетчер учетных данных (Credentials Manager)

1. Введите имя пользователя и пароль учетной записи администратора для каждой требуемой операционной системы в соответствующих полях в верхней части над заголовком таблицы. При желании, вы можете добавить описание, которое поможет вам проще определить каждый аккаунт. Если компьютеры находятся в домене, достаточно ввести учетные данные администратора домена.

   Используйте правила именования Windows при вводе имени учетной записи:

   - Для машин из службы каталогов Active Directory используйте следующий синтаксис: `username@domain.com` и `domain\username`. Чтобы быть уверенным, что введенные учетные данные будут работать, добавьте их в обоих видах (`username@domain.com` и `domain\username`).
   - Для машин из рабочей группы достаточно ввести только имя пользователя без имени рабочей группы.

2. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Новый набор учетных данных будет добавлен в таблицу.

> **Примечание**
> Если вы не указали учетные данные, вам будет необходимо ввести их при запуске задачи установки. Указанные учетные данные автоматически сохраняются в диспетчере учетных данных, так что вам не придется вводить их в следующий раз.

6.14.2. Удаление учетных данных из диспетчера учетных данных

Чтобы удалить устаревшие учетные данные из диспетчера учетных данных:

1. Нажмите на строку таблицы, содержащую учетные данные, которые вы хотите удалить.
2. Нажмите кнопку ⊗ **Удалить** с правой стороны соответствующей строки таблицы. Выбранный аккаунт будет удален.

7. ПОЛИТИКИ БЕЗОПАСНОСТИ (SECURITY POLICIES)

Сразу же после установки, объектам инвентаризации сети присваиваются политики по умолчанию, которые предварительно сконфигурированы с рекомендованными настройками защиты. Вы не можете изменить или удалить политики по умолчанию. Вы можете только использовать их в качестве шаблона для создания новых политик.

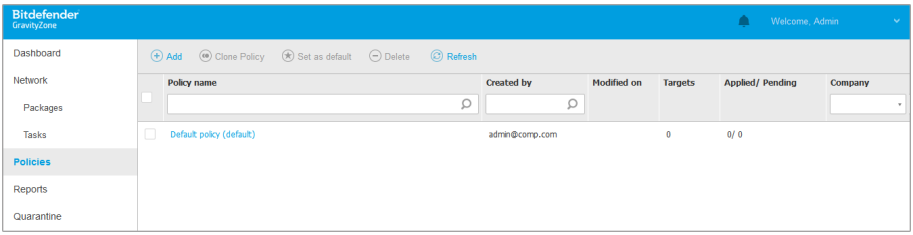
Вот то, что вам нужно знать о политиках:

- Политики создаются на странице **Политики** и назначаются сетевым объектам в разделе **Сеть**.
- Политики могут наследовать некоторые настройки модулей из других политик.
- Можно настроить назначение политик для конечных точек таким образом, что политика может применяться в любое время или только при определенных условиях, на основании местоположения конечной точки. Таким образом, конечная точка может иметь больше назначаемых политик.
- Конечные точки могут иметь одну активную политику одновременно.
- Вы можете назначить политику отдельным конечным точкам или группам конечных точек. При назначении политики также должны быть определены параметры наследования политики. По умолчанию каждая конечная точка наследует политику родительской группы.
- Политики отправляются объектам сети сразу после их создания или модификации. Настройки будут применены к объектам сети менее, чем за минуту (при условии, что они онлайн). Если объект сети не онлайн, настройки будут применены как только он станет онлайн.
- Политика применяется только к установленным модулям защиты.
- Страница **Политики** отображает только следующие виды политик:
  - Политики, созданные вами.
  - Другие политики (например, политики по умолчанию или шаблоны, созданные другими пользователями), которые назначаются конечным точкам под вашей учетной записью.
- Вы не можете редактировать политики, созданные другими пользователями (если владельцы политик не позволяют этого в настройках политики), но вы можете отменить их, назначив требуемым объектам иную политику.

Предупреждение
Только поддерживаемые модули политик будут применяться к требуемым конечным точкам.
Пожалуйста, обратите внимание, что только модуль защиты от вредоносных программ поддерживается серверными операционными системами.

7.1. Управление политиками

Вы можете просматривать и управлять политиками на странице **Политики**.



Страница политик

Существующие политики отобразятся в таблице. По каждой политике вы можете посмотреть:

- Имя политики.
- Пользователя, который создал политику.
- Дату и время последнего изменения политики.

Для детальной настройки политики, отображаемой в таблице:

1. Нажмите кнопку **Колонки** справа от Панель действий
2. Выберите столбцы, которые вы хотите отобразить.
3. Нажмите кнопку **Восстановить**, чтобы вернуться к виду столбцов по умолчанию.

Вы можете сортировать доступные политики, а также осуществлять поиск определенной политики, используя доступные критерии.

7.1.1. Создание политик

Вы можете создавать политики либо путем добавления новой или дублирования (клонирования) существующей политики.

Для создания политики безопасности:

1. Перейдите на страницу **Политики**.
2. Выберите способ создания политики:
   - **Добавить новую политику**.
     - Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Эта команда создает новую политику, начиная с шаблона политики по умолчанию.
   - **Копировать существующие политики**.
     a. Установите флажок на политике, которую вы хотите продублировать.
     b. Нажмите кнопку **Копировать** в верхней части таблицы.
3. Настройте параметры политики. Для получения дополнительной информации перейдите к «Политики компьютеров и виртуальных машин» (p. 146).
4. Нажмите **Сохранить**, чтобы создать политику и вернуться к списку политик.

7.1.2. Назначение политик

Конечным точкам первоначально назначена политика по умолчанию. После того, как вы создали необходимую политику на странице **Policies**, вы можете назначить ее конечным точкам.

Вы можете назначить политику двумя способами:

- Назначение на основе устройства, означает ручной выбор конечных точек, которым вы назначите политику. Эти политики также известны, как политики устройств.
- Назначение на основе правил, означает, что политика назначается управляемой конечной точке, сетевые настройки которой соответствуют заданным условиям существующего правила присвоения.

Примечание
Вы можете назначить только те политики, которые были созданы вами. Чтобы назначить политику, созданную другим пользователем, вы должны ее сначала клонировать в разделе **Политики**.

Назначение политик устройств

В GravityZone можно назначать политики несколькими способами:

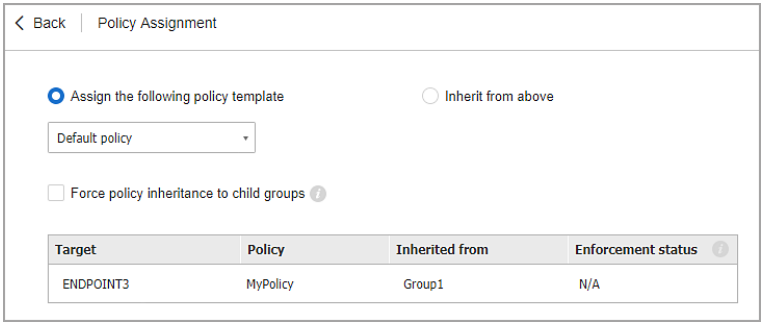
- Назначить политику непосредственно на цель.
- Назначить политику родительской группы через наследование.
- Принудительное наследование политики.

По умолчанию каждая конечная точка или группа конечных точек наследует политику родительской группы. Если вы измените политику родительской группы, будут затронуты все потомки этой группы, кроме тех, у которых есть принудительная политика.

Чтобы назначить политику устройства:

1. Перейдите в раздел **Сеть**.
2. Выберите целевые конечные точки Вы можете выбрать одну или несколько конечных точек или групп конечных точек.
3. Нажмите кнопку **Назначить политику** в верхней части рабочей области или выберите параметр **Назначить политику** в контекстном меню.

   Страница **Назначение политики** отображается:



Назначение политик

4. Проверьте таблицу с целевыми конечными точками. Для каждой конечной точки вы можете просмотреть:
   - Назначенная политика.
   - Родительская группа, от которой целевой объект наследует политику.

Если группа применяет политику, вы можете щелкнуть на её имя, чтобы просмотреть страницу **Назначение политики** с этой группой в качестве цели.

- Статус исполнения.

  Данный статус показывает, принуждает ли данная группа наследование политик дочерним группам, либо сама является принуждаемой.

  Обратите внимание на цели с принудительной политикой (статус **Принудительно**). Данные политики заменить нельзя. В таком случае отображается предупреждение.

5. В случае предупреждения нажмите на ссылку **Исключить эти цели** , чтобы продолжить.
6. Выберите один из доступных вариантов назначения политики:
   - **Назначьте следующий шаблон политики**- назначить конкретную политику непосредственно конечным точкам.
   - **Наследовать по убыванию** - использовать политику родительской группы.
7. Если вы решили назначить шаблон политики:
   a. Выберите политику из выпадающего списка.
   b. Выберите **Принудительное наследование политик дочерним группам** , чтобы добиться следующего:
      - Назначьте политику всем потомкам целевых групп, без исключения.
      - Запретите изменять его из других мест в иерархии.

      В новой таблице представлено рекурсивное отображение всех затронутых конечных точек и их групп, а также политики, которые будут заменены.
8. Нажмите **Завершить**, чтобы сохранить и применить изменения. В противном случае нажмите **Назад** или **Отмена** , чтобы вернуться на предыдущую страницу.

При завершении, политики сразу же направляются к конечным точкам. Настройки на конечных точках вступают в силу менее чем за минуту (при условии, что они онлайн). Если конечная точка не в сети, настройки будут применены, как только она появится в сети.

Для проверки успешного применения политики:

1. На странице **Сеть** щелкните имя интересующей вас конечной точки. Control Center отобразит окно **Информация**.
2. Проверьте раздел **Политика**, чтобы просмотреть статус текущей политики. Должно отображаться как **Применено**.

Другой способ проверить статус назначения - из деталей политики:

Назначение политик на основе правил

Страница **Политики > правила назначения** позволяет вам определять правила назначения политик для определенного местоположения. Например, вы можете применять более строгие правила брандмауэра, если пользователь подключается к сети Интернет из-за пределов компании, или вы можете задать более частое сканирование системы за пределами компании.

Что вам нужно знать о правилах назначения политик:

- Конечные точки могут иметь только одну активную политику одновременно.
- Применяемая политика перезапишет установленную на конечной точке политику устройства.
- Если ни одно из правил назначения не применимо, тогда будет назначена политика устройства.
- Правила упорядочены и обрабатываются по приоритетам, `1` имеет самый высокий приоритет. Вы можете иметь несколько правил для одного объекта. В этом случае будет применяться первое правило, которое соответствует активным настройкам соединения на определенной конечной точке.

  Например, если конечная точка соответствует пользовательскому правилу с приоритетом 4, а правило местонахождения имеет приоритет 3, будет применено правило местонахождения.

Предупреждение
Убедитесь, какие параметры вы считаете чувствительными - исключения, соединения или детальные настройки прокси - при создании правил.
Лучшие практики рекомендуют использовать наследование политик, чтобы сохранять критические параметры политик устройств также в политиках, назначаемых правилами.

Для создания нового правила:

1. Перейдите на страницу **Правила назначения** .
2. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.
3. Выберите тип правила:
   - Правило местонахождения
   - Правило для пользователя
4. Настройте нужные параметры правила.
5. Нажмите **Сохранить**, чтобы сохранить изменения и применить правило политики для выбранных конечных точек.

Чтобы изменить параметры существующего правила:

1. На странице **Правила назначения** найдите правило, которое вас интересует и нажмите на него для редактирования.
2. Настройте нужные параметры правила.
3. Нажмите **Сохранить**, чтобы применить изменения и закрыть окно. Чтобы выйти из окна без сохранения изменений, нажмите кнопку **Отменить**.

Если вы больше не хотите использовать правило, выберите правило и нажмите кнопку ⊖ **Удалить** в верхней части таблицы. Вам будет предложено подтвердить свои действия, нажатием кнопки **Да**.

Чтобы быть уверенным, что отображается актуальная информация, нажмите кнопку ⟳ **Обновить** в верхней части таблицы.

Настройка правил местоположения

Местонахождение сетевого сегмента определяется одним или несколькими сетевыми параметрами, такими как используемый шлюз, DNS-сервер для разрешения URL-адресов или подсеть IP-адресов. Например, вы можете определить местоположение по сети компании, набору серверов отдела.

В конфигурационном окне правила, выполните следующие действия:

1. Введите подходящее имя и описание правила, которое хотите создать.
2. Установите приоритет правила. Правила отсортированы по приоритетам, правило с приоритетом 1 имеет наивысший приоритет. Одинаковый приоритет не может быть установлен дважды.

3. Выберите политику, для которой вы создаете правило назначения.
4. Задайте местоположения, по которым применяется правило.
   a. Выберите тип сетевых настроек из меню в верхней части таблицы месторасположений. Доступны следующие типы:

Тип	Значение
Диапазон IP / IP-адресов	Укажите IP-адреса сети или подсетей. Для подсетей используйте формат CIDR. Например: `10.10.0.12` или `10.10.0.0/16`
Адрес шлюза	IP-адрес шлюза
Адрес сервера WINS	IP-адрес сервера WINS **Важно** Этот параметр не применяется в системах Linux и Mac.
Адрес сервера DNS	IP-адрес сервера DNS
DHCP-суффикс подключения DNS	DNS-имя без имени хоста для конкретного соединения DHCP Например: `hq.company.biz`
Конечная точка может разрешать имена хостов	Имя хоста. Например: `fileserv.company.biz`
Тип сети	Беспроводное/Ethernet-соединение При выборе беспроводного соединения, вы также можете добавить сетевой идентификатор SSID. **Важно** Этот параметр не применяется в системах Linux и Mac.
Имя хоста	Имя хоста For example: `cmp.bitdefender.com`

Тип	Значение

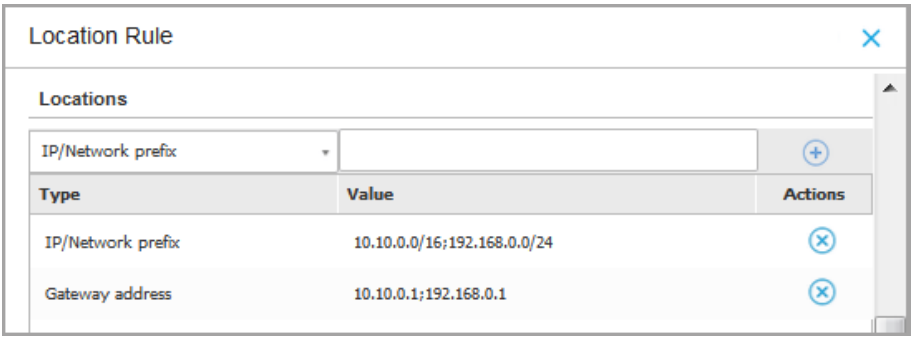
	Важно
	Вы также можете использовать подстановочные символы. Звездочка (*) заменяет ноль или более символов, а знак вопроса (?) заменяет ровно один символ. Примеры:
	`*.bitdefender.com`
	`cmp.bitdefend??.com`

b. Введите значение для выбранного типа. Там, где это применимо, вы можете ввести несколько значений в выделенном поле, разделенных точкой с запятой (;) и без дополнительных пробелов. Например, когда вы вводите `10.10.0.0/16;192.168.0.0/24`, правило будет относится к конечным точкам с IP-адресами, соответствующими любой из этих подсетей.

Предупреждение
Вы можете использовать только один тип сетевых настроек для каждого из правил месторасположения. Например, если вы добавили местоположение с помощью **IP/network prefix**, вы не можете использовать эту же настройку еще раз в этом же правиле.

c. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.

Сетевые настройки конечных точек должны полностью соответствовать всем условиям, заданным при определении местоположения, чтобы правило применилось к ним. Например, для идентификации офисной локальной сети можно задать шлюз, тип сети и сервер DNS; кроме того, при добавлении подсети, вы сможете определить отдел в локальной сети компании.



Правило местоположения

Нажмите поле **Значение** для редактирования существующих критериев, а затем нажмите кнопку Войти, чтобы сохранить изменения.

Чтобы удалить местоположение, выберите его и нажмите кнопку ⊗ **Удалить**.

5. Вы можете исключить определенные местоположения из правил. Чтобы создать исключение для определенного местоположения, которое будет исключено из правила:
   a. Отметьте чек-бокс **Исключения** в таблице местоположений.
   b. Выберите тип сетевых настроек в меню в верхней части таблицы исключений. Для получения более подробной информации о параметрах, пожалуйста, обратитесь к«Настройка правил местоположения» (p. 140).
   c. Введите значение для выбранного типа. Вы можете ввести несколько значений в выделенном поле, разделенных точкой с запятой (;) без дополнительных пробелов.
   d. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.

   Сетевые настройки конечных точек должны полностью соответствовать всем условиям, предусмотренным в таблице исключений, чтобы исключить применение.

   Нажмите поле **Значение** для редактирования существующих критериев, а затем нажмите кнопку Войти, чтобы сохранить изменения.

   Чтобы удалить исключение, нажмите кнопку ⊗ **Удалить** в правой части таблицы.

6. Нажмите **Сохранить**, чтобы сохранить правило назначения и применить его.

   После создания правила расположения оно автоматически применится ко всем управляемым конечным точкам.

Настройка правила для пользователя

Важно

- Вы можете создать правила для пользователей, только если выполнена интеграция с Active Directory.
- Вы можете создать правила для пользователей только для групп и пользователей из Active Directory. Правила, основанные на группах Active Directory, не поддерживаются в системах Linux.

В конфигурационном окне правила, выполните следующие действия:

1. Введите подходящее имя и описание правила, которое хотите создать.
2. Установка приоритета. Правила отсортированы по приоритетам, правило с приоритетом 1 имеет наивысший приоритет. Одинаковый приоритет не может быть установлен дважды.
3. Выберите политику, для которой вы создаете правило назначения.
4. В разделе **Targets**, выберите требуемых пользователей и группы безопасности, к которым вы хотите применить правило политики. Вы можете увидеть то, что выбрали, в таблице справа.
5. Нажмите **Сохранить**.

   После создания, правило для пользователей применяется к управляемым конечным точкам при входе пользователя в систему.

7.1.3. Изменение настроек политики

Параметры политики можно настроить изначально при ее создании. Позже вы можете изменить их по мере необходимости в любое удобное время.

Примечание
По умолчанию, только пользователь, создавший политику, может изменить ее. Чтобы внести изменения, владелец политики должен выбрать опцию **Разрешить**

другим пользователям изменять эту политику на странице политик в разделе **Подробности**.

Чтобы изменить настройки существующей политики:

1. Перейдите на страницу **Политики**.
2. Найдите в списке необходимую политику и нажмите для редактирования на ее имя.
3. Настройте необходимые параметры политики. Для получения дополнительной информации перейдите к «Политики компьютеров и виртуальных машин» (p. 146).
4. Нажмите **Сохранить**.

   Политики отправятся объектам сети сразу же после изменения объектов, которым они назначены, или после изменения параметров политик. Настройки будут применены к объектам сети менее чем за минуту (при условии, что они онлайн). Если объект сети не онлайн, настройки будут применены как только он станет онлайн.

7.1.4. Изменение имен политик

Политики должны иметь подходящие имена, чтобы вы или другой администратор могли их быстро и просто идентифицировать.

Чтобы переименовать политику:

1. Перейдите на страницу **Политики**.
2. Нажмите на имя политики. Откроется страница политики.
3. Введите новое имя политики.
4. Нажмите **Сохранить**.

Примечание
Имя политики должно быть уникальным. Вы должны присваивать разные имена для каждой новой политики.

7.1.5. Удаление политик

Если политика вам больше не нужна, удалите ее. После удаления политики, объектам сети, к которым она применялась, будет назначена политика родительской группы. Если никакая другая политика не будет применена,

объекту будет назначена политика по умолчанию. При удалении политики с разделами, унаследованными от других политик, настройки унаследованных разделов вернутся к дочерним.

Примечание
По умолчанию, только пользователь, создавший политику, может ее удалить. Чтобы внести изменения, владелец политики должен выбрать опцию **Разрешить другим пользователям изменять эту политику** на странице политик в разделе **Подробности**.

Чтобы удалить политику:

1. Перейдите на страницу **Политики**.
2. Установите флажок на политике, которую необходимо удалить.
3. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы. Вы должны будете подтвердить ваши действия, нажав **Да**.

7.2. Политики компьютеров и виртуальных машин

Параметры политики можно настроить изначально при ее создании. Позже вы можете изменить их по мере необходимости в любое удобное время.

Чтобы настроить параметры политики:

1. Перейдите на страницу **Политики**.
2. Нажмите на имя политики. Откроется страница настройки политики.
3. Настройте необходимые параметры политики. Настройки расположены в следующих разделах:
   - Основные
   - Защита от вредоносного ПО
   - Sandbox Analyzer
   - Брандмауэр
   - Защита сети
   - Управление исправлениями
   - Контроль устройств
   - Ретранслятор
   - Защита Exchange
   - Шифрование
   - Защита хранилища
   - Инциденты Sensor

- Управление рисками

Для перемещения по разделам используйте меню в левой части страницы.

4. Нажмите **Сохранить**, чтобы сохранить изменения и применить их на выбранных компьютерах. Чтобы покинуть страницу политик без сохранения изменений, нажмите **Отменить**.

Примечание
Чтобы узнать о работате с политиками, обратитесь к «Управление политиками» (p. 135).

7.2.1. Основные

Общие настройки помогут вам управлять настройками пользовательского интерфейса, парольной защитой, настройками прокси-сервера, настройками привилегированных пользователей, параметрами связи и обновлений для определенных конечных точек.

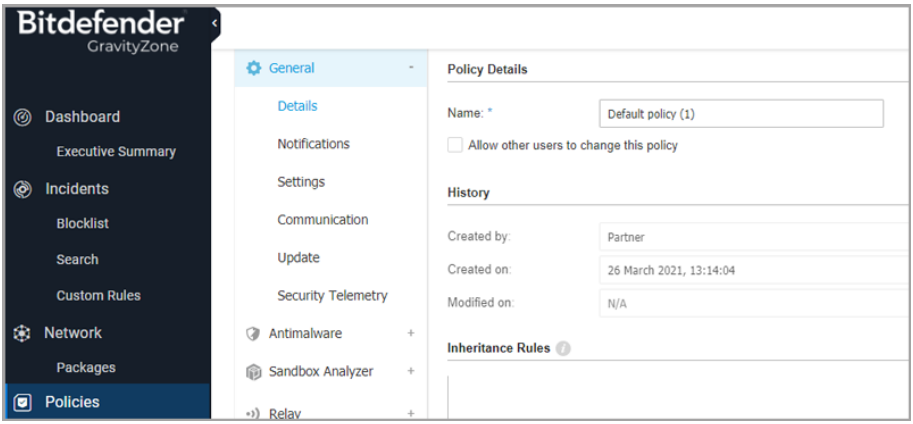
Настройки объединены в следующие разделы:

- Подробная информация
- Уведомления
- Настройки
- Коммуникации
- Обновления
- Телеметрия безопасности

Подробная информация

Страница **Подробности** содержит общие сведения о политике:

- Название политики
- Пользователь, который создал политику
- Дата и время, когда политика была создана
- Дата и время последнего изменения политики



Политики компьютеров и виртуальных машин

Вы можете переименовать политику, введя новое имя в соответствующем поле и нажав кнопку **Сохранить** в нижней части страницы. Политики должны иметь подходящие имена, чтобы вы или другой администратор могли их быстро и просто идентифицировать.

Примечание
По умолчанию, только пользователь, создавший политику, может изменить ее. Чтобы внести изменения, владелец политики должен выбрать опцию **Разрешить другим пользователям изменять эту политику** на странице политик в разделе **Подробности**.

Правила наследования

Вы можете задать разделы, которые будут наследовать параметры других политик. Чтобы это сделать:

1. Выберите модуль и раздел, для которого требуется включить наследование. Все разделы будут наследовать параметры, за исключением **Общее > Подробности**.
2. Выберите интересующий вас раздел политики, для которого вы хотите включить наследование.
3. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.

Если исходная политика удаляется, унаследованные точки и настройки разделов вернутся к дочерним настройкам.

Унаследованные разделы не могут дополнительно наследоваться другими политиками. Рассмотрим следующий пример:

Политика А наследует настройки раздела **Защита от вредоносных программ > По требованию** от политики Б. Политика В уже не сможет наследовать настройки раздела **Защита от вредоносных программ > По требованию** от политики А.

Информировать о технической поддержке

Вы можете настроить контактную информацию и информацию о технической поддержке, которая будет доступна в агенте безопасности в разделе **О программе**, заполнив соответствующие поля.

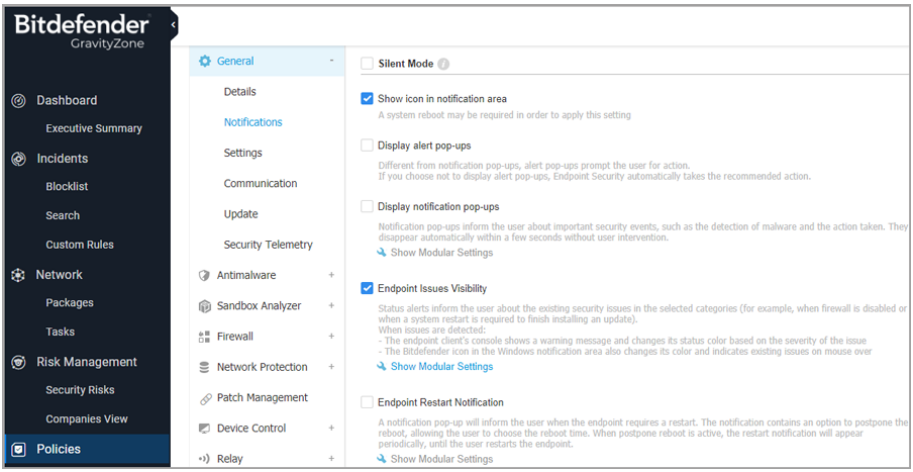
Чтобы настроить адрес электронной почты в окне **О программе**, чтобы он открывал приложение электронной почты по умолчанию на конечной точке, необходимо добавить его в поле с пометкой "mailto:"**Электронная почта**. Пример: `mailto: name@domain.com`.

Пользователь сможет получить данную информацию из агента безопасности, нажав правую кнопку мыши на значке Bitdefender в системном трее и выбрав раздел **О программе**.

Уведомления

В этом разделе вы можете настроить параметры отображения интерфейса пользователя агента безопасности Bitdefender в доступном и интуитивно понятном виде.

Всего лишь одним щелчком мыши вы можете включить или выключить типы уведомлений, оставив только те, которые действительно имеют значение для вас. Кроме того, на той же странице, вы получаете полный контроль над видимостью проблем конечных точек.



Политики - Настройки отображения

- **"Без оповещений".** Установите флажок, чтобы включить или выключить режим "Без оповещений" (Silent Mode). Режим "Без оповещений" разработан чтобы запретить вмешательство пользователей в действия агента безопасности. При включении режима "Без оповещений" вносятся следующие изменения в конфигурацию политики:
  - Опции **Показать значок в области уведомлений**, **Отображать всплывающие уведомления** и **Отображать всплывающие окна с предупреждениями** в этом разделе будут отключены.
  - Если уровень защиты файрвола установлен в **Правила и вопросы** или **Правила, известные файлы и вопросы** режим, то он будет изменен на **Набор правил, известные файлы и разрешения**. В противном случае, настройки уровня защиты останутся неизменными.
- **Отображать значок в области уведомлений.** Выберите эту опцию, чтобы показать значок Bitdefender в области уведомлений (также известной как системный трей). Значок информирует пользователей о состоянии их защиты, изменяя свой внешний вид и отображая соответствующие всплывающие уведомления. Кроме того, пользователи могут щелкнуть правой кнопкой мыши для быстрого открытия главного окна агента безопасности или окна **О программе**.

- **Отображать всплывающие предупреждения.** Пользователи информируются через всплывающие уведомления о событиях безопасности, которые требуют ответных действий. Если вы установили - не отображать всплывающие уведомления, то агент безопасности автоматически предпримет рекомендованные действия. Всплывающие предупреждения генерируются в следующих ситуациях:
  - Если настройки файрвола требуют запросить действия пользователя для неизвестных программ, требующих доступ к сети или в Интернет.
  - Если Расширенное управление угрозами/Система обнаружения вторжений (Advanced Threat Control / Intrusion Detection System) включены, каждый раз, когда обнаружено потенциально опасное приложения.
  - Если сканирование устройств включено, каждый раз, когда внешнее устройство хранения подключается к компьютеру. Вы можете настроить данные параметры в разделе **Защита от вредоносных программ > По требованию**.
- **Отображать всплывающие уведомления.** В отличие от всплывающих предупреждений, всплывающие уведомления информируют пользователей о различных событиях безопасности. Всплывающие уведомления будут автоматически исчезать в течение нескольких секунд без вмешательства пользователя.

  Выберите **Отображать всплывающие уведомления**, затем нажмите ссылку **Показать модульные настройки**, чтобы выбрать события, которые будут отображаться пользователям. Есть три типа всплывающих уведомлений, в зависимости от серьезности событий:
  - **Info**. Пользователи информируются о существенных событиях безвредных для безопасности. Например, о приложении, которое подключилось к сети Интернет.
  - **Низкий**. Пользователи информируются о важных событиях безопасности, которые могут потребовать вмешательства. Например, сканирование On-Access обнаружило угрозу и файл был удален или помещен в карантин.
  - **Критичный**. Эти всплывающие уведомления информируют пользователей об опасных ситуациях, например, сканирование On-Access обнаружило угрозу, но действие политики по умолчанию -

Не предпринимать действий (не предпринимать действий), в результате вредоносная программа по-прежнему присутствует на конечной точке, или процесс обновления не может быть завершен.

Установите соответствующий флажок, связанный с набранным именем, для такого рода всплывающих уведомлений во всех модулях одновременно. Установите флажки, связанные с отдельными модулями, для включения или отключения конкретных уведомлений.

Например, после выбора флажков, связанных с Sandbox Analyzer, Bitdefender Endpoint Security Tools информирует пользователя о том, что файл отправляется на поведенческий анализ.

Список модулей может варьироваться в зависимости от вашей лицензии.

- **Видимость проблем конечных точек.** В этом случае пользователи решают самостоятельно, когда их конечное устройство имеет проблемы с конфигурацией безопасности или при других угрозах безопасности, на основе предупреждений о состоянии. Например, пользователи могут видеть, когда возникают проблемы, связанные с их защитой от вредоносного ПО, например: отключение модуля сканирования или когда полное сканирование системы запущено. Пользователи информируются о состоянии их защиты в двух случаях:
  - Проверьте область уведомлений главного окна, которая отображает соответствующие сообщения о состоянии, и меняет свой цвет в зависимости от серьезности проблем безопасности. Пользователи имеют возможность просматривать возникающие проблемы более подробно, нажав соответствующую кнопку.
  - Проверьте иконку Bitdefender в системном трее, которая меняет свой внешний вид при обнаружении проблем.

  Агенты безопасности Bitdefender используют следующие цветовые схемы в области уведомлений:
  - Зеленая: Проблем не обнаружено.
  - Желтая: Конечное устройство имеет незначительные проблемы, влияющие на безопасность. Пользователи могут не прерывать свою текущую работу для решения таких проблем.
  - Красная: Конечное устройство имеет критическую проблему, требующую немедленной реакции пользователя.

Выберите **Видимость проблем конечной точки**, затем нажмите ссылку **Показать модульные настройки**, чтобы настроить оповещения о состоянии, отображаемые в интерфейсе агентов Bitdefender.

Для каждого модуля вы можете выбрать отображение уведомлений как предупреждений, как критических проблем, или не показывать вообще. Ниже приведены возможные варианты:

- **Общее**. Предупреждение о состоянии генерируется каждый раз при необходимости перезапуска системы во время или после установки продукта, а также, когда агент безопасности не может подключиться к облачному сервису Bitdefender.
- **Защита от вредоносных программ**. Предупреждении о состояние генерируется в следующих случаях:
  - Сканирование по запросу включено, но слишком много локальных файлов пропущено.
  - Прошло определенное количество дней с момента последнего полного сканирования системы, выполненного на компьютере.

    Вы можете задать, как отображать оповещения и задать количество дней для предупреждения после последнего полного сканирования системы.
  - Для завершения процесса лечения требуется перезагрузка системы.
- **Завершение**. Предупреждения о состоянии генерируется, когда модуль файрвола отключен.
- **Управление контентом**. Предупреждения о состоянии генерируется, когда модуль контентной фильтрации отключен.
- **Обновить**. Предупреждения о состоянии генерируется каждый раз, когда требуется перезагрузка системы для завершения обновлений.

- **Уведомление о перезапуске конечной точки.** Эта опция отображает предупреждение о перезапуске на конечной точке каждый раз, когда требуется перезагрузка системы из-за изменений, внесенных в конечную точку модулями GravityZone, выбранными в модульных настройках.

  Примечание
  Конечные точки, требующие перезагрузки системы, имеют определенный значок состояния ( ) в инвентаре GravityZone.

Вы можете дополнительно настроить оповещения о перезапуске, нажав **Показать модульные настройки**. Доступны следующие опции:

– **Перезапуск** - Выберите этот параметр, чтобы активировать уведомления о перезапуске обновления агента.

– **Управление патчами** - Выберите этот параметр, чтобы активировать уведомления о перезапуске установки патчей.

Примечание
Вы также можете установить ограничение на сколько часов пользователь может отложить перезапуск. Для этого выберите **Автоматический перезапуск машины после** и введите значение от 1 до 46.

Предупреждение о перезапуске требует от пользователя выбора одного из следующих действий:

– **Перезагрузить сейчас**. В этом случае система перезапустится автоматически.

– **Отложить перезагрузку**. В этом случае уведомление о перезапуске будет периодически появляться до тех пор, пока пользователь не перезапустит систему или пока не пройдет время, установленное администратором компании.

Настройки

В данном разделе вы можете изменить следующие настройки:

- **Настройка пароля.** Чтобы предотвратить деинсталляцию защиты с компьютеров пользователями с правами администратора, вы должны установить пароль.

  Пароль деинсталляции должен быть задан до процесса установки, путем настройки инсталляционного пакета. Если вы это сделали, то нажмите **Сохранить настройки установки**, чтобы сохранить текущий пароль.

  Чтобы установить пароль или изменить текущий пароль, выберите **Включить пароль** и введите желаемый пароль. Чтобы снять парольную защиту, выберите **Отключить пароль**.

- **Настройка прокси**

  Если ваша сеть находится за прокси-сервером, вам необходимо задать настройки прокси, которые позволят вашим конечным устройствам

соединяться с компонентами решения GravityZone. В этом случае вам необходимо разрешить опцию **Конфигурация прокси** и заполнить требуемые параметры.

- **Сервер** - введите IP-адрес прокси-сервера
- **Порт** - введите порт, используемый для подключения к прокси-серверу.
- **Имя пользователя** - введите имя пользователя, распознаваемое прокси-сервером.
- **Пароль** - введите корректный пароль указанного пользователя.

- **Привилегированный пользователь**

  Модуль привилегированных пользователей разрешает предоставление администраторских прав для уровня конечных устройств, что позволяет пользователям конечных устройств иметь доступ и модифицировать настройки политик через локальную консоль посредством интерфейса Bitdefender Endpoint Security Tools.

  Если вы хотите разрешить конечным устройствам работать с правами привилегированных пользователей, для начала вам необходимо включить данный модуль в состав агента безопасности, устанавливаемого на выбранном конечном устройстве. После этого вам необходимо настроить параметры привилегированных пользователей в политике, применяемой к этим конечным точкам:

  Важно
  Модуль привилегированных пользователей доступен только для серверов и рабочих станций, работающих под управлением Windows.

  1. Разрешить опцию **Power User**.
  2. Задать пароль привилегированного пользователя в поле ниже.

     Пользователи, пытающиеся получить доступ к режиму привилегированных пользователей на локальном конечном устройстве, должны будут ввести заданный пароль.

  Для доступа к режиму привилегированных пользователей, пользователи должны нажать правой кнопкой мыши на значок Bitdefender в системном трее и выбрать **Пользователь** из контекстного меню. После ввода пароля в окне входа, консоль будет отображать применяемые в настоящее время параметры политики, которые пользователь конечного устройства сможет просмотреть или модифицировать.

Примечание
Только некоторые функции безопасности могут быть доступны локально с помощью консоли привилегированных пользователей, касающиеся модулей защиты от вредоносных программ (Antimalware), файрвола (Firewall), контроля содержимого (Content Control) и управления устройством (Device Control).

Чтобы вернуть изменения, сделанные в режиме привилегированного пользователя:

– Откройте в Control Center шаблон политики, назначенной конечной точке, с правами привилегированного пользователя и нажмите **Сохранить**. В этом случае оригинальные настройки будут переприменены к целевой конечной точке.

– Примените новую политику конечной точке с правами привилегированного пользователя.

– Зайдите локально на конечное устройство, откройте консоль привилегированного пользователя и нажмите **Синхронизировать**.

Чтобы быстро найти конечные точки с модифицированной политикой в режиме привилегированного пользователя:

– В разделе **Сеть** нажмите меню **Фильтры** и выберите опцию **Отредактировано пользователем** на вкладке **Полиика**.

– В разделе **Сеть** нажмите на интересующее вас конечное устройство для отображения окна **Информация**. Если политика была изменена в режиме привилегированного пользователя, уведомление будет отображаться в разделе **Общее** > **Политика**.

Важно
Модуль привилегированного пользователя специально разработан для устранения неполадок, что позволяет администратору сети легко просматривать и изменять параметры политик на локальном компьютере. Назначение прав доступа привилегированного пользователя другим пользователям в компании должно быть ограничено уполномоченным персоналом, чтобы гарантировать, что политики безопасности всегда применялись на всех конечных точках сети компании.

- **Параметры**

  В этом разделе вы можете задать следующие параметры:

- **Удалять старые события (дни).** Агент безопасности Bitdefender ведет подробный журнал событий, касающихся его деятельности на компьютере (в том числе компьютерной активности, контролируемой модулем управления контентом). По умолчанию, из журнала удаляются события старше 30 дней. Если вы хотите изменить этот интервал, выберите другой вариант из меню.
- **Отправлять отчеты о сбоях в Bitdefender.** Выберите этот параметр, чтобы отчеты о сбоях агента безопасности отправлялись в лабораторию Bitdefender для анализа. Отчеты помогут нашим инженерам выяснить, что вызвало проблему и предотвратить ее повторное возникновение. Никакая персональная информация не будет отправлена.

Примечание
Для получения информации о том, как эти настройки нарушают правила HIPAA, обратитесь к разделу "GravityZone и HIPAA" в Руководстве по установке.

Коммуникации

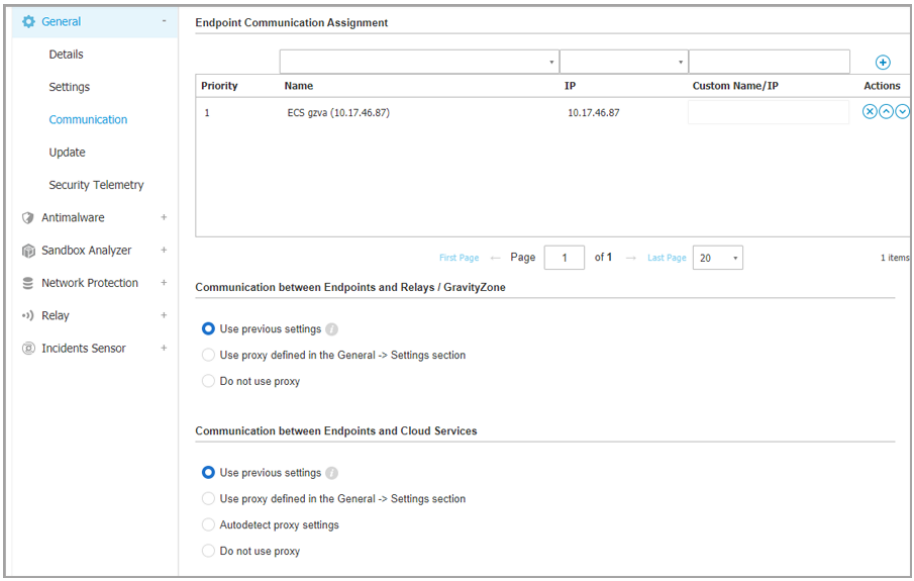
В этом разделе вы можете назначить одну или несколько машин-ретрансляторов для требуемых конечных точек, а затем настроить прокси-сервер для связи между этими конечными точками и GravityZone.

Назначение коммуникационных параметров конечной точке

При использовании нескольких агентов-ретрансляторов в сети, вы можете назначить выбранным компьютерам взаимодействие с одним или несколькими конечными точками-ретрансляторами с помощью политики.

Чтобы назначить конечную точку-ретранслятор выбранным компьютерам:

1. В окне **Назначение связи конечной точки**, нажмите на поле **Имя**. Отобразится список конечных точек-ретрансляторов, обнаруженных в вашей сети.
2. Выберите объект.



Политики - Настройки связи

3. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.

   Конечная точка-ретранслятор добавится в список. Все выбранные компьютеры будут общаться с Control Center через указанную конечную точку-ретранслятор.

4. Выполните те же шаги, чтобы добавить несколько ретрансляторов при их наличии.

5. Вы можете настроить приоритет использования конечных точек-ретрансляторов с помощью стрелок вверх ⌃ и вниз ⌄, имеющихся справа от каждого объекта. Связь выбранных компьютеров будет осуществляться через объект, размещенный вверху списку. Когда связь с этим объектом будет потеряна, использоваться будет следующий объект списка.

6. Для удаления одного объекта из списка нажмите на соответствующую кнопку ⊗ **Удалить** в правой части таблицы.

Связь между конечной точкой и ретранслятором / GravityZone

В этом разделе вы можете настроить параметры прокси-сервера для обмена данными между конечными точками и назначенными машины-ретрансляторами или между конечными точками и GravityZone Control Center (если ретранслятор не назначен):

- **Сохранить настройки установки**, чтобы использовать параметры прокси-сервера, определенные в установочном пакете.
- **Использовать прокси, определенный в общем разделе**, чтобы использовать параметры прокси-сервера, определенные в текущей политике в разделе **Общее > Настройки**.
- **Не использовать**, когда целевые конечные точки не взаимодействуют с определенными компонентами GravityZone через прокси-сервер.

Связь между конечными точками и облачными сервисами

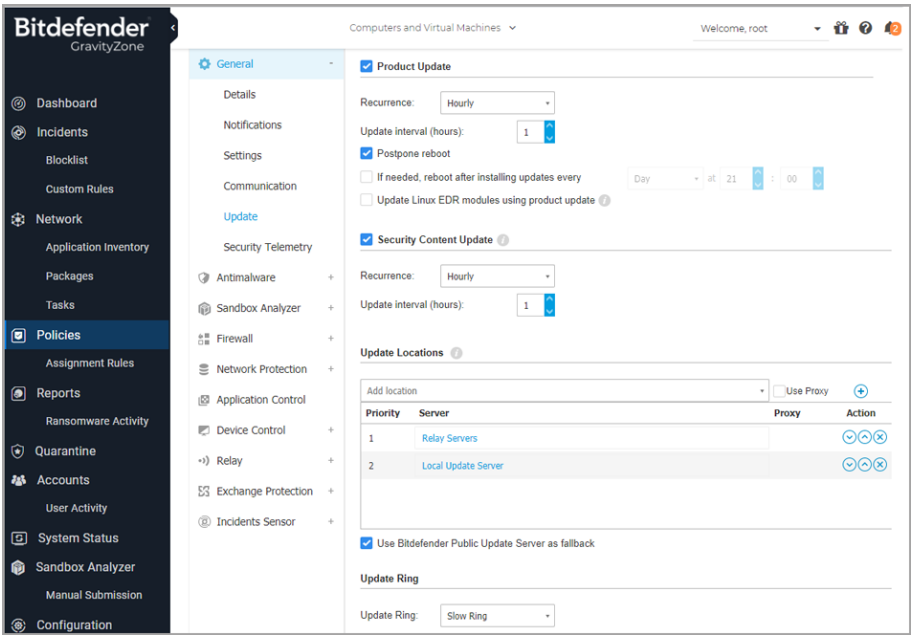
В этом разделе вы можете настроить параметры прокси-сервера для связи между конечными точками и облачным сервисом Bitdefender:

- **Сохранить настройки установки**, чтобы использовать параметры прокси-сервера, определенные в установочном пакете.
- **Использовать прокси, определенный в общем разделе**, чтобы использовать параметры прокси-сервера, определенные в текущей политике в разделе **Общее > Настройки**.
- **Не использовать**, когда целевые конечные точки не взаимодействуют с определенными компонентами GravityZone через прокси-сервер.

Обновления

Обновления являются очень важной деталью, которая позволяет противодействовать новейшим угрозам. Bitdefender публикует все обновления продукта и механизмов защиты через серверы Bitdefender в Интернете. Все обновления зашифрованы и имеют цифровую подпись, чтобы их нельзя было подделать. Когда доступно новое обновление, агент безопасности Bitdefender проверяет цифровую подпись обновления для аутентификации и содержимое пакета для обеспечения целостности. Затем каждый файл обновления анализируется, и его версия проверяется на соответствие установленной. Более новые файлы загружаются локально и проверяются на соответствие хэшу MD5, чтобы убедиться, что они не изменены. В этом разделе вы можете

настроить агент безопасности Bitdefender и параметры обновления механизмов защиты.



Политики - Параметры обновления

- **Обновление продукта.** Агент безопасности Bitdefender автоматически проверяет, загружает и устанавливает обновления каждый час (настройки по умолчанию). Автоматическое обновление выполняется в фоновом режиме.
  - **Возобновление**. Чтобы изменить периодичность автоматических обновлений, выберите другую опцию из меню и настройте ее в соответствии с вашими потребностями в последующих полях.
  - **Отложить перезагрузку**. Некоторые обновления для установки и корректной работы требуют перезагрузки системы. По умолчанию продукт будет продолжать работать со старыми файлами до перезапуска компьютера, после чего будут применены самые последние обновления. Уведомление в пользовательском интерфейсе будет предлагать пользователю перезагрузить систему всякий раз, когда

этого потребует обновление. Рекомендуется оставить этот параметр включенным. В противном случае система автоматически перезагрузится после установки необходимого обновления. Пользователи будут уведомлены о необходимости сохранить свою работу, но перезагрузка не может быть отменена.

– Если вы выберете отложенную перезагрузку, вы можете установить удобное время, когда компьютеры, в случае необходимости, будут перезагружаться автоматически. Такой вариант больше подходит для серверов. Выберите **При необходимости перезагрузите компьютер после установки обновлений.** и укажите удобное время перезагрузки (ежедневно или еженедельно в определенный день, в определенное время суток).

– Для большего контроля над изменением конфигурации и обновлением промежуточного процесса Вы можете настроить лучший агент на Ваших устройствах Linux для выполнения обновлений модуля ядра EDR через **Обновление продукта**.

  Если включен флажок **Обновление продукта** :

  - Если Вы включите флажок **Обновить модули Linux EDR с помощью обновления продукта**, то GravityZone обновит версии ядра с помощью **Обновления продукта**.
  - Если Вы оставите эту опцию отключенной, версии ядра будут обновлены с помощью **Security Content Update**.

  Примечание
  Если Вы включите флажок **Обновить модули Linux EDR с помощью обновления продукта**, но отключите параметр **Обновление продукта**, модули Linux EDR обновляться не будут.

- **Обновление механизмов защиты.** К механизмам защиты относятся статические и динамические меры предотвращения угроз, такие как движки сканирования, модели машинного обучения, эвристические методы, правила, сигнатуры и черные списки. Агент безопасности Bitdefender автоматически проверяет, загружает и устанавливает обновления механизмов защиты каждый час (настройки по умолчанию). Автоматическое обновление выполняется в фоновом режиме. Чтобы изменить периодичность автоматических обновлений, выберите другую

опцию из меню и настройте ее в соответствии с вашими потребностями в последующих полях.

- **Расположение обновлений**. Агент безопасности Bitdefender по умолчанию обновляется из http://upgrade.bitdefender.com. Добавить источник обновлений можно путем выбора предварительно заданных ресурсов в выпадающем меню или путем ввода IP-адреса или имени хоста одного или нескольких серверов обновлений в вашей сети. Настройте их приоритет, используя кнопки вверх и вниз, отображаемые при наведении мыши. Если первый источник обновлений недоступен, будет использован следующий в списке и так далее.

  Чтобы настроить локальный адрес для обновлений:

  1. Введите адрес сервера обновлений в поле **Добавить локацию**. Доступны следующие возможности:
     - Выбор предопределенного источника:
       - **серверы-ретрансляторы** Конечная точка будет автоматически подключаться к назначенным серверам-ретрансляторам.

         Предупреждение
         Серверы ретрансляции не поддерживаются в устаревших операционных системах. Для подробной информации обратитесь в Гид по установке.

         Примечание
         Вы можете проверить назначенные серверы-ретрансляторы в окне **Information**. За более подробной информацией обратитесь к Просмотр сведений о компьютере

       - **update.cloud.2d585.cdn.bitdefender.net**. Это является местом обновления Bitdefender по умолчанию, с которого Bitdefender предоставляет обновления. Это место обновления всегда должно оставаться последним параметром в списке.
     - Введите IP-адрес или имя хоста одного или нескольких серверов обновлений в вашей сети. Используйте один из следующих вариантов синтаксиса:
       - `update_server_ip:port`

- `update_server_name:port`

По умолчанию используется порт 7074.

Флажок **Применять серверы Bitdefender в качестве резервного местоположения** установлен по умолчанию. Если источники обновлений недоступны, будет использоваться резервный вариант.

Предупреждение
Отключение резервного источника остановит автоматическое обновление, что приведет к образованию уязвимостей в вашей сети, если указанные источники обновлений окажутся недоступны.

2. Если клиентские компьютеры подключаются к локальному серверу обновлений через прокси-сервер, выберите **Использовать прокси**.
3. Нажмите кнопку **Добавить** в верхней части таблицы.
4. Используйте стрелки вверх / вниз в колонке **Действие**, чтобы установить приоритет использования источников обновлений. Если первый источник обновлений недоступен, будет использован следующий в списке и так далее.

Чтобы удалить папку из списка, нажмите соответствующую кнопку **Удалить**. Вы можете удалить источник обновлений по умолчанию (не рекомендуется).

- **Последовательность Обновлений .** Вы можете задать последовательность обновлений продуктов по очереди, с помощью порядка обновления:
  - **Медленное обновление** Машины с политикой медленного обновления будут получать обновления в более поздний срок, в зависимости от готовности конечных точек с быстрым обновлением. Это дополнительная мера предосторожности в процессе обновления. Данные настройки приняты по умолчанию.
  - **Быстрое обновление** Машины с политикой быстрого обновления получат новейшие доступные обновления в первую очередь. Данные параметры рекомендуются для некритичных машин, используемых в деятельности компании.

Важно

- Маловероятно, но в случае возникновения проблем с быстрым обновлением у машин с определенными конфигурациями, то они будут исправлены еще до выхода медленных обновлений.
- BEST for Windows Legacy не поддерживает постановку. Устаревшие конечные точки в промежуточном местоположении должны быть перемещены в производственное местоположение.

Телеметрия безопасности

Примечание
Эта функция требует лицензии EDR и доступна только для конечных точек Windows.

Благодаря телеметрии безопасности у Вас появился доступ к данным, связанным с событиями безопасности, так что Вы можете создавать пользовательские корреляции.

Чтобы обеспечить оптимальную производительность и объем данных, агенты отправляют лишь те события, которые имеют отношение к безопасности Вашей сети. Такие события имеют отношение к:

- Процессы: создание, завершение
- Файлы: создание, чтение, изменение, перемещение, удаление
- egistry: создание и удаление ключей, изменение и удаление значения
- Пользовательский доступ: логин
- Сетевые подключения

Агент Bitdefender отправляет эту информацию в стандартном отраслевом формате (JSON,) непосредственно в используемое Вами SIEM-решение. (Splunk).

Чтобы отправить события безопасности из целевых конечных точек в решение SIEM, настройте политику следующим образом:

1. Установите флажок **Телеметрия безопасности**, чтобы включить эту функцию.
2. Выберите SIEM решение, к которому Вы собираетесь подключиться.

3. Обеспечьте URL сервера SIEM.

   Предупреждение
   Требуется протокол HTTPS с TLS 1.2 или выше. В противном случае отправка события завершится неудачей.

4. Выберите **Обойти проверку SSL-сертификата на сборщике HTTP** в случае возникновения ошибки проверки сертификата безопасности, когда Вы все равно хотите использовать сервер SIEM для защиты от ошибки.

   Такая ошибка возникает, если GravityZone Control Center не может проверить SSL-сертификат сборщика HTTP в общедоступном центре сертификации или в DNS сервера. Например, когда Ваш HTTP-коллектор использует самозаверяющий сертификат безопасности.

   Предупреждение
   Эта опция применима только к консоли GravityZone.
   Служба телеметрии безопасности запускается на каждой защищенной конечной точке. Control Center несет полную ответственность за соблюдение политики, настройки сбора и выбор событий.
   Чтобы обеспечить успешную отправку событий телеметрии безопасности, необходимо убедиться, что конечные точки доверяют сборщику HTTP Обязательно, чтобы каждая защищенная конечная точка имела обновленную схему сертификата, которая позволяет проверять конечную точку SSL-сертификата (TLS 1.2 или выше, а DNS сборщика соответствует записям CN/SAN в сертификате), защищая HTTP-сборщик SIEM.

5. Введите маркер авторизации, который обеспечивает безопасность соединения.
6. Выберите типы событий, которые Вы хотите отправить с конечной точки в SIEM.

   По умолчанию отправляются все типы событий, кроме создания раздела реестра.
7. В разделе **Связь между конечными точками и SIEM** выберите, следует ли использовать прокси-сервер или нет.

Примечание
Агент использует для связи с SIEM тот же прокси-сервер, что и для связи с GravityZone. Вы можете проверить его настройки в разделе **Общие настройки** .

После применения политики к конечным точкам агент начинает отправлять события по мере их возникновения на настроенный SIEM-сервер.

7.2.2. Защита от вредоносного ПО

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов
- Linux
- ОС MAK

Модуль защиты от вредоносного ПО обеспечивает защиту системы от всех типов вредоносных угроз (вирусов, вирусов-троянов, шпионских и рекламных программ, руткитов и пр.). Защита делится на три категории:

- Сканирование при доступе: предотвращает проникновение новых угроз в систему.
- Проверка при выполнении: активно защищает от угроз.

  Проверка при выполнении: проактивно защищает от угроз, автоматически обнаруживает и блокирует безфайловые атаки при предварительном выполнении.
- Сканирование по требованию: позволяет распознавать и удалять вредоносные программы, уже присутствующие в системе.

В случае обнаружения вируса или других вредоносных программ агент безопасности Bitdefender попытается автоматически удалить вредоносный код из зараженного файла и воссоздать исходный файл. Эта операция называется "лечение". Файлы, которые не удается вылечить, перемещаются в папку карантина для исключения распространения вируса. Вирус, изолированный в карантине, не может причинить никакого вреда, так как его нельзя запустить или открыть для чтения.

Если сканирование определенных файлов или типов файлов выполнять не требуется, опытные пользователи могут настроить исключения при сканировании.

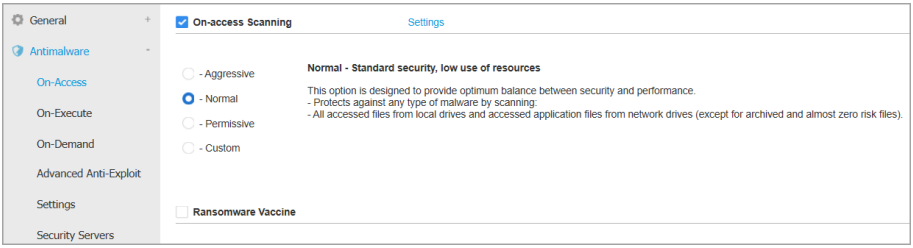
Настройки объединены в следующие разделы:

- Сканирование при доступе (On-Access)
- При выполнении
- Сканирование по запросу (On-Demand)
- Обнаружение гипервизора
- Advanced Anti-Exploit
- Настройки
- Серверы безопасности (Security Servers)

Сканирование при доступе (On-Access)

В этом разделе вы можете настроить компоненты, которые обеспечивают защиту при доступе к файлу или приложению:

- Сканирование при доступе
- Средство от вымогателей



Политики - Настройки при доступе

Сканирование при доступе

Сканирование при доступе предотвращает проникновение в систему новых угроз вредоносных программ путем сканирования локальных и сетевых файлов, если они доступны (открыты, перемещены, скопированы или выполняются), загрузочных секторов и потенциально нежелательных приложений (PUA).

Примечание
Эта функция имеет определенные ограничения в системах на основе Linux. Подробнее см. Главу требований в Руководстве по установке GravityZone.

Чтобы настроить сканирование при доступе к файлам:

1. Установите флажок, чтобы включить или отключить сканирование.

   Предупреждение
   Если вы отключите сканирование при доступе, конечные точки будут уязвимы для вредоносных программ.

2. Выберите для быстрой настройки уровень безопасности, который лучше всего соответствует вашим потребностям (интенсивный, нормальный или рекомендуемый). Используйте описание справа от шкалы, чтобы выбрать необходимый уровень.
3. Вы можете более детально настроить параметры сканирования, выбрав уровень защиты **Пользователь** и нажав на ссылку **Настройки**. Появится окно **Настройки сканирования при доступе**, содержащее несколько вариантов, организованных в двух вкладках - **Общее** и **Расширенные**.

   Опции вкладки **Общее** описаны ниже:

   - **Расположение файлов**. Используйте данную настройку, чтобы задать типы файлов, которые вы хотите просканировать. Параметры сканирования можно настроить отдельно для локальных файлов (сохраненных на локальной конечной точке) или сетевых файлов (хранящихся на сетевых ресурсах). Если защита от вредоносных программ установлена на всех компьютерах в сети, вы можете отключить сканирование сетевых файлов, чтобы разгрузить сеть.

     Вы можете указать агенту безопасности просканировать все доступные файлы (независимо от их расширений), только файлы приложений или специфические расширения файлов, которые вы считаете потенциально опасными. Наиболее качественная защита обеспечивается посредством сканирования всех открываемых файлов, однако сканирование только приложений обеспечивает оптимальную производительность системы.

Примечание
Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов. Для получения более подробной информации, обратитесь к «Типы файлов приложений» (p. 509).

Если вы хотите просканировать только файлы со специфическими расширениями, выберите в меню **Пользовательские расширения** и затем введите желаемые расширения в редактируемом поле, нажимая `Войти` после каждого расширения.

Примечание
В системах на основе Linux расширения файлов чувствительны к регистру, а файлы с одинаковым именем, но с другим расширением считаются различными объектами. Например, `file.txt` и `file.TXT` - разные файлы.

Для повышения производительности системы вы можете также исключить из сканирования большие файлы. Выберите флажок **Maximum size (MB)** и укажите ограничение по размеру файлов, которые будут проверяться. Используйте эту опцию аккуратно, так как вредоносные программы могут также затронуть и большие файлы.

- **СКАНИРОВАТЬ.** Выберите соответствующие флажки, чтобы включить нужные параметры сканирования.
  - **Только новые или измененные файлы.** Сканируя только новые и измененные файлы, можно значительно повысить общее быстродействие системы с минимальными потерями в безопасности.
  - **Загрузочные секторы.** Проверка загрузочных секторов системы. Этот сектор жесткого диска содержит компьютерный код, необходимый для запуска процесса загрузки. Заражение вирусом загрузочного сектора может привести к тому, что диск станет недоступен и вы не сможете загрузить систему и получить доступ к своим данным.
  - **Сканирование на наличие клавиатурных шпионов.** Кейлоггеры (клавиатурные перехватчики) записывают то, что вы набираете на клавиатуре и отправляют отчеты хакерам через интернет. В украденных данных хакер может найти личную информацию, такую как номера банковских счетов и пароли, и использовать ее в личных целях.

- **Сканирование на наличие потенциально нежелательных приложений (PUA).** Потенциально нежелательные приложения (PUA) это программы, которые могут быть нежелательными для ПК, а иногда и поставляться в комплекте с программным обеспечением бесплатного. Такие программы могут быть установлены без согласия (также называются рекламными) или включены по умолчанию в комплект экспресс-установки (как дополнение). Потенциальное воздействие этих программ заключается в показе всплывающих окон, установке нежелательных панелей инструментов в браузере по умолчанию или работе нескольких процессов в фоновом режиме, что замедляет производительность компьютера.
- **Архивы**. Выберите эту опцию, если вы хотите включить сканирование при доступе к файлам архивов. Сканирование архивов — медленный процесс, занимающий большой объем системных ресурсов. Именно поэтому не рекомендуется выполнять такое сканирование в режиме реального времени. Архивы, содержащие инфицированные файлы, не представляют непосредственной угрозы безопасности системы. Вредоносные программы могут повлиять на систему только если зараженный файл извлечен из архива и будет исполнен при выключенной защите в реальном времени.

  Если вы решили использовать данную опцию, вам необходимо настроить следующие параметры оптимизации:
  - **Максимальный размер архива (МБ).** Вы можете установить максимально допустимый размер архивов, которые необходимо сканированировать. Поставьте флажок в соответствующем поле и введите максимальный размер архива (в МБ).
  - **Максимальная глубина архива (уровни).** Отметьте соответствующий флажок и выберите в меню максимальную глубину архива. Для лучшей производительности выберите наименьшее значение, для максимальной защиты выберите наибольшее значение.
- **Отложенное Сканирование.** Отложенное сканирование повышает производительность системы при выполнении операций доступа к файлам. Например, системные ресурсы не задействуются, когда копируются большие файлы. Эта опция включена по умолчанию.

- **Сканирование**. В зависимости от типа обнаруженного файла автоматически выполняются следующие действия:

– **Действие по умолчанию для зараженных файлов.** Bitdefender определяет файлы как зараженные с помощью различных передовых механизмов, которые включают сигнатуры вредоносного ПО, технологии машинного обучения и искусственного интеллекта (ИИ). Агент безопасности Bitdefender может удалить вредоносный код из зараженного файла и воссоздать исходный файл. Эта операция известна как лечение.

  По умолчанию, если зараженный файл обнаружен, агент безопасности Bitdefender автоматически попытается вылечить его. Если файл не удается вылечить, он перемещается в карантин в целях предотвращения распространения вируса. Вы можете изменить этот рекомендуемый поток в соответствии с вашими потребностями.

  Важно
  В случае определенных типов вредоносных программ лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. В таких случаях выполняется удаление зараженного файла с диска.

– **Действие по умолчанию для подозрительных файлов.** Для обнаружения подозрительных файлов Bitdefender использует Эвристический анализ и другие технологии . Такой подход обеспечивает высокий уровень обнаружения, но в некоторых случаях пользователь должен знать о случаях ложных сигналов (чистые файлы, определенные как подозрительные). Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.

  Если обнаружен подозрительный файл, доступ пользователей к этому файлу блокируется, во избежание потенциальной инфекции.

Хотя это и не рекомендуется, вы можете изменить действие по умолчанию. Можно определить два вида действий для каждого типа файлов. Доступны следующие действия:

Запретить доступ
Запретить доступ к обнаруженным файлам.

Важно
Для конечных точек MAC применяется опция перемещения в карантин (**Перейти на карантин**), а не запрета доступа (**Запретить доступ**).

Лечить
Удаляет вредоносный код из зараженных файлов. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов.

Удалить
Удаляет обнаруженные файлы с диска без предупреждения. Желательно избегать использование этого действия.

Перемещение файлов в карантин
Перемещает зараженные файлы из исходного расположения в папку карантина. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице консоли Quarantine.

Не предпринимать никаких действий
Система только сообщает, когда зараженные файлы обнаружены Bitdefender.

Вкладка **Дополнительные настройки** предназначена для сканирования при доступе на Linux-машинах. Используйте флажок, чтобы включить или отключить его.

В приведенной ниже таблице вы можете настроить каталоги Linux, которые вы хотите сканировать. По умолчанию есть пять записей, каждая из которых соответствует определенному местоположению в конечных точках: `/home`, `/ bin`, `/sbin`, `/usr`, `/etc`.

Добавить больше записей:

- Запишите любое имя пользовательского местоположения в поле поиска в верхней части таблицы.
- Выберите предопределенные каталоги из списка, отображаемого при нажатии стрелки в правом конце поля поиска.

Нажмите кнопку ⊕ **Добавить**, чтобы сохранить местоположение в таблице и кнопку ⊗ **Удалить**, чтобы удалить его.

Средство от вымогателей

Средство от вымогателей иммунизирует ваши машины против **известных** вымогателей, блокируя процесс шифрования, даже если компьютер заражен. Используйте флажок, чтобы включить или выключить средство от вымогателей.

Функция борьбы с вымогателями по умолчанию отключена. Лаборатория Bitdefender анализирует поведение широко распространенных программ-вымогателей, а для устранения новейших угроз с каждым обновлением механизмов защиты поставляются новые сигнатуры.

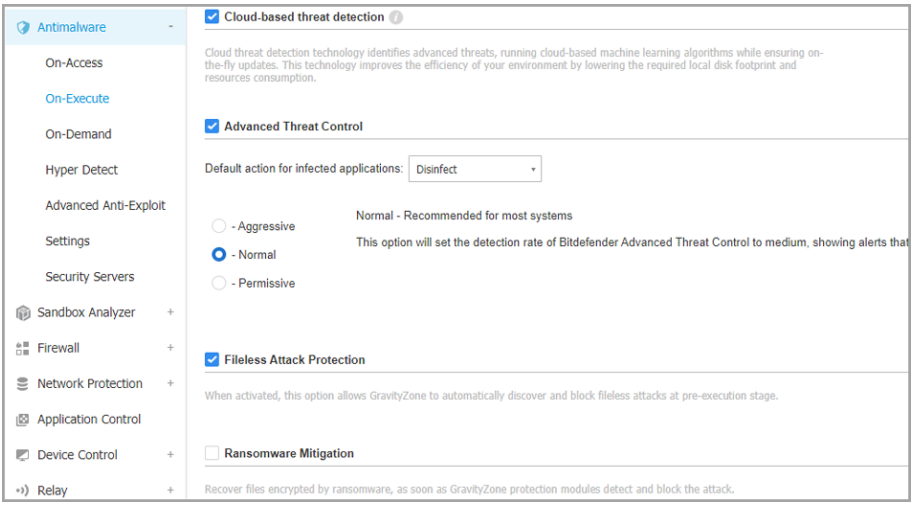
Предупреждение
Для большего повышения защиты от вымогателей, проявляйте осторожность в отношении нежелательных или подозрительных вложений и убедитесь, что все механизмы защиты обновлены.

Примечание
Вакцина от вымогателей доступна лишь при Bitdefender Endpoint Security Tools для Windows.

При выполнении

В этом разделе вы можете настроить защиту от вредоносных процессов, когда они выполняются. Он охватывает следующие защитные слои:

- Облачное обнаружение угроз
- Расширенный контроль угроз (Advanced Threat Control)
- Защита от безфайловых атак
- Смягчение последствий вымогателей



Политики - Настройки при выполнении

Расширенный контроль угроз (Advanced Threat Control)

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов
- ОС MAK

Bitdefender Advanced Threat Control - это технология проактивного обнаружения, которая использует расширенные эвристические методы для обнаружения новых потенциальных угроз в режиме реального времени.

Advanced Threat Control беспрерывно отслеживает приложения, запущенные на компьютере, на предмет признаков вредоносных действий. Для всех вышеперечисленных действий присваивается определенный балл и для каждого процесса подсчитывается общий рейтинг. При достижении общим рейтингом процесса заданного порогового значения, процесс считается вредоносным.

Advanced Threat Control будет автоматически пытаться вылечить обнаруженный файл. Если лечение не удалось, Advanced Threat Control удалит данный файл.

Примечание
Перед выполнением действий по лечению, копия файла отправляется в карантин, так что вы сможете позже восстановить данный файл в случае ложного срабатывания. Это действие может быть настроено с помощью опции **Скопируйте файлы на карантин перед применением дезинфицирующего действия.**, которая доступна на вкладке **Защита от вредоносных программ > Настройки** параметров политики. Эта опция включена по умолчанию в шаблонах политик.

Для настройки Advanced Threat Control:

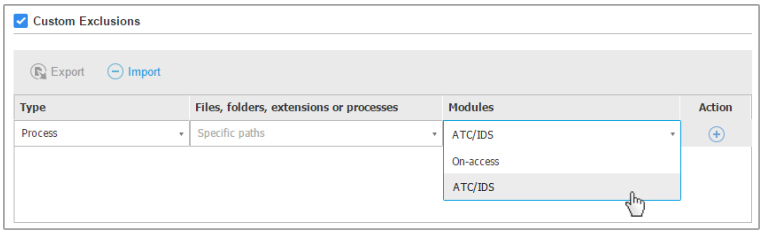
1. Установите этот флажок, чтобы включить или отключить Advanced Threat Control .

   Предупреждение
   Если вы выключите Advanced Threat Control, компьютеры станут уязвимы для неизвестного вредоносного ПО.

2. По умолчанию, используется действие лечения для инфицированных приложений, обнаруженных Advanced Threat Control . Вы можете задать другие действия по умолчанию, используя доступное меню:
   - **Блокировать** чтобы отказать в доступе к зараженному приложению.
   - **Не предпринимать действий**, только сообщать о зараженных приложениях, обнаруженных Bitdefender.
3. Выберите уровень безопасности, который наилучшим образом соответствует вашим потребностям (**Агрессивный, Обычный или Разрешительный**). Используйте описание справа от шкалы, чтобы выбрать необходимый уровень.

   Примечание
   При установке более высокого уровня защиты Advanced Threat Control будет требовать меньше признаков вредоносного поведения для отметки процесса как вредоносного. В результате этого увеличится количество приложений, признанных вредоносными, при этом, также повысится вероятность ложных срабатываний (безопасные приложения отмечаются как вредоносные).

Настоятельно рекомендуется создать правила исключений для часто используемых или известных приложений, с целью предотвращения ложных срабатываний (ошибочное распознавание допустимых приложений). Перейдите на вкладку Защита от вредоносных программ > Настройки и настройте правила исключения процессов для доверенных приложений (ATC/IDS).



Политики - исключение процессов ATC/IDS

Защита от безфайловых атак

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов

Защита от безфайловых атак обнаруживает и блокирует вредоносные безфайловые программы при предварительном выполнении, в том числе завершает работу PowerShell, запускающего вредоносную командную строку, блокирует вредоносный трафик, анализирует буфер памяти до внедрения кода и блокирует процесс внедрения кода.

Смягчение последствий вымогателей

Защита от программ-вымогателей использует технологии обнаружения и исправления, чтобы защитить Ваши данные от атак программ-вымогателей Независимо от того, является ли программа-вымогатель известной или новой, GravityZone обнаруживает аномальные попытки шифрования и блокирует процесс. После этого он восстанавливает файлы из резервных копий в их исходное местоположение.

Важно
Для предотвращения распространения программ-вымогателей требуются расширенный контроль угроз и сканирование при доступе.

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов

Настройка смягчения действий программ-вымогателей

1. Выберите **Смягчение действий вымогателей** и установите флажок **Antimalware > на выполнение** политики, чтобы включить функцию.
2. Выберите режимы мониторинга, которые Вы хотите использовать:
   - Локально. GravityZone отслеживает процессы и обнаруживает атаки вымогателей, инициированные локально на конечной точке. Рекомендуется для рабочих станций. Будьте осторожны при использовании на серверах в связи со снижением производительности.
   - Удаленно GravityZone отслеживает доступ к сетевым общим путям и обнаруживает атаки программ-вымогателей, инициируемые с другого устройства. Используйте этот параметр, если конечная точка является файловым сервером или имеет доступные сетевые ресурсы.
3. Выберите метод восстановления:
   - По запросу. Вы вручную выбираете атаки, из которых будут восстановлены файлы. Вы можете сделать это со страницы **Reports > Ransomware Activity** в любое удобное для Вас время, но не позже, чем через 30 дней с момента атаки. По истечении этого времени восстановление будет уже невозможно
   - Автоматический GravityZone автоматически восстанавливает файлы сразу после обнаружения вымогателей.

   Для успешного восстановления конечные точки должны быть доступны.

После включения у Вас появляется несколько вариантов проверить, не подвергается ли Ваша сеть атаке вымогателей:

- Проверяйте уведомления и ищите **Обнаружение вымогателей**.

Для получения более подробной информации об уведомлениях, пожалуйста, обратитесь к «Типы уведомлений» (p. 484).

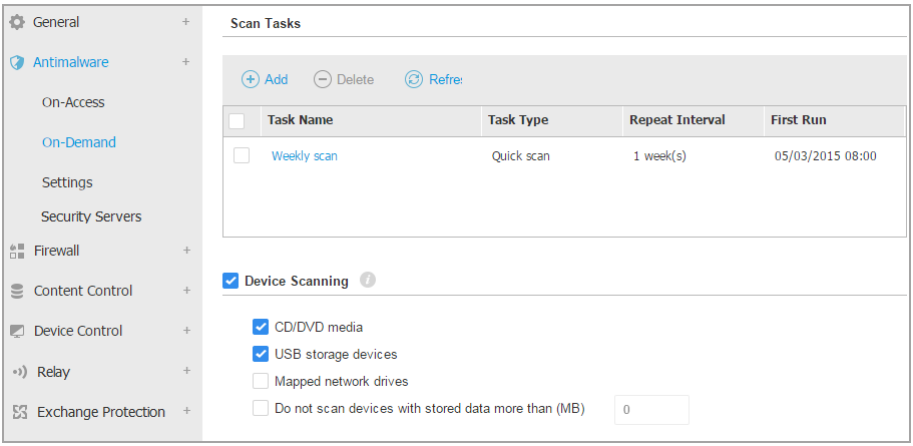
- Проверьте **Security Audit** отчет.
- Проверьте страницу **Деятельность вымогателей**.

  Далее, на этой странице Вы можете запустить задачи восстановления, если это необходимо. Для получения более подробной информации, обратитесь к **Активность вредоносных программ** .

Если Вы заметили обнаружение, которое является законным процессом шифрования, у Вас есть определенные пути, где Вы разрешаете шифрование файлов или удаленный доступ с определенных компьютеров, добавьте исключения в раздел **Antimalware > Settings > Custom Exclusions** policy или из **Ransomware Activity** страницы. Смягчение воздействия программ-вымогателей позволяет исключать папки, процессы и IP-адреса/маски. Для получения более подробной информации, обратитесь к «Исключения» (p. 198).

Сканирование по запросу (On-Demand)

В этом разделе вы можете добавить и настроить задачи проверки защиты от вредоносного ПО, которые будут регулярно работать на определенных компьютерах, в соответствии с установленным графиком.



Политики - Задачи сканирования по требованию

Сканирование производится в фоновом режиме, независимо от того вошел пользователь в систему или нет.

Хотя это и не обязательно, рекомендуется запланировать полное сканирование системы еженедельно на всех конечных точках. Регулярное сканирование конечных точек является активной мерой безопасности, которая может помочь обнаружить и блокировать вредоносные программы, которые могли обойти функции защиты в реальном времени.

Кроме того, вы также можете настроить регулярное сканирование внешних съемных носителей.

Управление задачами сканирования

Панель задач сканирования информирует вас о существующих задачах, предоставляя важную информацию о каждой из них:

- Имя и тип задачи.
- Расписание регулярно выполняемых задач (повторяющихся).
- Время первого запуска задачи.

Вы можете добавить и настроить следующие типы задач сканирования:

- **Быстрое сканирование** использует облачное сканирование для обнаружения вредоносных программ, запущенных в системе. Быстрое сканирование занимает, как правило, менее минуты. Быстрое сканирование использует лишь незначительную часть системных ресурсов, в отличие от процесса стандартного антивирусного сканирования.

  Bitdefender автоматически переходит к обезвреживанию, если обнаружены вредоносные программы или руткиты. Если по какой-либо причине файл нельзя вылечить, он перемещается в карантин. Этот тип сканирования игнорирует подозрительные файлы.

  Быстрое сканирование (Quick Scan) - задача проверки по умолчанию с предустановленными опциями, которые не могут быть изменены. Вы можете добавить только одну задачу быстрого сканирования для одной политики.

- **Полное сканирование** (Full Scan) - проверяет все конечные точки по всем типам вредоносных программ, угрожающих безопасности, таких как вирусы, программы-шпионы, рекламное ПО, руткиты и другие.

Bitdefender автоматически пытается обезвреживать файлы, обнаруженные вредоносными программами. Если вредоносная программа не может быть удалена, она перемещается в карантин, где она не может навредить. Подозрительные файлы игнорируются. Если вы хотите принять меры и в отношении подозрительных файлов, или если вы хотите выполнить другие действия по умолчанию для зараженных файлов, выберите вариант «Запуск пользовательского сканирования».

Полное сканирование - задача проверки по умолчанию с предустановленными опциями, которые не могут быть изменены. Вы можете добавить только одну задачу полного сканирования для одной политики.

- **Пользовательское сканирование** (Custom Scan) - позволяет выбирать расположение объектов для сканирования и настроить параметры сканирования.
- **Сетевое сканирование** (Network Scan) - это тип пользовательского сканирования, который может быть назначен одной управляемой конечной точке для сканирования сетевых дисков, задав определенные настройки параметров сканирования и указав определенные области, которые будут проверяться. Для агента безопасности вам необходимо ввести учетные данные пользователя с правами чтения/записи для выбранных сетевых дисков, чтобы иметь возможность получить доступ и выполнить требуемые действия на этих сетевых дисках.

  Задача повторяющегося сетевого сканирования будет отправлена только выбранной сканирующей конечной точке. Если выбранная конечная точка недоступна, будут применены параметры локального сканирования.

  Примечание
  Создавать задачи сканирования сети можно только в политике, которая уже применяется к конечной точке, используемой в качестве сканера.

Кроме задач сканирования по умолчанию (которые вы не можете удалить или дублировать), вы можете создать столько пользовательских задач сканирования и задач сканирования сети, сколько вы хотите.

Чтобы создать и настроить новые пользовательские задачи или задачи сканирования сети, нажмите кнопку ⊕ **Добавить** в правой части таблицы. Чтобы изменить параметры существующей задачи сканирования, щелкните

на имя этой задачи. Обратитесь к следующей теме, чтобы узнать, как настроить параметры задач.

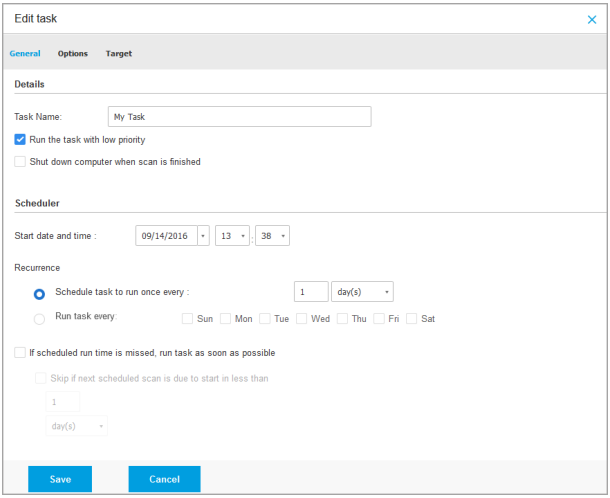
Чтобы удалить задачу из списка, выберите задачу и нажмите кнопку ⊖ **Удалить** в правой части таблицы.

Настройка задач сканирования

Настройки задач сканирования расположены в трех вкладках:

- **Общее**: имя задачи и график выполнения.
- **Опции**: выбор профиля сканирования для быстрой конфигурации параметров и настройка параметров проверки пользовательского сканирования.
- **Цель**: выбор файлов и папок, которые будут проверяться и настройка исключений сканирования.

Опции, от первой до последней вкладки, описаны далее:



Политики - Настройка Задач сканирования по требованию. Общие настройки

- **Подробности.** Выберите подходящее имя задаче, которое поможет вам легче определить ее назначение. При выборе имени задачи, учитывайте ее назначение и возможные параметры сканирования.

По умолчанию, задачи проверки запускаются с наименьшим приоритетом. Таким образом, Bitdefender позволяет другим программ работать быстрее, но увеличивает время, необходимое для завершения процесса проверки. Используйте флажок **Запустите задачу с низким приоритетом**, чтобы запретить или разрешить данную функцию.

Примечание
Эта опция применима только к Bitdefender Endpoint Security Tools и Endpoint Security (устаревший агент)

Отметьте флажок **Выключите компьютер после завершения сканирования**, чтобы выключить машину, если вы не собираетесь использовать ее некоторое время.

Примечание
Эта опция применима к Bitdefender Endpoint Security Tools, Endpoint Security (устаревший агент) и Endpoint Security for Mac.

- **Проверка по расписанию.** Используйте параметры планирования для настройки расписаний сканирований. Вы можете установить время запуска задачи сканирования каждые несколько часов, дней или недель, начиная с указанной даты и времени.

  Конечные точки должны быть включены по графику. Запланированная задача сканирования не будет выполнятся если машина выключена, находится в режиме гибернации или в спящем режиме. В таких ситуациях, проверка будет отложена до следующего раза.

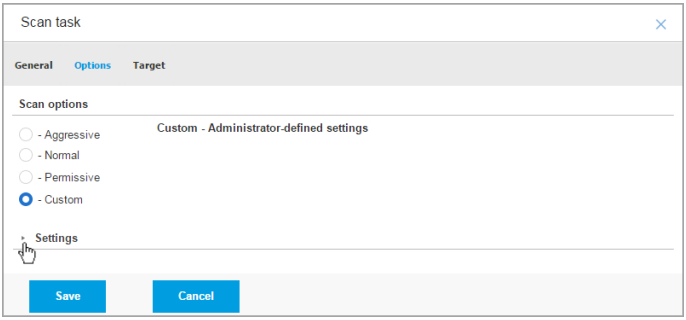
  Примечание
  Проверка по расписанию будет работать на выбранных конечных точках с учетом местного времени. Например, если запланирована задача сканирования, которая должна начаться в 6:00, и конечная точка находится в другом часовом поясе с Control Center, задача сканирования начнется в 6:00 (по времени конечной точки).

  При желании вы можете указать, что происходит, когда задача проверки не может быть запущена в запланированное время (конечная точка была отключена или отключена). Используйте параметр **Если запланированное время выполнения пропущено, запустите задачу как можно скорее** в соответствии с вашими потребностями:

- Если вы оставите этот флажок выключенным, задача проверки будет выполняться снова в следующий запланированный момент времени.
- Когда вы выбираете опцию, вы запускаете сканирование как можно скорее. Чтобы настроить оптимальное время выполнения сканирования и не беспокоить пользователя в рабочее время, выберите **Пропустить, если следующее запланированное сканирование должно начаться менее чем через**, затем укажите интервал, который вы хотите.

- **Параметры сканирования.** Выберите уровень безопасности, который лучше всего соответствует вашим потребностям (Интенсивный, Нормальный или Рекомендуемый). Используйте описание справа от шкалы, чтобы выбрать необходимый уровень.

  В зависимости от выбранного профиля, параметры сканирования в разделе **Настройки** будут сконфигурированы автоматически. Тем не менее, при желании, вы можете настроить их более детально. Чтобы сделать это, отметьте флажком опцию **Пользователь** и затем перейдите в раздел **Настройки**.



Задача сканирования - Настройка пользовательского режима

- **Типы файлов.** Используйте данную настройку, чтобы задать типы файлов, которые вы хотите просканировать. Вы можете указать агенту безопасности просканировать все файлы (независимо от их расширений), только файлы приложений или специфические типы файлов, которые вы считаете потенциально опасными. При сканировании всех файлов обеспечивается оптимальная защита. Сканируя только приложения, можно повысить скорость сканирования.

Примечание

Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов. Для получения более подробной информации, обратитесь к «Типы файлов приложений» (p. 509).

Если вы хотите просканировать только файлы со специфическими расширениями, выберите в меню **Пользовательские расширения** и затем введите желаемые расширения в редактируемом поле, нажимая `Войти` после каждого расширения.

- **Архивы.** Архивы, содержащие инфицированные файлы, не представляют непосредственной угрозы безопасности системы. Вредоносные программы могут повлиять на систему только если зараженный файл извлечен из архива и будет исполнен при выключенной защите в реальном времени. Тем не менее, рекомендуется использовать этот параметр для обнаружения и удаления всех угроз, даже тех, которые не представляют собой непосредственной опасности для системы.

  Примечание

  Сканирование файлов, сжатых в архив, увеличивает общее время сканирования и занимает больший объем системных ресурсов.

  – **Сканирование внутри архивов.** Выберите эту опцию, если вы хотите проверить заархивированные файлы на наличие вредоносных программ. Если вы решили использовать данную опцию, вам необходимо настроить следующие параметры оптимизации:

    - **Ограничение размера архива (Мб).** Вы можете установить максимально допустимый размер архивов для сканирования. Поставьте флажок в соответствующем поле и введите максимальный размер архива (в МБ).
    - **Максимальная глубина архива (уровни).** Отметьте соответствующий флажок и выберите в меню максимальную глубину архива. Для лучшей производительности выберите наименьшее значение, для максимальной защиты выберите наибольшее значение.

  – **Сканировать архивы электронной почты.** Выберите данную опцию если хотите разрешить проверку почтовых сообщений и почтовых баз, включая такие форматы файлов как .eml, .msg, .pst, .dbx, .mbx, .tbb и другие.

Примечание
Процесс сканирования почтовых архивов является достаточно ресурсоемким и может повлиять на производительность системы.

- **Разное.** Выберите соответствующие флажки, чтобы включить нужные параметры сканирования.
  - **Сканирование загрузочных секторов.** Проверка загрузочных секторов системы. Этот сектор жесткого диска содержит компьютерный код, необходимый для запуска процесса загрузки. Заражение вирусом загрузочного сектора может привести к тому, что диск станет недоступен и вы не сможете загрузить систему и получить доступ к своим данным.
  - **Сканирование реестра.** Выберите этот параметр для сканирования ключей реестра. Реестр Windows — это база данных, в которой хранятся настройки и параметры конфигурации для компонентов операционной системы Windows и установленных приложений.
  - **Сканирование на наличие руткитов.** Выберите этот параметр для сканирования на наличие руткитов и объектов, скрытых с помощью такого программного обеспечения.
  - **Сканирование на наличие клавиатурных шпионов.** Выберите данную опцию для сканирования системы на наличие клавиатурных шпионов.
  - **Сканировать общие сетевые ресурсы.** Эта опция сканирует подключенные сетевые диски.

    Для быстрого сканирования эта опция отключена по умолчанию. Для полного сканирования опция активирована по умолчанию. Для сканирования по выбору пользователя, если вы установите уровень безопасности **Интенсивный/Нормальный**, параметр **Сканирование общих сетевых ресурсов** включается автоматически. Если вы установите уровень безопасности **Рекомендуемый**, параметр **Сканирование общих сетевых ресурсов** автоматически отключается.
  - **Сканирование памяти.** Выберите этот параметр для сканирования программ, запущенных в системной памяти.
  - **Сканирование файлов cookie.** Выберите эту опцию для сканирования файлов cookie, сохраненных браузерами на конечных точках.

- **Сканирование только новых/измененных файлов.** Сканируя только новые и измененные файлы, можно значительно повысить общее быстродействие системы с минимальными потерями в безопасности.
- **Сканирование на наличие потенциально нежелательных приложений (PUA).** Потенциально нежелательные приложения (PUA) это программы, которые могут быть нежелательными для ПК, а иногда и поставляться в комплекте с программным обеспечением бесплатного. Такие программы могут быть установлены без согласия (также называются рекламными) или включены по умолчанию в комплект экспресс-установки (как дополнение). Потенциальное воздействие этих программ заключается в показе всплывающих окон, установке нежелательных панелей инструментов в браузере по умолчанию или работе нескольких процессов в фоновом режиме, что замедляет производительность компьютера.

- **Действия.** В зависимости от типа обнаруженного файла автоматически выполняются следующие действия:
  - **Действие по умолчанию для зараженных файлов.** Bitdefender определяет файлы как зараженные с помощью различных передовых механизмов, которые включают сигнатуры вредоносного ПО, технологии машинного обучения и искусственного интеллекта (ИИ). Агент безопасности может удалить вредоносный код из зараженного файла и воссоздать исходный файл. Эта операция известна как лечение.

    Если зараженный файл обнаружен, агент безопасности будет пытаться вылечить его автоматически. Если файл не удается вылечить, он перемещается в карантин в целях предотвращения распространения вируса.

    Важно
    В случае определенных типов вредоносных программ лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. В таких случаях выполняется удаление зараженного файла с диска.

  - **Действие по умолчанию для подозрительных файлов.** Для обнаружения подозрительных файлов Bitdefender использует Эвристический анализ и другие технологии . Такой подход обеспечивает высокий уровень обнаружения, но в некоторых случаях пользователь должен знать о

случаях ложных сигналов (чистые файлы, определенные как подозрительные). Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.

По умолчанию, задачи сканирования настроены игнорировать подозрительные файлы. Вы можете изменить действие по умолчанию, чтобы перемещать подозрительные файлы в карантин. Помещенные в карантин файлы отправляются на анализ в лабораторию Bitdefender на регулярной основе. Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит его удалить.

– **Действие по умолчанию для руткитов.** Руткиты представляют собой специализированное программное обеспечение, используемое для того, чтобы скрыть файлы операционной системы. Однако, руткиты часто используются, чтобы скрыть вредоносные программы, либо для сокрытия присутствия злоумышленника в системе.

  Обнаруженные руткиты и скрытые файлы по умолчанию игнорируются.

Хотя это и не рекомендуется, вы можете изменить действие по умолчанию. Можно задать дополнительное действие, которое будет выполнено в случае, если не удалось выполнить первое, а также различные действия для каждой из категорий. Выберите в соответствующих меню первое и второе действие, которые будут выполняться в отношении всех типов обнаруженных файлов. Доступны следующие действия:

Не предпринимать никаких действий
Никаких действий не будет предпринято в отношении обнаруженных файлов. Эти файлы будут отображаться только в журнале сканирования.

Лечить
Удаляет вредоносный код из зараженных файлов. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов.

Удалить
Удаляет обнаруженные файлы с диска без предупреждения. Желательно избегать использование этого действия.

Перемещение файлов в карантин
Перемещает зараженные файлы из исходного расположения в папку карантина. Файлы, помещенные в карантин, не могут быть выполнены

или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице консоли Quarantine.

- **Сканирование объектов.** Добавьте в список все области, которые вы хотите просканировать, на выбранных компьютерах.

  Чтобы добавить новый файл или папку для сканирования:

  1. Выберите предопределенное месторасположение из выпадающего меню или введите конкретные пути в **конкретные пути**, которые вы хотите просканировать.
  2. Укажите путь к объекту для сканирования в поле редактирования.
     - Если вы выбрали предопределенное место, необходимо корректно завершить путь. Например, для сканирования всей папки `Програмные файлы`, достаточно выбрать соответствующее предопределенное место из выпадающего меню. Для сканирования конкретной папки из `Програмные файлы`, необходимо завершить путь, добавив обратную косую черту (\) и имя папки.
     - Если вы выбрали **Конкретные пути**, введите полный путь к объекту проверки. Желательно использовать системные переменные (в соответствующих случаях), чтобы быть уверенным, что путь действителен для всех нужных компьютеров.
  3. Нажмите соответствующую кнопку ⊕ **Добавить**.

  Чтобы изменить существующий путь, нажмите на него. Чтобы удалить папку из списка, наведите курсор на эту папку и нажмите соответствующую кнопку ⊖ **Удалить**.

- Для агента безопасности вам необходимо ввести учетные данные пользователя с правами чтения/записи для выбранных сетевых дисков, чтобы иметь возможность получить доступ и выполнить требуемые действия на этих сетевых дисках.

- **Исключения.** Вы можете использовать либо исключения, определенные в разделе **Защита от вредоносных программ > Исключения** нынешней политики, либо вы можете задать пользовательские исключения для текущего задания сканирования. За более подробной информацией об исключениях, обратитесь к «Исключения» (p. 198).

Сканирование устройств

Вы можете настроить агент безопасности на автоматическое обнаружение и сканирование внешних устройств хранения данных при их подключении к конечной точке. Обнаруженные устройства относятся к одной из следующих категорий:

- CD/DVD
- Запоминающие устройства USB, такие как флэш-носители и внешние жесткие диски
- Устройства с более определенным количеством хранимых данных.

Сканирование устройств автоматически попытается вылечить файлы, обнаруженные как зараженные или переместит их в карантин, если лечение невозможно. Обратите внимание, что некоторые устройства, такие как CD/DVD, предназначены только для чтения. Никакие действия не могут быть предприняты для зараженных файлов, содержащихся в такой поддержке хранилища.

Примечание
Во время сканирования устройства пользователь может получать доступ к любым данным этого устройства.

Если всплывающие предупреждения включены в разделе **Основные> Уведомления**, то вместо автоматического запуска, у пользователя будет запрошено действие на сканирование или отмену сканирования обнаруженного устройства.

При запуске сканирования устройства:

- Всплывающее уведомление информирует пользователя о сканировании устройства, при условии, что всплывающие уведомления включены в разделе **Основные > Уведомления**.

После завершения задачи сканирования, пользователь должен проверить обнаруженные угрозы, если таковые имеются.

Выберите опцию **Сканирование устройства** для того, чтобы включить автоматическое обнаружение и сканирование устройств хранения. Чтобы настроить проверку устройств индивидуально для каждого типа устройства, используйте следующие параметры:

- **Носители CD/DVD**

- **Запоминающие устройства USB**
- **Не сканируйте устройства с сохраненными данными более(MB)**. Используйте эту опцию, чтобы автоматически пропускать сканирование обнаруженного устройства, если количество хранимых данных превысит указанный объем. Введите в соответствующем поле ограничение по размеру (в мегабайтах). Ноль означает, что ограничения по размеру не предусмотрены.

Обнаружение гипервизора

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов
- Linux

HyperDetect добавляет дополнительный уровень безопасности к существующим технологиям сканирования (сканирование при доступе, по требованию и сканирование трафика) для борьбы с новым поколением киберугроз, включая вирусы для атак на объекты критической инфраструктуры (APT). Hyper Detect расширяет модули защиты от вредоносных программ и контента с помощью мощных эвристических программ на основе искусственного интеллекта и машинного обучения.

Благодаря своей способности прогнозировать целенаправленные атаки и обнаруживать самые сложные вредоносные программы на этапе предварительного исполнения, HyperDetect обнаруживает угрозы намного быстрее, чем технологии, основанные на сигнатуре или поведенческом режиме.

Чтобы настроить HyperDetect:

1. Установите флажок **HyperDetect** , чтобы включить или выключить модуль.
2. Выберите, от какого типа угроз вы хотите защитить свою сеть. По умолчанию защита включена для всех типов угроз: целенаправленных атак, подозрительных файлов и сетевого трафика, эксплойтов, вирусов-вымогателей или условно вредоносного ПО .

Примечание
Для эвристики сетевого трафика требуется включить **Контроль контента > Сканирование трафика** .

3. Настройте уровень защиты от угроз выбранных типов.

   Используйте главный переключатель в верхней части списка угроз, чтобы выбрать уникальный уровень защиты для всех типов объектов, или выберите индивидуальные уровни для точной настройки защиты.

   Установка модуля на определенном уровне приведет к тому, что действия будут приняты на этом уровне. Например, если установлено значение **Нормальный уровень** , модуль обнаруживает и сдерживает угрозы, подходящие под параметр **Рекомендуемый уровень** и **Нормальный уровень** , но не **Интенсивный уровень**.

   Защита увеличивается от уровня **Рекомендуемый** до **Интенсивный**.

   Имейте в виду, что Интенсивный уровень защиты может привести к ложным срабатываниям, в то время как Рекомендуемый уровень может подвергнуть вашу сеть некоторым угрозам. Рекомендуется сначала установить уровень защиты на максимум, а затем постепенно снижать его в случае множества ложных срабатываний, пока вы не достигнете оптимального баланса.

   Примечание
   Всякий раз, когда вы включаете защиту для типа угроз, для их обнаружения автоматически устанавливается значение по умолчанию (уровень **Нормальный**).

4. В разделе **Действия** настройте реакцию HyperDetect на обнаруженное ПО. Используйте параметры раскрывающегося меню, чтобы установить действие, которое необходимо предпринять в случае обнаружения угроз:
   - Для файлов: запретить доступ, обезвреживание, удаление, карантин или просто отчет о файле.
   - Для сетевого трафика: блокировать или просто сообщать о подозрительном трафике.
5. Установите флажок **Расширить отчетность на более высоких уровнях** рядом с раскрывающимся меню, если вы хотите просматривать угрозы, обнаруженные на более высоких уровнях защиты, чем установленные.

Если вы не уверены в текущей конфигурации, вы можете легко восстановить первоначальные настройки, нажав кнопку **Сбросить по умолчанию** в нижней части страницы.

Advanced Anti-Exploit

Примечание
Данный модуль доступен для:

- Windows для рабочих станций и серверов

Advanced Anti-Exploit - активная технология для обнаружения эксплойтов в реальном времени. Основанная на машинном, она защищает от известных и неизвестных эксплойтов, включая безфайловые атаки.

Чтобы активировать защиту от эксплойтов, отметьте галочку напротив **Advanced Anti-Exploit**.

Advanced Anti-Exploit изначально настроен на запуск с рекомендуемыми параметрами. Вы можете настроить защиту по-другому, если это необходимо. Для восстановления изначальных настроек, нажмите на ссылку **Настройки по умолчанию** в правой части заголовка раздела.

Настройки анти-эксплойта в GravityZone распределены по трем разделам:

- **Общесистемные обнаружения**

  Методы защиты от эксплойтов в этом разделе отслеживают системные процессы, которые являются объектами эксплойтов.

  Для получения дополнительной информации о доступных методах и о том, как настроить их параметры, см. «Настройка общесистемного смягчения» (p. 193).

- **Предопределенные приложения**

  Модуль Advanced Anti-Exploit предварительно настроен со списком распространенных приложений, таких как Microsoft Office, Adobe Reader или Flash Player, которые наиболее подвержены эксплойтам.

  Для получения дополнительной информации о доступных методах и о том, как настроить их параметры, см. «Настройка Application-Specific Techniques» (p. 194).

- **Дополнительные приложения**

В этом разделе вы можете добавить и настроить защиту для других приложений на ваш выбор.

Для получения дополнительной информации о доступных методах и о том, как настроить их параметры, см. «Настройка Application-Specific Techniques» (p. 194).

Вы можете развернуть или свернуть любой раздел, нажав его заголовок. Таким образом, вы быстро перейдете к параметрам, которые хотите настроить.

Настройка общесистемного смягчения

В данном разделе присутствуют следующие опции:

Метод	Описание
Повышение прав	Предотвращает процессы, направленные на получение несанкционированных привилегий и доступа к ресурсам. Действие по умолчанию: Завершает процесс
Защита процесса LSASS	Защищает процесс LSASS от утечки секретной информации, такой как хеши паролей и настройки безопасности. Действие по умолчанию: Блокирует процесс

Эти методы защиты от эксплойтов включены по умолчанию. Чтобы отключить любой из методов, снимите флажок.

При желании вы можете изменить действие, предпринимаемое автоматически при обнаружении. Выберите действие, доступное в соответствующем меню:

- **Завершить процесс**: немедленно завершает эксплуатируемый процесс.
- **Блокировать процесс**: предотвращает доступ вредоносного процесса к недоверенным ресурсам.
- **Только отчет**: GravityZone сообщает о событии без каких-либо действий по смягчению последствий. Вы можете просмотреть подробности события в уведомлении **Advanced Anti-Exploit**, а также в отчетах "Заблокированные приложения" и "Аудит безопасности".

Настройка Application-Specific Techniques

Будь то предопределенные или дополнительные приложения, все они используют один и тот же набор методов защиты от эксплойтов. Вы можете найти описание здесь:

Метод	Описание
ROP Emulation	Обнаруживает попытки сделать страницы памяти данных исполняемыми, использующие метод возвратно-ориентированного программирования (ROP). Действие по умолчанию: Завершить процесс
ROP Stack Pivot	Обнаруживает попытки перехвата потока кода, использующих метод ROP, путем проверки местоположения стека. Действие по умолчанию: Завершить процесс
ROP Illegal Call	Обнаруживает попытки перехвата потока кода, использующих метод ROP,путем проверки инициаторов вызова чувствительных системных функций. Действие по умолчанию: Завершить процесс
ROP Stack Misaligned	Обнаруживает попытки повреждения стека, использующих метод ROP, путем проверки выравнивания адресов стека. Действие по умолчанию: Завершить процесс
ROP Return To Stack	Обнаруживает попытки выполнения кода непосредственно в стеке, использующих метод ROP, путем проверки диапазона адресов возврата. Действие по умолчанию: Завершить процесс
ROP сделать стек исполняемым	Обнаруживает попытки повреждения стека, использующих метод ROP, путем проверки защиты страницы стека. Действие по умолчанию: Завершить процесс
Flash Generic	Обнаруживает попытки эксплуатации Flash Player. Действие по умолчанию: Завершить процесс

Метод	Описание
Flash Payload	Обнаруживает попытки выполнения вредоносного кода во Flash Player путем сканирования объектов Flash в памяти. Действие по умолчанию: Завершить процесс
VBScript Generic	Обнаруживает попытки использования VBScript. Действие по умолчанию: Завершить процесс
Выполнение Shellcode	Обнаруживает попытки создания новых процессов или загрузки файлов, использующих шелл-код. Действие по умолчанию: Завершить процесс
Библиотека загрузки шелл-кода	Обнаруживает попытки выполнения кода по сетевым путям, использующих шелл-код. Действие по умолчанию: Завершить процесс
Anti-Detour	Обнаруживает попытки обхода проверки безопасности для создания новых процессов. Действие по умолчанию: Завершить процесс
Shellcode EAF (Export Address Filtering)	Обнаруживает попытки получения вредоносным кодом доступа к чувствительным системным функциям из экспорта DLL. Действие по умолчанию: Завершить процесс
Shellcode Thread	Обнаруживает попытки внедрения вредоносного кода путем проверки вновь созданных потоков. Действие по умолчанию: Завершить процесс
Anti-Meterpreter	Обнаруживает попытки создания обратной оболочки путем сканирования страниц исполняемой памяти. Действие по умолчанию: Завершить процесс
Создание процесса устарело	Обнаруживает попытки создания новых процессов с использованием устаревших методов. Действие по умолчанию: Завершить процесс
Создание дочернего процесса	Блокирует создание любого дочернего процесса. Действие по умолчанию: Завершить процесс

Метод	Описание
Enforce Windows DEP	Обеспечивает предотвращение выполнения данных (DEP) для блокировки выполнения кода на страницах данных. По умолчанию: Отключено
Принудительное перемещение модулей (ASLR)	Предотвращает загрузку кода в предсказуемые места путем перемещения модулей памяти. По умолчанию: Включено
Новые эксплойты	Защищает от любых новых возникающих угроз или эксплойтов. Быстрые обновления используются для этой категории, прежде чем могут быть сделаны более всеобъемлющие изменения. По умолчанию: Включено

Чтобы отслеживать другие приложения, кроме предопределенных, нажмите кнопку **Добавить приложение**, расположенную вверху и внизу страницы.

Чтобы настроить параметры защиты от эксплойтов для приложения:

1. Для существующих приложений, нажмите на название приложения. Для новых приложений нажмите кнопку **Добавить**.

   На новой странице отображаются все методы и их настройки для выбранного приложения.

   Важно
   Будьте осторожны при добавлении новых приложений для мониторинга. Bitdefender не может гарантировать совместимость с любым приложением. Таким образом, рекомендуется сначала протестировать функцию на нескольких некритичных конечных точках, а затем развернуть ее в сети.

2. При добавлении нового приложения введите его имя и имена его процессов в соответствующие поля. Используйте точку с запятой (;) для разделения процессов.
3. Если необходимо быстро проверить описание метода, нажмите на стрелку рядом с его названием.

4. При необходимости установите или снимите флажки используемых методов.

   Используйте опцию **Все**, если хотите выделить все методы разом.

5. Если необходимо, измените автоматическое действие при обнаружении. Выберите действие, доступное в соответствующем меню:

   - **Завершить процесс**: немедленно завершает эксплуатируемый процесс.
   - **Только отчет**: GravityZone сообщает о событии без каких-либо действий по смягчению последствий. Подробные сведения о событии можно просмотреть в уведомлении **Advanced Anti-Exploit** и в отчетах.

   По умолчанию все методы для предопределенных приложений настроены для смягчения проблемы, а для дополнительных приложений - просто сообщать о событии.

   Для быстрой смены действия, применяемого ко всем методам зашиты сразу, выберите действие из меню, соответствующее варианту **Все**.

Нажмите кнопку **Назад** в верхней части страницы для того, чтобы вернуться к общим настройкам модуля Anti-Exploit.

Настройки

В этом разделе вы можете настроить параметры карантина и правила исключений для сканирования.

- Изменение настроек карантина
- Настройка исключений сканирования

Карантин

Вы можете настроить следующие параметры для файлов в карантине на конечных точках:

- **Удалить файлы, чей срок более (дней)..** По умолчанию, файлы в карантине старше 30 дней автоматически удаляются. Если вы хотите изменить этот интервал, выберите другой вариант из меню.
- **Отправить помещенные в карантин файлы Bitdefender Лаборатории каждые (часы).** По умолчанию файлы из карантина автоматически отправляются в лаборатории Bitdefender каждый час. Вы можете отредактировать интервал времени отправки файлов из карантина (один

час по умолчанию). Специалисты по вирусам Bitdefender проанализируют образцы файлов. Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит его удалить.

Примечание
Для получения информации о том, как эти настройки нарушают правила HIPAA, обратитесь к разделу "GravityZone и HIPAA" в Руководстве по установке.

- **Повторно сканировать файлы из карантина после обновления механизмов защиты.** Выберите данную опцию для автоматического сканирования файлов карантина после каждого обновления механизмов защиты. Очищенные файлы автоматически возвращаются на свое место.
- **Скопируйте файлы на карантин перед применением дезинфицирующего действия.** Выберите эту опцию, чтобы предотвратить потерю данных в случае ложных срабатываний и копировать каждый инфицированный файл в карантине перед лечением. После этого вы сможете восстановить здоровые файлы из карантина на странице **Карантин**.
- **Разрешить пользователям выполнять действия в локальном карантине.** Этот параметр управляет действиями, которые пользователи конечной точки могут предпринять в локальных файлах, помещенных на карантин, с помощью интерфейса Bitdefender Endpoint Security Tools. По умолчанию локальные пользователи могут восстанавливать или удалять файлы, помещенные на карантин, с помощью параметров, доступных в Bitdefender Endpoint Security Tools. Отключив эту опцию, пользователи больше не будут иметь доступа из интерфейса Bitdefender Endpoint Security Tools к кнопкам действий с файлами на карантине.

Исключения

Агент безопасности Bitdefender может исключить из сканирования определенные типы объектов. Исключения при сканировании должны использоваться в особых случаях или при рекомендациях Microsoft или Bitdefender. Чтобы просмотреть обновленный список исключений, рекомендованный Microsoft, пожалуйста, обратитесь к этой статье article.

В этом разделе вы можете настроить использование различных типов исключений агентом безопасности Bitdefender.

- **Встроенные исключения**, которые по умолчанию доступны и включены в агенте безопасности Bitdefender.

  Вы можете отключить встроенные исключения, если хотите просканировать все типы объектов, но этот вариант будет значительно влиять на производительность машины и увеличит время сканирования.

- Вы также можете задать **Пользовательские исключения** для собственных приложений или специально настроенных утилит, в соответствии с вашими требованиями.

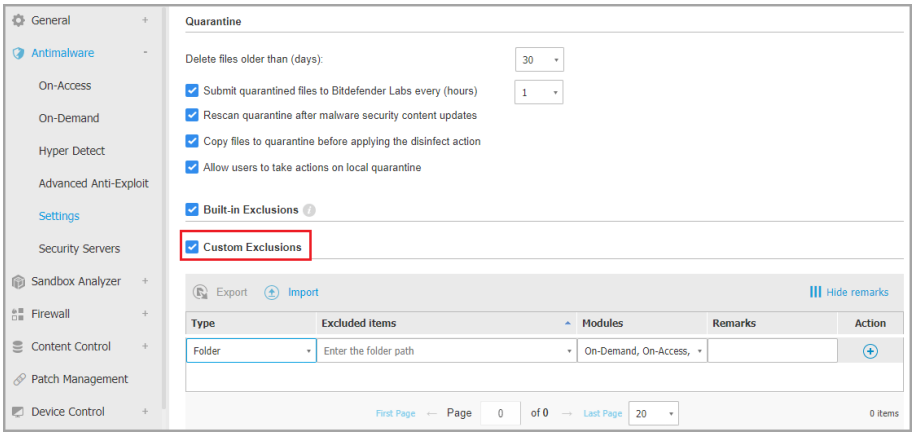
  Пользовательские исключения сканирования применяются к одному или нескольким следующим методам:

  – Сканирование при доступе
  – Сканирование по требованию
  – Расширенный контроль угроз (Advanced Threat Control)
  – Защита от безфайловых атак
  – Смягчение последствий вымогателей

  Важно

  – При наличии тестового файла EICAR, который периодически используется для тестирования защиты от вредоносных программ, необходимо исключить его из сканирования при доступе.
  – Если вы используете VMware Horizon View 7 и AppStacks AppStacks, пожалуйста, ознакомьтесь с Документ VMware .

  Для исключения определенных элементов из сканирования, отметьте галочку **Пользовательские исключения** и добавьте правила в таблицу снизу.



Политики компьютеров и виртуальных машин - Пользовательские исключения

Чтобы добавить пользовательское правило исключений:

1. Выберите тип исключения из меню:
   - **Файл**: только указанный файл
   - **Папка**: только указанная папка, без всех файлов и процессов внутри нее или из всех ее вложенных папок
   - **Расширение**: все элементы с указанным расширением
   - **Процесс**: любой объект доступный данному исключенному процессу.
   - **Хэш файла**: файл с указанным хэшем
   - **Хэш Сертификата**: все приложения с указанным хэшем сертификата (отпечатком)
   - **Название угрозы**: любой элемент с именем обнаружения (недоступно для операционных систем Linux)
   - **Командная строка**: указанная командная строка (доступно только для операционных систем Windows)

Предупреждение
В безагентной среде VMware , интегрированной с VSHIELD, вы можете исключать только папки и расширения. Установив Bitdefender Tools на виртуальных машинах, вы также сможете исключать файлы и процессы.

Во время процесса установки, при настройке пакета, вам необходимо отметить соответствующий флажок **Развертывание конечной точки с помощью vShield при обнаружении среды VMware, интегрированной с vShield** Для получения дополнительной информации обратитесь к разделу **Создание инсталляционных пакетов** Руководства по установке.

2. Заполните информацию для указанного типа исключения:

   Файл, Папка или Процесс

   Введите путь к элементу, исключаемому из сканирования. Для написания пути вы можете воспользоваться несколькими способами:

   – Указать путь явно.

     Например: `C: emp`

     Чтобы добавить исключение в формате UNC, используйте следующий синтаксис:

     `\\hostName\shareName\filePath`

     `\\IPaddress\shareName\filePath`

   – Используйте системные переменные, доступные из выпадающего меню.

     Для исключения процесса необходимо также добавить имя исполняемого файла приложения.

     Например:

     `%ProgramFiles%` - исключает папку Program Files

     `%WINDIR%\system32` – исключает папку system32 в папке Windows

     Примечание
     Желательно использовать системные переменные (где это возможно), чтобы путь был действительным для всех выбранных компьютеров.

   – Используйте подстановочные символы.

     Двойная звездочка (**) заменяет неопределенное количество символов. Звездочка (*) заменяет неопределенное количество символов. Вопросительный знак (?) заменяет только один символ. Вы можете использовать несколько вопросительных знаков, чтобы

задать любую возможную комбинацию из определенного количества символов. Например, ??? заменяет любую комбинацию, состоящую из трех символов.

Примечание
Этот параметр доступен как в Control Center, так и в настройках политики привилегированного пользователя в разделе **Antimalware** > **Настройки** > **Пользовательские исключения**.

Например:

Исключения файлов:

`**\example.txt` – исключает любой файл с именем example.txt, независимо от его местоположения на конечной точке

`C:\Test\*` - исключает все файлы из папки Test

`C:\Test\*.png` - Исключает все PNG файлы из папки Test

Исключение папок:

`C:\Test\*` - исключает все папки из папки Test

`C:\Test\*` - исключает все папки и файлы из папки Test

Исключения процесса:

`C:\Program Files\WindowsApps\Microsoft.Not??.exe` – Исключает все процессы Microsoft Notes

Примечание
Исключения процессов не поддерживают подстановочные символы в операционных системах Linux.

Расширение

Укажите одно или несколько расширений файлов для исключения из сканирования, разделив их точкой с запятой ";". Можно вводить расширения с или без точки. Например, введите txt, чтобы исключить текстовые файлы.

Примечание
В системах на основе Linux расширения файлов чувствительны к регистру, а файлы с одинаковым именем, но с другим расширением

считаются различными объектами. Например, `file.txt` и `file.TXT` - разные файлы.

Хэш файла, Хэш сертификата, Имя угрозы или Командная строка

Введите хэш файла, отпечаток сертификата (хэш), точное название угрозы и командную строку в зависимости от правила исключения. Вы можете использовать один элемент для исключения.

3. Выберите методы сканирования, к которым правило будет применяться. Некоторые исключения могут быть актуальны только для сканирования при доступе, некоторые только для сканирования по запросу, некоторые только для ATC/IDS,а другие могут быть рекомендованы для всех трех модулей.
4. При необходимости нажмите кнопку **Показать замечания**, чтобы добавить заметку о правиле в столбец **Замечания**.
5. Нажмите кнопку ⊕ **Добавить**.

   Новое правило будет добавлено в список.

Чтобы удалить правило из списка, нажмите соответствующую кнопку ⊗ **Удалить**.

Важно
Пожалуйста, обратите внимание, что исключения сканирования по запросу НЕ будут применяться к контекстному сканированию. Контекстное сканирование запускается при нажатии правой кнопки мыши на файле или папке и выборе **Сканировать с Bitdefender Endpoint Security Tools**.

Импорт и экспорт исключений

Если вы намерены использовать правила исключений в других политиках, вы можете их экспортировать и импортировать.

Чтобы экспортировать пользовательские исключения:

1. Нажмите **Экспорт** в верхней части таблицы исключений.
2. Сохраните файл CSV на вашем компьютере. В зависимости от настроек вашего браузера, файл может автоматически загрузится или вам будет предложено сохранить его в определенное место.

Каждая строка в файле CSV соответствует одному правилу с полями в следующем порядке:

```
<exclusion type>, <object to be excluded>, <modules>
```

Доступные значения для полей в файле CSV:

Тип исключения:

- 1, для исключений файлов
- 2, для исключений папок
- 3, для исключений расширений
- 4, для исключений процессов
- 5, для исключений хеша файла
- 6, для исключений хеша сертификата
- 7, для исключений по имени угрозы
- 8, для исключений командной строки

Исключаемый объект:

Путь или расширение файла

Модули:

- 1, для сканирования по запросу
- 2, для сканирования при доступе
- 3, для всех модулей
- 4, для ATC/IDS

Например, файл CSV, содержащий исключения, может выглядеть следующим образом:

```
1,"d:\\temp",1
1,%WinDir%,3
4,"%WINDIR%\\system32",4
```

Примечание
Пути Windows должны иметь двойной обратный слеш (\). Например, `%WinDir%\\System32\\LogFiles`.

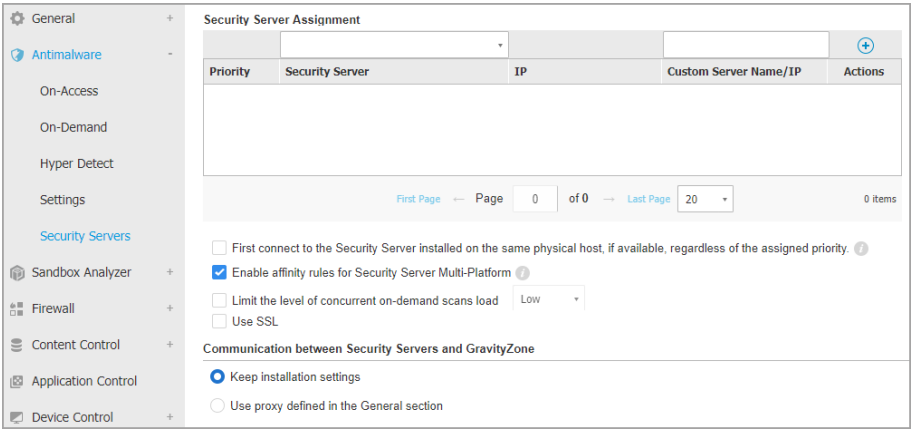
Чтобы ипортировать пользовательские исключения:

1. Нажмите **Импорт**. Откроется окно **Import Policy Exclusions**.
2. Нажмите **Добавить** и затем выберите файл CSV.
3. Нажмите **Сохранить**. Таблица заполняется корректными правилами. Если файл CSV содержит некорректные правила, предупреждение проинформирует вас о соответствующих номерах строк.

Серверы безопасности (Security Server)

В данном разделе вы можете настроить:

- Назначение Security Server
- Специальные настройки Security Server



Политики - Компьютеры и виртуальные машины - Защита от вредоносного ПО - Серверы безопасности

Назначение Security Server

Вы можете назначить один или несколько Security Server целевым конечным точкам и установить приоритет, с которым конечные точки будут выбирать Security Server для отправки запросов сканирования.

Примечание
Рекомендуется использовать Security Servers для сканирования виртуальных машин или компьютеров с ограниченными ресурсами.

Чтобы назначить Security Server целевым конечным точкам, добавьте Security Servers, которые вы хотите использовать, в таблицу **Назначение Security Server**, выполнив следующие действия:

1. Нажмите на выпадающий список **Security Server** и выберите Security Server.
2. Если Security Server находится в DMZ или за сервером NAT, введите FQDN или IP-адрес сервера NAT в поле **Пользовательское имя сервера/ IP-адрес**.

   Важно
   Убедитесь, что переадресация портов правильно настроена на сервере NAT, чтобы трафик от конечных точек мог доходить до Security Server. Подробнее о портах см. Коммуникационные порты GravityZoneБаза знаний.

3. Нажмите кнопку ⊕ **Добавить** в столбце **Действия**.

   Security Server добавится в список.
4. Повторите предыдущие шаги, чтобы добавить другие Security Servers, если они доступны или необходимы.

Чтобы установить приоритет Security Servers:

1. Используйте стрелки вверх и вниз, доступные в столбце **Действия**, чтобы увеличить или уменьшить приоритет каждого Security Server.

   При назначении большего количества Security Servers, находящийся сверху будет иметь наибольший приоритет и будет выбран первым. Если этот Security Server недоступен или перегружен, выбирается следующий Security Server. Трафик сканирования перенаправляется на первый доступный и имеющий подходящую загрузку Security Server.

Чтобы удалить Security Server из списка, нажмите соответствующую кнопку ⊗ **Удалить** в столбце **Действия**.

Настройки Security Server

При назначении политики для Security Servers вы можете настроить следующие параметры:

- **Ограничить количество одновременных проверок по требованию**.

  Запуск нескольких задач сканирования по запросу на виртуальных машинах, использующих одно хранилище данных, может создать Сканирование вредоносных программ. Чтобы предотвратить это и разрешить одновременное выполнение только определенного количества задач сканирования:

  1. Выберите параметр **Ограничить количество одновременных проверок по требованию**.
  2. Выберите уровень разрешенных одновременных задач сканирования в выпадающем меню. Вы можете выбрать предопределенный уровень или ввести пользовательское значение.

     Формула для нахождения максимального количества задач сканирования для каждого предопределенного уровня:`N = a x MAX(b ; vCPUs - 1)`, где:

     - `N` = максимальное количество задач сканирования
     - `a` = коэффициент умножения, имеющий следующие значения: `1` - для Низкого; `2` - для Среднего; `4` - для Высокого
     - `MAX(b;vCPU-1)` = функция, которая возвращает максимальное количество слотов сканирования, доступных на Security Server.
     - `b` = количество слотов для сканирования по требованию, которое по умолчанию равно 4.
     - `vCPUs` = количество виртуальных процессоров, выделенныхSecurity Server

     Например:

     Для Security Server с 12 процессорами и Высоким уровнем одновременных сканирований, мы имеем:

     `N = 4 x MAX(4 ; 12-1) = 4 x 11 = 44` одновременных задач сканирования по запросу.

- **Включить правила привязки для Security Server Multi-Platform**

  Выберите поведение Security Server при переходе в режим обслуживания:

  – Если включено, Security Server остается привязанным к хосту и GravityZone отключает его. По окончанию обслуживания, GravityZone автоматически перезапускает Security Server.

    Данное поведение установлено по умолчанию.

  – Если отключено, Security Server переходит к другому хосту и продолжает работу. В данном случае, имя Security Server изменяется в Control Center для указания старого хоста. Измененное имя сохраняется до тех пор, пока Security Server не возвратится к первоначальному хосту.

    При достаточном количестве ресурсов, Security Server можете перейти на хост с другим установленным Security Server.

- **Использовать SSL**

  Активируйте эту функцию для шифрования подключения между целевыми конечными точками и указанными устройствами Security Server.

  По умолчанию, GravityZone использует самоподписанные сертификаты безопасности. Вы можете изменить их своими собственными сертификатами в **Настройка > Сертификаты** на странице Control Center. Для получения дополнительной информации см. главу «Настройка параметров Control Center» в Руководстве по установке.

- **Связь между Security Servers и GravityZone**

  Выберите один из доступных вариантов, чтобы задать параметры прокси-сервера для связи между выбранными машинами Security Server и GravityZone:

  – **Сохранить настройки установки**, чтобы использовать параметры прокси-сервера, определенные в установочном пакете.

  – **Использовать прокси, определенный в общем разделе**, чтобы использовать параметры прокси-сервера, определенные в текущей политике в разделе **Общее > Настройки**.

  – **Не использовать прокси-сервер**, когда целевые конечные точки не взаимодействуют с определенными компонентами Bitdefender через прокси-сервер.

7.2.3. Sandbox Analyzer

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов

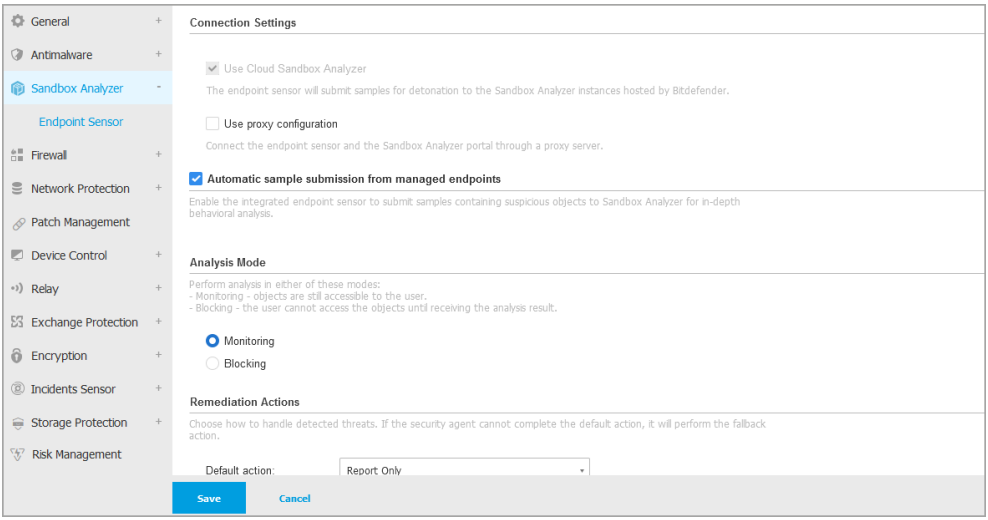
Sandbox Analyzer обеспечивает мощный уровень защиты от расширенных угроз, выполняя автоматический всесторонний анализ подозрительных файлов, которые еще не подписаны механизмами защиты от вредоносных программ Bitdefender.

В этом разделе вы можете настроить параметры Sandbox Analyzer для автоматической отправки через Bitdefender Endpoint Security Tools. Подробнее о ручной подаче см. «Manual Submission» (p. 477).

Примечание
Для получения информации о том, как Sandbox Analyzer нарушает правила HIPAA, обратитесь к разделу "GravityZone и HIPAA" в Руководстве по установке.

Датчик конечной точки

Bitdefender Endpoint Security Tools может выступать в качестве датчика подачи для Sandbox Analyzer с конечных точек Windows.



Политики > Sandbox Analyzer > Датчик конечной точки

Чтобы настроить параметры Sandbox Analyzer для автоматической отправки:

1. **Настройки соединения**. Датчик конечной точки настроен на отправку образцов в экземпляр Sandbox Analyzer по умолчанию, предоставленный Bitdefender, в зависимости от вашего региона.

   - **Использовать облако Sandbox Analyzer** - датчик конечной точки отправит образцы в экземпляр Sandbox Analyzer, размещенный Bitdefender, в зависимости от вашего региона.
   - **Использовать локальный экземпляр Sandbox Analyzer**- датчик конечной точки отправит образцы в экземпляр Sandbox Analyzer On-Premises. Выберите предпочтительный экземпляр Sandbox Analyzer из выпадающего меню.

   Если у вас есть сеть за прокси-сервером или брандмауэром, вы можете настроить прокси для подключения к Sandbox Analyzer, установив флажок **Используйте настройки прокси**.

   Вы должны заполнить следующие поля:

   - **Сервер** - IP-адрес прокси-сервера.
   - **Порт** - порт, используемый для подключения к прокси-серверу.

- **Имя польхователя** имя пользователя, опознаваемое прокси-сервером.
- **Пароль** - корректный пароль указанного пользователя.

2. Выберите **Автоматическая отправка файлов с управляемых конечных точек**, чтобы включить автоматическую передачу подозрительных файлов в Sandbox Analyzer.

   Важно

   - Sandbox Analyzer требует сканирование при доступе. Убедитесь, что включен модуль **Антивирусная защита > Сканирование по доступу**.
   - Sandbox Analyzer использует те же цели и исключения, которые определены в **Антивирусная защита > Сканирование при доступе**. При настройке Sandbox Analyzer внимательно просмотрите параметры сканирования при доступе.
   - Чтобы предотвратить ложные срабатывания (неправильное обнаружение законных приложений), вы можете настроить исключения по имени файла, расширения, размеру файла и пути к файлу. Для получения дополнительной информации о сканировании по доступу см.«Защита от вредоносного ПО» (p. 166).
   - Предел загрузки для любого файла или архива составляет 50 МБ.

3. Выберите **Режим анализа** . Доступны две опции:
   - **Мониторинг**. Пользователь может получить доступ к файлу во время анализа безопасной среды, но ему не рекомендуется выполнять его до получения результата анализа.
   - **Блокировка**. Пользователь не может выполнить файл, пока результат анализа не будет возвращен в конечную точку из кластера Sandbox Analyzer через портал Sandbox Analyzer.
4. Укажите **Действия по восстановлению** . Они берутся во внимание когда Sandbox Analyzer обнаруживает угрозу. Для каждого режима анализа вам предоставляется двойная настройка, состоящая из одного действия по умолчанию и одного резервного действия. Sandbox Analyzer сначала выполняет действие по умолчанию, а затем возвращается, если первое не может быть выполнено.

   При первом доступе к этому разделу доступны следующие настройки:

Примечание
Наилучшим решением будет предпринять действия по исправлению в этой конфигурации.

- В режиме **Мониторинг** действием по умолчанию является **Только отчет** , при этом аварийное действие отключено.
- В режиме **Блокировка** действием по умолчанию является **Карантин** , при этом аварийным действием является действие **Удалить**.

Sandbox Analyzer предоставляет вам следующие действия по исправлению:

- **Обезвредить**. Данное действие удаляет вредоносный код из зараженных файлов.
- **Удалить**. Данное действие полностью удаляет обнаруженный файл с диска.
- **Карантин**. Данное действие перемещает зараженные файлы из исходного расположения в папку карантина. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице **Карантин** на Control Center.
- **только отчет**. Sandbox Analyzer анализирует только обнаруженные угрозы без каких-либо других действий.

Примечание
В зависимости от действия по умолчанию резервное действие может быть недоступно.

5. В разделе **Предварительная фильтрация контента** настройте уровень защиты от потенциальных угроз. Датчик конечной точки имеет встроенный механизм фильтрации содержимого, который определяет необходимость проверки подозрительного файла в Sandbox Analyzer.

   Поддерживаемые типы объектов: приложения, документы, сценарии, архивы, электронные письма. Для получения дополнительной информации о поддерживаемых типах объектов см. «Типы Файлов Поддерживаемые Предварительной Фильтрацией Контента при Автоматической Отправке» (p. 512).

Используйте главный переключатель в верхней части списка угроз, чтобы выбрать уникальный уровень защиты для всех типов объектов, или выберите индивидуальные уровни для точной настройки защиты.

Установка модуля на определенном уровне приведет к определенному количеству отправленных образцов:

- **Разрешимый**. Датчик конечной точки автоматически отправляет Sandbox Analyzer только объекты с наибольшей вероятностью вредоносности и игнорирует остальные объекты.
- **Обычный**. Датчик конечной точки находит баланс между отправленными и игнорируемыми объектами и отправляет в Sandbox Analyzer оба объекта с большей и с меньшей вероятностью быть вредоносными.
- **Агрессивный**. Датчик конечной точки передает Sandbox Analyzer практически все объекты, независимо от их потенциального риска.

В отдельном поле вы можете определить исключения для типов объектов, которые вы не хотите отправлять в Sandbox Analyzer.

Вы также можете определить ограничения по размеру отправленных объектов, установив соответствующий флажок и введя требуемые значения от 1 КБ до 50 МБ.

Sandbox Analyzer поддерживает локальную отправку файлов через конечные точки с ролью ретрансляции, которые могут подключаться к различным адресам портала Sandbox Analyzer в зависимости от вашего региона. Подробнее о настройках конфигурации ретранслятора см. «Ретранслятор» (p. 255).

Примечание
Прокси-сервер, настроенный в настройках соединения Sandbox Analyzer, переопределит любые конечные точки с ролью ретрансляции.

7.2.4. Брандмауэр

Примечание
Этот модуль доступен для Windows для рабочих станций.

Брандмауэр служит для защиты конечных точек от попыток установления несанкционированных входящих и исходящих соединений.

Функциональность брандмауэра основана на сетевых профилях. Профили основаны на уровнях доверия, которые должны быть определены для каждой сети.

Брандмауэр обнаруживает каждое новое подключение, сравнивает информацию адаптера с информацией существующих профилей и применяет подходящий профиль. Для получения более подробной информации о применении профилей, обратитесь к «Настройки сети» (p. 217).

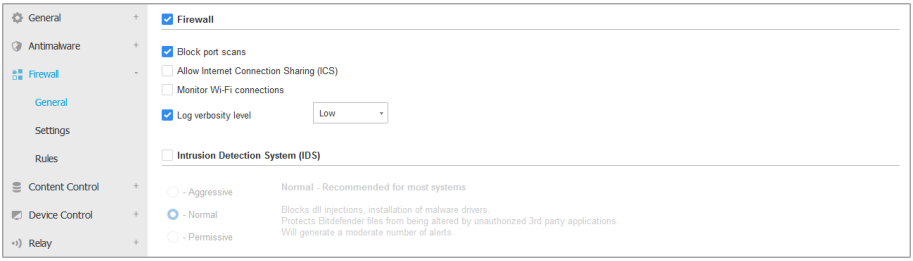
Важно
Модуль файрвола доступен только для поддерживаемых рабочих станций Windows.

Настройки объединены в следующие разделы:

- Основные
- Настройки
- Правила

Основные

В этом разделе можно включить или отключить файрвол Bitdefender и настроить общие параметры.



- **Брандмауэр.** Используйте флажок, чтобы включить или выключить брандмауэр.

Предупреждение
Если вы отключите брандмауэр, компьютеры будут уязвимы к сетевым и Интернет-атакам.

- **Блокировать сканирование портов.** Сканирование портов часто используется хакерами для обнаружения открытых портов на вашем компьютере. Они могут проникнуть в ваш компьютер, если найдут уязвимый или менее защищенный порт.
- **Разрешить использование общего доступа к Интернет (ICS).** Выберите эту опцию, чтобы разрешить файрволу пропускать трафик общего доступа к сети интернета.

  Примечание
  Эта опция автоматически не разрешает совместный доступ к Интернет на системах пользователей.

- **Отслеживать Wi-Fi подключения.** Агент безопасности Bitdefender может сообщать пользователям, подключенным к сети Wi-Fi, о подключении к сети нового компьютера. Для отображения таких уведомлений на экране пользователя, выберите эту опцию.
- **Уровень детализации сообщений.** Агент безопасности Bitdefender ведет журнал событий, касающихся использования модуля файрвола (включение/выключение, блокировка трафика, изменение параметров) или генерируется обнаруженными данным модулем действиями (сканирование портов, блокировка попыток соединения или трафика согласно правилам). Выберите опцию из **Уровень детализации журнала**, чтобы указать, какую информацию должен накапливать журнал.
- **Система обнаружения вторжений.** Система обнаружения вторжений проверяет вашу систему на подозрительные действия (к примеру, неавторизированная попытка изменить файлы Bitdefender, DLL-инъекции, попытки кейлоггера и др.)

  Примечание
  Параметры политики системы обнаружения вторжений (IDS) применяются только к Endpoint Security (устаревшему агенту безопасности). Агент Bitdefender Endpoint Security Tools интегрирует возможности системы обнаружения вторжений на основе хоста в свой модуль Advanced Threat Control (ATC).

  Настройка системы обнаружения вторжений:

1. Используйте кнопку-флажок, чтобы включить или выключить систему обнаружения вторжений.
2. Выберите уровень безопасности, который лучше всего соответствует вашим потребностям (Интенсивный, Нормальный или Рекомендуемый). Используйте описание справа от шкалы, чтобы выбрать необходимый уровень.

Чтобы предотвратить срабатывание системы обнаружения вторжений на действия доверенных приложений, добавьте **ATC/IDS правило исключения процесса** для этого приложения в разделе **Защита от вредоносных программ > Настройки > Пользовательские исключения** .

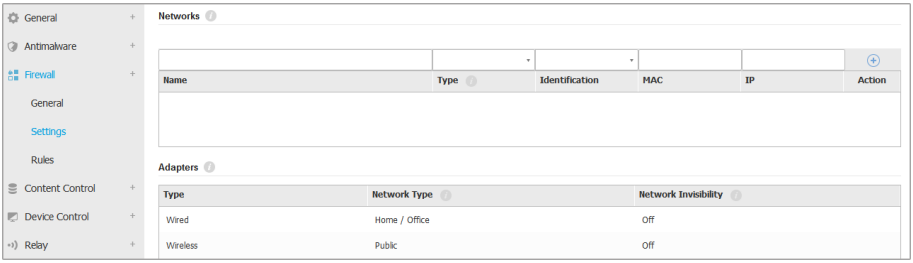
Важно
Система обнаружения вторжений доступна только для клиентов Endpoint Security.

Настройки

Файрвол автоматически применит подходящий профиль, основанный на уровне доверия. Вы можете установить различные уровни доверия для сетевых соединений в зависимости от архитектуры сети или типа адаптера, использующегося для установления сетевого соединения. Например, если внутри сети вашей компании существуют подсети, вы можете установить уровень доверия к каждой подсети.

Настройки расположены в следующих разделах:

- Сети
- Адаптеры



Политики - Настройки файрвола

Настройки сети

Если вы хотите, чтобы файрвол применял различные профили для разных сегментов сети вашей компании, вы должны указать управляемые сети в разделе **Networks**. Заполните поля в таблице **Сети**, как описано ниже:

- **Имя.** Введите имя, по которому вы сможете распознавать сеть в списке.
- **Тип.** Выберите из меню тип профиля, назначаемый сети.

  Агент безопасности Bitdefender автоматически применяет один из четырех сетевых профилей для каждого обнаруженного сетевого соединения на конечной точке, чтобы установить основные параметры фильтрации трафика. Типы профилей:

  - **Безопасная**. сеть Надежная сеть, в которой файрвол отключается на определенных адаптерах.
  - **Домашяя/Офисная** сеть Домашняя или офисная сеть, в которой разрешается весь трафик "в" и "из" компьютеров в локальной сети, а остальной трафик фильтруется.
  - **Общественная** Сеть Весь трафик фильтруется.
  - **Небезопасная**. Ненадежная сеть, в которой блокируется весь сетевой трафик и доступ в Интернет через соответствующий адаптер.
- **Идентификация.** Выберите из меню способ, через который сеть будет идентифицирована агентом безопасности Bitdefender. Сети могут быть определены тремя способами: **DNS**, **Gateway** и **Network**.
  - **DNS**: идентифицирует все конечные точки, используя указанный DNS.
  - **Gateway**: идентифицирует все конечные точки связанные через указанный шлюз.
  - **Network**: идентифицирует все конечные точки из указанного сегмента сети, определенных по их сетевому адресу.
- **MAC**. Используйте это поле, чтобы указать MAC-адрес DNS-сервера или шлюза, разделяющего сети, в зависимости от выбранного метода идентификации.

  Вы должны ввести MAC-адрес в шестнадцатеричном формате, разделенный дефисом (-) или двоеточием (:). Например, оба данных адреса будут действительны `00-50-56-84-32-2b` и `00:50:56:84:32:2b`.

- **IP.** Используйте это поле, чтобы указать конкретные IP-адреса в сети. Формат IP-адреса зависит от способа идентификации:
  - **Сеть.** Введите номер сети в формате CIDR. Например, `192.168.1.0/24`, где `192.168.1.0` это адрес сети и `/24` это маска сети.
  - **Шлюз.** Введите IP-адрес шлюза.
  - **DNS.** Введите IP-адрес DNS-сервера.

После того как вы задали характеристики сети, нажмите кнопку **Добавить** в правой части таблицы, чтобы добавить ее в список.

Настройки адаптеров

Если будет обнаружена сеть, которая отсутствует в списке **Сети**, агент безопасности Bitdefender определит тип сетевого адаптера и применит к нему соответствующий профиль подключения.

Поля в таблице **Адаптеры** обозначают следующее:

- **Тип.** Отображает тип сетевых адаптеров. Агент безопасности Bitdefender может обнаруживать три предопределенных типа адаптеров: проводной (**Wired**), беспроводной (**Wireless**) и виртуальный (**Virtual** - виртуальная частная сеть).
- **Тип сети.** Описывает профиль сети, назначенный определенному типу адаптера. Сетевые профили описаны в разделе настроек сети. Нажав на тип сети, вы сможете изменить настройки.

  Если вы выберите **Let Windows decide**, то для любого нового подключения к сети, обнаруженного после применения политики, агент безопасности Bitdefender применит профиль файрвола, основанный на сетевой классификации Windows, не обращая внимания на настройки из раздела **Адаптеры**.

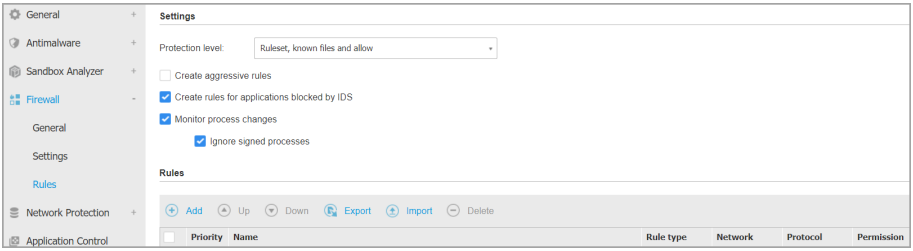
  Если обнаружение, основанное на управлении сетями Windows, даст сбой, будет применена попытка основного обнаружения. Общий профиль используется, когда назначен сетевой профиль **Общественный** и настройки видимости установлены в состояние **Включен**.

  Когда конечная точка, подключенная в Active Directory, подключается к домену, для профиля брандмауэра автоматически устанавливается значение **Дом/офис**, а для параметров скрытности - **Удаленный**. Если компьютер не в домене, то это условие не применимо.

- **Сетевое Обнаружение.** Скрывает компьютер от вредоносного программного обеспечения и хакеров в сети или в Интернете. При необходимости настройте видимость компьютера в сети для каждого типа адаптера, выбрав один из следующих параметров:
  - **Да.** любой человек из локальной сети или Интернета может проверять и обнаруживать компьютер.
  - **Нет.** компьютер невидим как из локальной сети, так и из Интернета.
  - **Удаленный.** Компьютер не может быть обнаружен из сети Интернет. Любой желающий в локальной сети сможет пропинговать и обнаружить компьютер.

Правила

В этом разделе вы можете настроить правила доступа приложений к сети и для трафика данных, назначаемых файрволом. Обратите внимание, что имеющиеся параметры применяются только к **Домашний/Офисный** и **Общественный** профилям.



Политики - Настройки правил файрволла

Настройки

Вы можете настроить следующие параметры:

- **Уровень защиты.** Выбранный уровень защиты определяет логику принятия решений файрволом, используемую, когда приложения выдают запросы на доступ к сети и Интернет-услугам. Доступны следующие опции:

Применить правило и разрешить

Применяет существующие правила файрвола и автоматически разрешает все другие попытки соединений. Для каждой новой попытки соединения создается правило и добавляется к набору.

Применить правило и спросить

Применяет существующие правила файрвола и запрашивает у пользователя действия для всех других попыток подключения. Предупреждающее окно с подробной информацией о неизвестной попытке подключения будет отображено на экране пользователя. Для каждой новой попытки соединения создается правило и добавляется к набору.

Применить правило и запретить

Применяет существующие правила файрвола и автоматически запрещает все другие попытки соединения. Для каждой новой попытки соединения создается правило и добавляется к набору.

Применить правило для известных файлов и разрешить

Применяет существующие правила файрвола, автоматически разрешает попытки подключения, сделанные известными приложениями, и автоматически разрешает все другие неизвестные попытки подключений. Для каждой новой попытки соединения создается правило и добавляется к набору.

Применить правило для известных файлов и спросить

Применяет существующие правила файрвола, автоматически разрешает попытки подключения, сделанные известными приложениями, и запрашивает у пользователя действия для всех других неизвестных попыток подключения. Предупреждающее окно с подробной информацией о неизвестной попытке подключения будет отображено на экране пользователя. Для каждой новой попытки соединения создается правило и добавляется к набору.

Применить правило для известных файлов и запретить

Применяет существующие правила файрвола, автоматически разрешает попытки подключения, сделанные известными приложениями, и автоматически запрещает все другие неизвестные попытки подключения. Для каждой новой попытки соединения создается правило и добавляется к набору.

Примечание
Известные файлы представляют собой большую базу безопасных, надежных приложений, которая составляется и постоянно поддерживается Bitdefender.

- **Создать интенсивные правила.** При выборе данного параметра файрвол создаст правила для каждого процесса, который открывает приложения, запрашивающие доступ к сети или в Интернет.
- **Создать правила для приложений, заблокированных IDS.** При выборе данной опции файрвол автоматически создает правило **Отказать** каждый раз, когда система обнаружения вторжений блокирует приложение.
- **Мониторинг процесса изменений.** Выберите эту опцию если хотите проверять каждое изменившееся приложение, которое пытается подключиться к Интернет, дополнительным правилом, контролирующим его доступ в Интернет. Если приложение было изменено, новое правило будет создано в соответствии с существующим уровнем защиты.

Примечание
Как правило, изменения в приложения вносятся посредством обновлений. Однако существует риск того, что приложения могут быть изменены вредоносными программами с целю заражения локального компьютера и остальных компьютеров в сети.

Приложения с цифровой подписью считаются надежными и имеют более высокую степень безопасности. Вы можете выбрать **Игнорировать подписанные процессы**, автоматически позволяя измененным подписанным приложениям подключения к сети Интернет.

Правила

В таблице правил перечислены существующие правила файрвола, содержащие важную информацию о каждом из них:

- Имя правила или приложения, к которому оно относится.
- Протокол, к которому применяется правило.
- Действие правила (разрешить или запретить пакеты).
- Действия, которые вы можете выполнять над правилом.
- Приоритет правил.

Примечание

Существуют правила файрвола однозначно назначаемые политикой. Дополнительные правила могут быть сконфигурированы для компьютеров в результате применения параметров файрвола.

Существует ряд правил файрвола по умолчанию, позволяющий достаточно просто разрешить или запретить популярные типы трафика. Выберите нужную опцию из меню **Разрешение**.

Входящие ICMP/ICMPv6
Разрешите или запретите сообщения ICMP/ICMPv6. Сообщения ICMP часто используются хакерами для проведения атак на компьютерные сети. По умолчанию этот тип трафика разрешен.

Входящие подключения к удаленному рабочему столу
Разрешите или запретите другим компьютерам подключения к удаленному рабочему столу. По умолчанию этот тип трафика разрешен.

Отправка сообщений электронной почты
Разрешите или запретите отправку электронных сообщений по SMTP. По умолчанию этот тип трафика разрешен.

Веб-просмотр HTTP
Разрешите или запретите веб-просмотр по протоколу HTTP. По умолчанию этот тип трафика разрешен.

Сетевая печать
Разрешите или запретите доступ к принтерам в другой локальной сети. По умолчанию этот тип трафика запрещен.

Трафик проводника Windows по протоколу HTTP/FTP
Разрешите или запретите трафик HTTP и FTP из Windows Explorer. По умолчанию этот тип трафика запрещен.

Кроме правил по умолчанию, вы можете создать дополнительные правила файрвола для других приложений, установленных на конечных точках. Эти настройки предназначены для администраторов с хорошим уровнем знания сетей.

Чтобы создать и настроить новое правило, нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Обратитесь к этой теме для получения дополнительной информации.

Чтобы удалить правило из списка, выберите его и нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

Примечание
Вы не можете удалить или изменить правила файрвола по умолчанию.

Настройка пользовательских правил

Вы можете настроить два типа правил файрвола:

- **Правила, основанные на приложениях.** Такие правила применяются к конкретному программному обеспечению, найденному на клиентских компьютерах.
- **Правила, основанные на подключениях.** Такие правила распространяются на любые приложения или службы, которые используют сетевые подключения.

Чтобы создать и настроить новое правило, нажмите кнопку ⊕ **Добавить** в верхней части таблицы и выберите нужный тип правила из меню. Чтобы отредактировать существующее правило, щелкните на имя правила.

Доступна настройка следующих параметров:

- **Имя правила.** Введите имя, под которым правило будет отображаться в таблице правил (например, имя приложения, к которому применяется данное правило).
- **Путь приложения** (только для правил, основанных на приложениях). Вы должны указать путь к исполняемому файлу приложения на требуемых компьютерах.
  - Выберите из меню предопределенное месторасположение и завершите путь по мере необходимости. Например, приложение установлено в папке `Программные файлы`, выберите `%ProgramFiles%` и завершите путь, добавив обратную косую черту (\) и имя папки приложения.
  - Введите полный путь в поле редактирования. Желательно использовать системные переменные (в соответствующих случаях), чтобы быть уверенным, что путь действителен для всех нужных компьютеров.
- **Командная строка** (только для правил, основанных на приложениях). Если вы хотите, чтобы правило применялось только когда указанное приложение запущено определенной командой в интерфейсе командной

строки Windows, введите соответствующую команду в поле ввода. В противном случае оставьте это поле пустым.

- **Приложение MD5** (только для правил, основанных на приложениях). Если вы хотите, чтобы правило проверяло целостность данных файлов приложений, основанную на их MD5 хэш-коде, введите его в поле редактирования. В противном случае оставьте это поле пустым.
- **Локальный адрес.** Укажите локальный IP-адрес и порт, к которому будет применяться правило. Если у вас несколько сетевых адаптеров, вы можете снять флажок **Любой** и ввести определенный IP-адрес. Аналогично для фильтрации соединений по конкретному порту или диапазону портов, снимите флажок **Любой** и введите нужные порт или диапазон портов в соответствующем поле.
- **Удаленный адрес.** Укажите удаленный IP-адрес и порт, к которому будет применяться правило. Чтобы отфильтровать трафик к и от конкретного компьютера, снимите флажок **Любой** и введите его IP-адрес.
- **Применить это правило только для непосредственно подключенных компьютеров.** Вы можете фильтровать доступ на основе MAC-адресов.
- **Протокол.** Выберите IP-протокол, к которому будет применяться правило.
  - Если вы хотите, чтобы правило применялось ко всем протоколам, выберите **Любой**.
  - Если вы хотите применить правило к TCP, выберите **TCP**.
  - Если вы хотите применить правило к UDP, выберите **UDP**.
  - Если вы хотите, чтобы правило применялось к определенному протоколу, выберите этот протокол из меню **Другое**.

    Примечание

    Диапазоны IP-адресов выделяются Администрацией адресного пространства Интернет (IANA). Полный список выделенных IP-адресов можно найти на странице http://www.iana.org/assignments/protocol-numbers.

- **Направление.** Выберите направление трафика, к которому будет применяться правило.

Направление	Описание
Исх.	Правило будет применяться только к исходящему трафику.
Входящий	Правило применяется только ко входящему трафику.
Оба	Правило будет применяется и к входящему, и к исходящему трафику.

- **Версия IP.** Выберите версию IP (напр., IPv4, IPv6 или any), к которой будет применяться правило.
- **Сеть.** Выберите тип сети, для которого будет назначено правило.
- **Разрешение.** Выберите одно из доступных разрешений:

Разрешение	Описание
Разрешить	Указанному приложению будет разрешен доступ в сеть/Интернет при определенных обстоятельствах.
Запретить	Указанному приложению будет запрещен доступ в сеть/Интернет при определенных обстоятельствах.

Нажмите **Сохранить**, чтобы добавить правило.

Для правил, которые вы создали, используйте стрелки в правой части таблицы, чтобы установить каждому приоритет. Правило с более высоким приоритетом будет находиться в списке выше.

Правила импорта и экспорта

Вы можете экспортировать и импортировать правила брандмауэра, чтобы использовать их в других политиках или компаниях. Чтобы экспортировать правила:

1. Нажмите **Экспорт** в верхней части таблицы правил.
2. Сохраните файл CSV на вашем компьютере. В зависимости от настроек вашего браузера, файл может автоматически загрузится или вам будет предложено сохранить его в определенное место.

Важно

- Каждая строка в CSV-файле соответствует одному правилу и имеет несколько полей.
- Место правил брандмауэра в файле CSV определяет их приоритет. Вы можете изменить приоритет правила, перемещая всю строку.

Для набора правил по умолчанию вы можете изменить только следующие элементы:

- **Приоритет**. Установите приоритет правила в любом желаемом порядке, перемещая строку CSV.
- **Разрешение**. Измените поле `set.Permission`, используя доступные разрешения:
  - 1 для **Разрешить**
  - 2 за **Запретить**

Любые другие корректировки игнорируются при импорте.

Для пользовательских правил брандмауэра все значения полей настраиваются следующим образом:

Поле	Имя и значение
`ruleType`	**Тип правила**: 1 для **Правила приложений** 2 для **Правила подключений**
`тип`	Значение для этого поля не является обязательным.
`details.name`	**Имя правила**
`details.applictionPath`	**Путь приложения** (только для правил, основанных на приложениях)
`details.commandLine`	**Командная строка** (только для правил, основанных на приложениях)

Поле	Имя и значение
`details.applicationMd5`	**Приложение MD5** (только для правил, основанных на приложениях)
`settings.protocol`	**Протокол** 1 для **Любого** 2 для **TCP** 3 для **UDP** 4 для **Другого**
`settings.customProtocol`	Требуется только в том случае, если для **Протокола** установлено значение **Другой**. Для конкретных значений, рассмотрите эту страницу. Значения 0, 4, 6, 41, 61, 63, 68, 99, 114, 124, 34–37, 141–143 не поддерживаются.
`settings.direction`	**Направление**: 1 для **Оба** 2 для **Входящие** 3 для **Исходящие**
`settings.ipVersion`	**IP-версия**: 1 для **Любого** 2 для **IPv4** 3 для **IPv6**
`settings.localAddress.any`	**Локальный адрес** установлен на **Любой**. 1 для Правильного 0 или пустой для Неправильного

Поле	Имя и значение
`settings.localAddress.ipMask`	**Локальный адрес** установлен на **IP или IP/Mask**
`settings.remoteAddress.portRange`	**Удаленный адрес** имеет значение **Порт или диапазон портов**
`settings.directlyConnected.enable`	**Применять правило только к компьютерам с прямым подключением**. 1 для включен 0 для пуст или отключен
`settings.directlyConnected.remoteMac`	**Применять правило только к компьютерам с прямым подключением** с фильтром **MAC-адрес**.
`permission.home`	**Сеть**, к которой применяется правило: **Дом/Офис**: 1 для Правильного 0 для пустой или неправильной
`permission.public`	**Сеть**, к которой применяется правило, является **Общедоступной**: 1 для Правильного 0 для пустой или неправильной
`permission.setPermission`	Доступные разрешения: 1 для **Разрешить** 2 за **Запретить**

Чтобы импортировать правила:

1. Нажмите **Импорт** в верхней части таблицы правил.

2. В новом окне нажмите **Добавить** и выберите файл CSV.
3. Нажмите **Сохранить**. Таблица заполняется корректными правилами.

7.2.5. Защита сети

Используйте раздел «Защита сети», чтобы настроить параметры фильтрации содержимого, защиты данных для действий пользователей, включая просмотр веб-страниц, почтовых и программных приложений, а также обнаружение методов сетевых атак, которые пытаются получить доступ к определенным конечным точкам. Вы можете ограничить или разрешить веб-доступ и использование приложений, настроить параметры сканирования трафика, антифишинг и правила защиты данных.

Пожалуйста, обратите внимание, что настроенные параметры управления контентом будут применяться ко всем пользователям, которые вошли на рабочие станции.

Настройки объединены в следующие разделы:

- Основные
- Контроль контента
- Веб-защита
- сетевые атаки

Примечание

- Модуль Контент Контроля доступен для:
  - Windows для рабочих станций
  - ОС MAK
- Модуль Network Attack Defense доступен для:
  - Windows для рабочих станций
  - Windows для серверов

Важно

На macOS Контроль устройств использует расширение ядра или системы. Установка расширения ядра требует подтверждения пользователя на macOS High Sierra (10.13.x). Система уведомляет пользователя о том, что расширение системы от Bitdefender было заблокировано. Пользователь может разрешить это в настройках **Безопасность и конфиденциальность** . Пока пользователь не утвердит расширение системы Bitdefender, этот модуль не будет работать, а пользовательский интерфейс Endpoint Security for Mac покажет критическую проблему, запрашивающую утверждение.

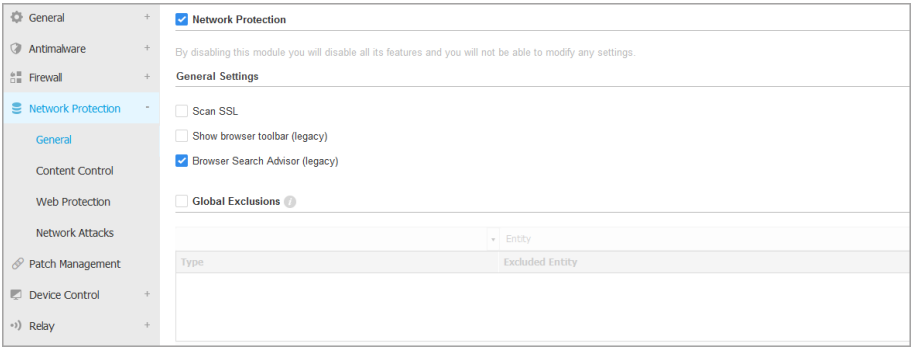
Чтобы исключить вмешательство пользователя, вы можете предварительно утвердить расширение Bitdefender, занеся его в белый список с помощью инструмента управления мобильными устройствами. Подробнее о расширениях Bitdefender см. эту статью базы знаний .

Основные

На этой странице вы можете настроить такие параметры, как включение или отключение функций и настроить исключения.

Настройки объединены в следующие разделы:

- Общие настройки
- Глобальные исключения



Политики - Защита сети - Общее

Общие настройки

- **Сканировать SSL**. Выберите эту опцию, если вы хотите, чтобы веб-трафик SSL (Secure Sockets Layer) проверялся защитными модулями агента безопасности Bitdefender.
- **Показать панель инструментов браузера (старая версия)**. Панель Bitdefender информирует пользователей о рейтинге безопасности веб-страниц, которые они просматривают. Панель инструментов Bitdefender отличается от стандартной панели инструментов браузера. В браузере появляется только небольшой значок в верхней части каждой веб-страницы. Нажатие на значок открывает панель инструментов.

В зависимости от того, как Bitdefender классифицирует веб-страницу, одна из следующих оценок отображается в левой части панели:

- Сообщение "This page is not safe"(страница небезопасна) появляется на красном фоне.
- Сообщение "Caution is advised" (требуется осторжность) появляется на оранжевом фоне.
- Сообщение "This page is safe" (страница безопасна) появляется на зеленом фоне.

Примечание

- Эта опция недоступна для macOS.
- Эта опция удалена из Windows, начиная с новых установок Bitdefender Endpoint Security Tools версии 6. 6. 5. 82.

- **Поисковой советник браузера (устаревший).** Поисковой Советник оценивает результаты поисковых систем Google, Bing и Yahoo!, а также ссылки из Facebook и Twitter, поместив значок перед каждым результатом. Используемые значки и их значение:

  Эту веб-страницу посещать не следует.
  Данная веб-страница может содержать опасную информацию. Соблюдайте осторожность, если вы решите ее посетить.
  Эта страница безопасна для посещения.

Примечание

- Эта опция недоступна для macOS.
- Эта опция удалена из Windows, начиная с новых установок Bitdefender Endpoint Security Tools версии 6. 6. 5. 82.

Глобальные исключения

Вы можете пропустить определенный трафик при проверке на наличие вредоносных программ, пока включены параметры **Защита сети**.

Примечание
Эти исключения применяются к **Сканированию трафика** и **Антифишингу** в разделе **Веб-защита**, и **Network Attack Defense** в разделе **Сетевые атаки**.

Исключения **Защиты данных** настраиваются отдельно, в разделе **Контроль контента**.

Чтобы определить исключение:

1. Выберите тип исключения из меню.
2. В зависимости от типа исключения, задайте содержимое трафика, которое будет исключено из сканирования, следующим образом:
   - **IP/mask**. Введите IP-адрес или IP-маску, для которой вы не хотите сканировать входящий и исходящий трафик, включая методы сетевой атаки.
   - **URL**. Исключает из сканирования указанные веб-адреса. Обратите внимание, что исключения на основе URL применяются по-разному для соединений HTTP и HTTPS, как описано ниже.

     Вы можете определить исключение на основе URL следующим образом:

     – Введите определенный URL, такой как `www.example.com/example.html`
       - В случае с HTTP-соединениями, только конкретный URL будет исключен из процесса сканирования.
       - Для HTTPS-соединений, добавление конкретного URL исключит целый домен и любые его субдомены. Следовательно, в этом случае вы можете указать домен, который следует исключить из сканирования.

     – Используйте подстановочные знаки для определения шаблонов веб-адресов (только для HTTP-соединений).

       Важно
       Исключения с подстановочными знаками не работают для соединений HTTPS.

       Можно использовать следующие подстановочные символы:
       - Двойная звездочка (**) заменяет неопределенное количество символов.
       - Одна звездочка (*) заменяет ноль или более символов между разделителями пути.

- Знак вопроса (?) заменяет ровно один символ. Вы можете использовать несколько вопросительных знаков, чтобы задать любую возможную комбинацию из определенного количества символов. Например, ??? заменит любую комбинацию ровно из трех символов.

Примечание
Этот параметр доступен как в Control Center, так и в настройках политики привилегированного пользователя в разделе **Antimalware** > **Настройки** > **Пользовательские исключения**.

В следующей таблице вы можете найти несколько примеров синтаксиса для указания веб-адресов (URLs).

Синтаксис	Применимость исключений
**\example.txt	Любой файл с именем example.txt будет исключен (независимо от его местоположения на конечной точке).
www.example*	Любой URL начинающийся с www.example вне зависимости от доменного расширения. Исключение не будет применяться к поддоменам указанного веб-сайта, например, subdomain.example.com.
*example.com	Любой URL заканчивающийся на example.com, включая их субдомены.
example.com	Любой URL, который содержит указанную строку.
*.com	Любой веб-сайт, имеющий доменное расширение .com, включая их субдомены. Используйте этот синтаксис, чтобы исключить из сканирования целые домены верхнего уровня.
www.example?.com	Любой веб-адрес, начинающийся с www.example?.com, где ? заменяет один любой символ. Это могут быть сайты:

Синтаксис	Применимость исключений
	`www.example1.com` или `www.exampleA.com` и др.

Примечание
Вы можете использовать относящиеся к протоколу URL.

- **Application**. Исключает из сканирования указанный процесс или приложение. Чтобы определить исключения при сканировании приложений:
  - Введите полный путь к приложению. Например, `C:\Program Files\Internet Explorer\iexplore.exe`
  - Используйте переменные среды, чтобы определить точный путь к приложению. Например: `%programfiles%\Internet Explorer\iexplore.exe`
  - Используйте маски, чтобы указать любые приложения, соответствующие определенному шаблону имени. Например:
    - `c*.exe` соответствует всем приложениям, начинающимся с "c" (chrome.exe).
    - `??????.exe` соответствует всем приложениям с именем, которое состоит из шести символов (chrome.exe, safari.exe и т.д.).
    - `[^c]*.exe` соответствует всем приложениям, кроме тех, которые начинаются с "c".
    - `[^ci]*.exe` соответствует всем приложениям, кроме тех, которые начинаются с "c" или "i".

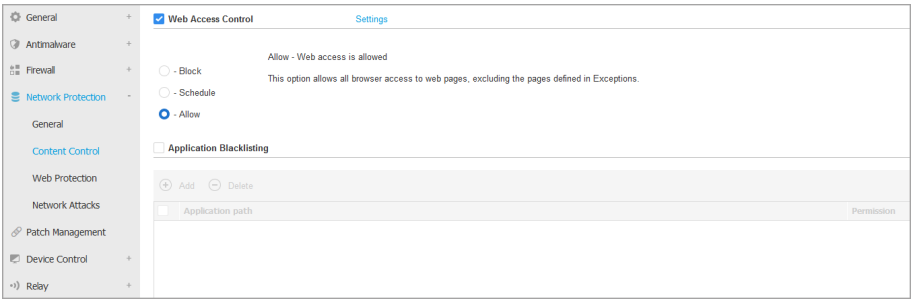
3. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.

Чтобы удалить объект из списка, нажмите соответствующую кнопку ⊗ **Удалить**.

Контроль контента

Настройки Контент Контроля организованы в следующие разделы:

- Управление веб-доступом
- Application Blacklisting
- Защита данных



Управление веб-доступом

Управление веб-доступом позволяет разрешить или запретить веб-доступ пользователям или приложениям в определенные интервалы времени.

Веб-страницы, заблокированные модулем управления веб-доступом, не будут отображаться в браузере. Вместо этого будет отображаться веб-страница по умолчанию, сообщающая пользователю о том, что запрашиваемая веб-страница была заблокирована модулем управления веб-доступом.

Используйте переключатель, чтобы включить или выключить **Web Access Control**.

У вас есть три возможных варианта:

- Выберите **Разрешить**, чтобы всегда предоставлять доступ в интернет.
- Выберите **Блокировать**, чтобы всегда запрещать доступ в интернет.
- Выберить **Запланировать**, чтобы ввести временные ограничения на веб-доступ по подробному расписанию.

Если вы выберете разрешить или запретить веб-доступ, можно настроить исключения в этих действиях для целых веб-категорий или только для определенных веб-адресов. Нажмите **Настройки**, чтобы настроить расписание веб-доступа и исключения, следующим образом:

Проверка по расписанию

Чтобы ограничить доступ к сети Интернет в определенное время дня еженедельно:

1. Выберите из сетки временные интервалы, в течение которых вы хотите запретить доступ в Интернет.

Можно щелчком мыши отметить отдельные клетки или нажать и расширить ее, чтобы задать более длительный период. Нажмите еще раз на клетку, чтобы изменить выбор.

Чтобы создать новый интервал, нажмите **Разрешить всем** или **Блокировать все**, в зависимости от типа ограничения, которое вы хотите реализовать.

2. Нажмите **Сохранить**.

Примечание
Агент безопасности Bitdefender будет обновляться каждый час независимо от блокировки веб-доступа.

Категории

Веб-фильтр по категориям это динамическая фильтрация доступа к сайтам на основе их содержимого. Вы можете использовать веб-Фильтр по категориям для создания исключений в выбранных действиях управления веб-доступом (Allow или Block) для целых веб-категорий (таких как игры, контент для взрослых или онлайн сети).

Чтобы настроить веб-фильтр по категориям:

1. Включите **Фильтр веб-категорий**.
2. Для быстрой настройки, выберите один из предустановленных профилей (**Интенсивный**, **Нормальный** или **Рекомендуемый**). Используйте описание справа от шкалы, чтобы выбрать необходимый уровень. Вы можете просмотреть предопределенные действия для доступных веб-категорий, раскрыв раздел **Правила сети**, размещенный ниже.
3. Если параметры по умолчанию вам не подходят, вы можете создать пользовательский фильтр:
   a. Выберите **Пользователь**.
   b. Нажмите **Правила сети**, чтобы раскрыть соответствующий раздел.
   c. Найдите категорию, которая вам нужна, в списке и выберите нужное действие из меню. Дополнительную информацию о доступных категориях веб-сайтов см. В этой статье базы знаний .

4. Выберите вариант **Обработать веб-категории как исключения для веб-доступа** , если вы хотите игнорировать существующие настройки веб-доступа и применять только фильтр веб-категорий.
5. Сообщение по умолчанию, отображаемое для пользователя,дает доступ к ограниченным веб-сайтам, также содержит категорию, которой соответствует содержимое веб-сайта. Снимите флажок **Показывать подробные оповещения на клиенте** , если вы хотите скрыть эту информацию от пользователя.

   Примечание
   Эта опция недоступна для macOS.

6. Нажмите **Сохранить**.

Примечание

- Разрешение **Разрешить** для указанных веб-категорий также будет учтено во время блокировки веб-доступа модулем управления.
- Разрешение **Разрешить** работает только тогда, когда веб-доступ запрещен модулем управления, в то время как разрешение **Блокировать** работает только тогда, когда веб-доступ разрешен.
- Вы можете переопределить разрешения категорий для отдельных веб-адресов, добавив их с противоположными разрешениями в **Контроль веб-доступа > Настройки > Исключения**. Например, если веб-адрес заблокирован веб-фильтром категории, можно добавить веб-правило для этого адреса с разрешением **Разрешить**.

Исключения

Вы также можете задать веб-правила по блокировке или разрешению определенных веб-адресов, переопределив существующие настройки модуля управления веб-доступом. Например, пользователи смогут получить доступ к определенной веб-странице, даже если веб-браузинг заблокирован модулем управления веб-доступом.

Чтобы создать веб-правило:

1. Включите опцию **Использовать исключения**.
2. Введите адрес, который вы хотите разрешить или запретить в поле **Веб-адрес**.

3. Выберите **Разрешить** или **Блокировать** из меню **Разрешение**.
4. Нажмите на кнопку ⊕ **Добавить** в правой части таблицы, чтобы добавить адрес в список исключений.
5. Нажмите **Сохранить**.

Чтобы изменить веб-правило:

1. Нажмите веб-адрес, который вы хотите отредактировать.
2. Измените существующий URL.
3. Нажмите **Сохранить**.

Чтобы удалить веб-правило, нажмите соответствующую кнопку ⊗ **Удалить**.

Application Blacklisting

В этом разделе вы можете настроить "черный" список приложений, который поможет вам полностью заблокировать или ограничить доступ пользователей к приложениям на своих компьютерах. Таким образом можно заблокировать игры, мультимедиа и программы обмена мгновенными сообщениями, а также другие категории программного обеспечения и вредоносных программ.

Чтбоы настроить "черный" список приложений:

1. Включите опцию **Черный список приложений**.
2. Укажите приложения, к которым вы хотите ограничить доступ. Чтобы ограничить доступ к приложению:
   a. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Появится окно конфигурации.
   b. Вы должны указать путь к исполняемому файлу приложения на требуемых компьютерах. Существует два способа сделать это:
      - Выберите из меню предопределенное местоположение и завершите путь по мере необходимости. Например, для приложения, установленного в папке `Программные файлы`, выберите `%ProgramFiles` и завершите путь, добавив обратную косую черту (\) и имя папки приложения.
      - Введите полный путь в поле редактирования. Желательно использовать системные переменные (где это возможно), чтобы путь был действительным для всех выбранных компьютеров.

c. **Планировщик доступа**. Еженедельное расписание доступа к приложениям в определенное время дня:
   - Выберите из сетки временные интервалы, в течение которых вы хотите, чтобы доступ к приложению был заблокирован. Можно щелчком мыши отметить отдельные клетки или нажать и расширить ее, чтобы задать более длительный период. Нажмите еще раз на клетку, чтобы изменить выбор.
   - Чтобы создать новый отбор, нажмите **Разрешить все** или **Блокировать все**, в зависимости от типа ограничения, которое вы хотите реализовать.
   - Нажмите **Сохранить**. Новое правило будет добавлено в список.

Чтобы удалить правило из списка, выберите его и нажмите кнопку ⊗ **Удалить** в верхней части таблицы. Чтобы отредактировать существующее правило, щелкните на него, чтобы открыть окно настроек.

Защита данных

Защита данных предотвращает несанкционированное разглашение конфиденциальных данных, основываясь на определенных правилах, заданных администратором.

Примечание
Данный компонент недоступен для macOS.

Вы можете создать правила для защиты любой части личной или конфиденциальной информации, такой как:

- Персональная информация заказчика
- Названия и ключевые детали, разрабатываемых продуктов и технологий
- Контактная информация руководителей компании

Защищаемая информация может включать имена, номера телефонов, кредитные карты и информацию о банковских счетах, адреса электронной почты и так далее.

На основании правил защиты данных, которые вы создаете, Bitdefender Endpoint Security Tools сканирует веб и исходящий трафик электронной почты для конкретных символьных строк (например, номер кредитной карты). Если будет найдено совпадение, соответствующая веб-страница или сообщение электронной почты заблокируется, чтобы предотвратить отправку

защищаемых данных. Пользователь будет немедленно оповещен о действиях, предпринятых Bitdefender Endpoint Security Tools, через веб-страницу с предупреждением или сообщением электронной почты.

Чтобы настроить защиту данных:

1. Отметьте соответствующий флажок, чтобы включить защиту данных.
2. Создайте правила защиты для всех конфиденциальных данных, которые необходимо защитить. Чтобы создать правило:
   a. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Появится окно конфигурации.
   b. Введите имя, под которым правило будет отображаться в таблице правил. Выберите подходящее имя, чтобы вы или другой администратор мог легко определить назначение этого правила.
   c. Выберите тип данных, которые вы хотите защитить.
   d. Введите данные, которые вы хотите защитить (например, номер телефона представителя компании, или внутреннее имя нового продукта, над которым работает компания). Это может быть любая комбинация слов, цифр или строк, состоящих из буквенно-цифровых и специальных символов (например, @, # или $) принимается.

      Введите по меньшей мере пять символов для того, чтобы избежать ошибочной блокировки сообщений электронной почты и веб-страниц.

      Важно

      Данные будут храниться в зашифрованном виде на защищаемых конечных точках, но эту информацию можно будет увидеть под вашим аккаунтом в Control Center. Для дополнительной безопасности не вводите полные данные, которые вы хотите защитить. В этом случае, вы должны очистить опцию **Совпадение целых слов**.

   e. Настройте требуемые параметры сканирования трафика.
      - **Веб сканирование (HTTP traffic)** - сканирует HTTP (веб) трафик и блокирует исходящие данные, которые соответствуют данным правилам.

- **Email сканирование (SMTP traffic)** - сканирует SMTP (почта) трафик и блокирует исходящие сообщения электронной почты, содержащие данные правил.

Вы можете выбрать: применять правило только в случае если совпадение произойдет по всему слову целиком или же если совпадение произойдет по нахождению искомой строки.

f. Нажмите **Сохранить**. Новое правило будет добавлено в список.

3. Настройте исключения в правилах защиты данных так, чтобы пользователи могли отправлять защищаемые данные разрешенным веб-сайтам и получателям. Исключения могут быть применены в глобальном масштабе (для всех правил) или только для определенных правил. Чтобы добавить исключение:
   a. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Появится окно конфигурации.
   b. Введите веб-адрес или адрес электронной почты пользователей, которым разрешено раскрывать защищаемые данные.
   c. Выберите тип исключения (веб-адрес или адрес электронной почты).
   d. Из таблицы **Правила**, выберите правило(а) защиты данных, для которого это исключение следует применять.
   e. Нажмите **Сохранить**. Новое правило исключений будет добавлено в список.

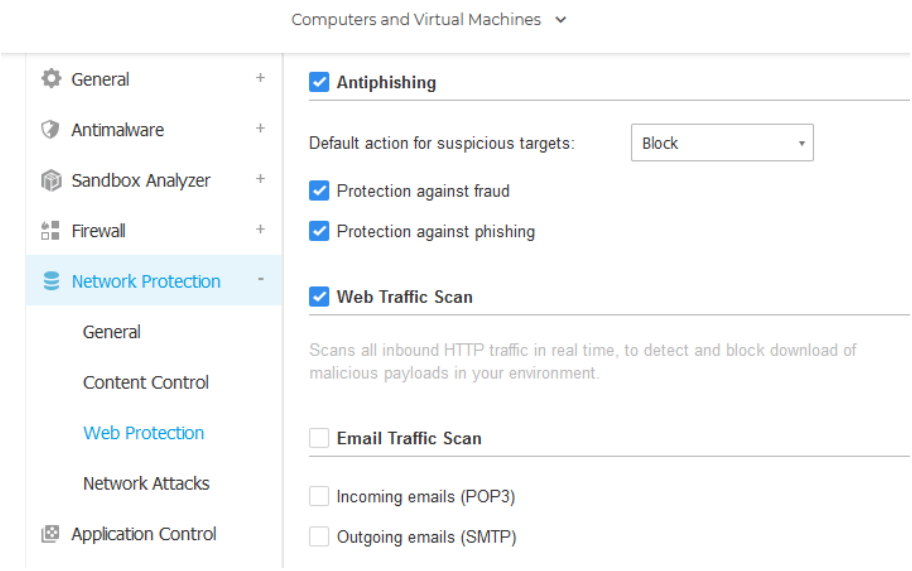
Примечание
Если письмо, содержащее блокируемые данные, адресовано нескольким получателям, для которых были определены исключения, они его получат.

Чтобы удалить правило или исключения из списка, нажмите соответствующую кнопку ⊗ **Удалить** в правой части таблицы.

Веб-защита

На этой странице настройки организованы в следующие разделы:

- Антифишинг
- Сканирование веб-трафика
- Сканирование трафика электронных писем



Политики - Защита сети - Веб-защита

Антифишинг

Защита от фишинга автоматически блокирует известные фишинговые веб-страницы, чтобы пользователи случайно не раскрыли частную или конфиденциальную информацию интернет-мошенникам. При этом вместо фишинговых веб-страниц отображается особая страница предупреждения в браузере, чтобы сообщить пользователю, что запрошенная веб-страница опасна.

Выберите **Анти-Фишинг**, чтобы активировать антифишинговую защиту. Вы можете дополнительно настроить антифишинг, с помощью следующих параметров:

- **Защита от мошенничества**. Выберите эту опцию если вы хотите расширить защиту от других видов мошенничества, помимо фишинга. Например, от веб-сайтов, представляющих поддельные компании, которые непосредственно не запрашивают конфиденциальную информацию, но вместо этого пытаются представиться в качестве законных предприятий и получить прибыль, обманывая людей в деловых отношениях с ними.

- **Защита от фишинга**. Используйте эту опцию, чтобы защитить пользователей от попыток фишинга.

Если легитимная веб-страница некорректно определяется как фишинговая и блокируется, вы можете добавить ее в белый список, чтобы позволить пользователям доступ к ней. Список должен содержать только веб-сайты, которым вы полностью доверяете.

Для управления исключениями модуля антифишинга:

1. Перейдите в раздел **Общие настройки** и нажмите кнопку **Глобальные исключения**.
2. Введите веб-адрес и нажмите кнопку ⊕ **Добавить**.

   Если вы хотите исключить весь сайт, напишите имя домена, например, `http://www.website.com`, а если вы хотите исключить только веб-страницу, напишите точный веб-адрес этой страницы.

   Примечание
   Символы шаблонов не применяются при указании URL.

3. Чтобы удалить исключение из списка, нажмите соответствующую кнопку ⊗ **Удалить**.
4. Нажмите **Сохранить**.

Сканирование веб-трафика

Сканирование веб-трафика может несколько замедлить работу в Интернет, однако такое сканирование позволяет блокировать вредоносные программы, которые проникают в ваш компьютер из Интернет, включая скрытые загрузки.

Если веб-страница содержит или распространяет вредоносные программы, она автоматически блокируется. При этом будет отображена специальная страница предупреждения, информирующая пользователя о том, что запрашиваемая веб-страница опасна.

Можно отключить сканирование веб-трафика, чтобы увеличить производительность системы (не рекомендуется). Данное действие не будет представлять существенной угрозы до тех пор, пока сканирование при доступе локальных файлов остается включенным.

Сканирование трафика электронных писем

Входящие сообщения электронной почты (POP3) и веб-трафик проверяются в режиме реального времени, чтобы предотвратить проникновение вредоносного ПО в конечную точку. Исходящие письма (SMTP) проверяются для предотвращения заражения вредоносными программами других конечных точек.

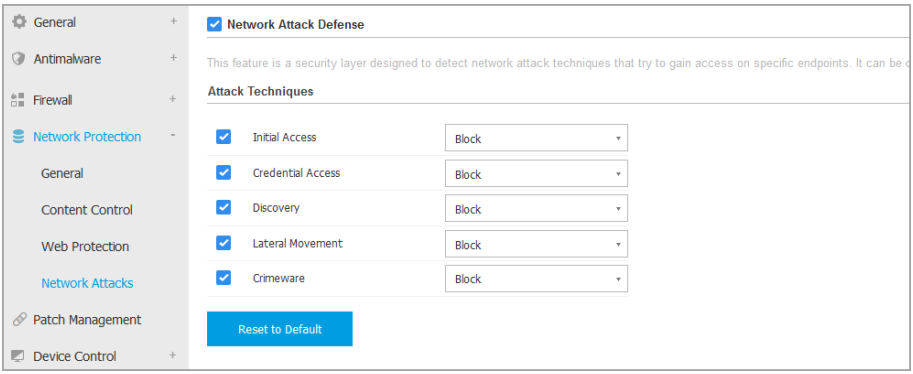
При обнаружении зараженной электронной почты, она автоматически заменяется стандартным письмом, информирующим получателя оригинального зараженного письма.

В целях повышения производительности системы можно отключить сканирование электронной почты. Данное действие не будет представлять существенной угрозы до тех пор, пока сканирование при доступе локальных файлов остается включенным.

Примечание
Параметры **Входящие сообщения** и **Исходящие сообщения** недоступны для macOS.

сетевые атаки

Network Attack Defense предоставляет уровень безопасности, основанный на технологии Bitdefender, которая обнаруживает и предпринимает действия против сетевых атак, предназначенных для получения доступа к конечным точкам, с помощью специальных методов, таких как: атаки методом перебора, сетевые "эксплоиты" и программы для кражи паролей.



Политики - Защита сети - Сетевые атаки

Чтобы настроить Network Attack Defense:

1. Установите флажок **Network Attack Defense** , чтобы включить модуль.
2. Установите соответствующие флажки, чтобы включить защиту от каждой категории сетевых атак. Методы сетевых атак сгруппированы в соответствии с данными MITRE ATT&CK, основанными на следующем:
   - **Начальный доступ** - злоумышленник получает доступ в сеть различными способами, в том числе уязвимости общедоступных веб-серверов. Например: эксплойты для раскрытия информации, эксплойты SQL-инъекций, векторы заражения посредством скрытой загрузки.
   - **Доступ к учетным данным** - злоумышленник крадет такие учетные данные, как имена пользователей и пароли, чтобы получить доступ к системам. Например: атаки методом перебора, эксплойты несанкционированной аутентификации, программы для кражи паролей.
   - **Обнаружение** - после проникновения злоумышленник пытается получить информацию о системах и внутренней сети, прежде чем решить, что делать дальше. Например: эксплойты выхода в файловую систему сервера, эксплойты выхода в файловую систему HTTP.
   - **Боковое движение** - злоумышленник исследует сеть, часто перемещаясь по нескольким системам, чтобы найти основную цель. Злоумышленник может использовать специальные инструменты для достижения цели.

Например: эксплойты с использованием командных инъекций, эксплойты Shellshock, эксплойты с двойным расширением.

- **Мошенническое ПО** - эта категория включает в себя методы, предназначенные для автоматизации киберпреступности. Например, методы мошенничества: ядерные эксплойты, различные вредоносные программы, такие как трояны и боты.

3. Выберите действия, которые вы хотите предпринять против каждой категории методов сетевой атаки, из следующих вариантов:
   a. **Блокировка** - Network Attack Defense останавливает попытку атаки после обнаружения.
   b. **Только отчет**- Network Attack Defense информирует вас о обнаруженной попытке атаки, но не пытается остановить ее.

Вы можете легко восстановить первоначальные настройки, нажав кнопку **Восстановление настроек по умолчанию** в нижней части страницы.

Подробная информация о попытках сетевых атак доступна в отчете о сетевых инцидентах и в уведомлении о сетевых инцидентах.

7.2.6. Управление исправлениями

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов

Модуль управления исправлениями освобождает вас от необходимости обновлять конечные точки с помощью последних обновлений программного обеспечения, автоматически распределяя и устанавливая исправления для широкого спектра продуктов.

Примечание
Вы можете проверить список поддерживаемых поставщиков и продуктов в этой статье базы знаний .

Этот раздел политики содержит параметры для автоматического развертывания исправлений. Сначала вы будете настраивать, как патчи загружаются в конечные точки, а затем какие патчи устанавливать и когда.

Настройка параметров загрузки исправления

В процессе распространения исправлений используются серверы кэширования исправлений для оптимизации сетевого трафика. Конечные точки подключаются к этим серверам и загружают исправления через локальную сеть. Для высокой доступности исправлений рекомендуется использовать более одного сервера.

Чтобы назначить серверы кэширования исправлений целевым конечным точкам:

1. В разделе **Параметры загрузки исправлений** щелкните поле в верхней части таблицы. Появится список обнаруженных серверов кеширования патчей.

   Если список пуст, вам нужно установить роль сервер кеширования исправлений на реле в вашей сети. Для подробной информации обратитесь в Гид по установке.

2. Выберите сервер из списка.
3. Нажмите кнопку ⊕ **Добавить**.
4. Если необходимо, повторите предыдущие шаги чтобы добавить другие серверы.
5. Используйте стрелки вверх и вниз с правой стороны таблицы, чтобы установить приоритет сервера. Приоритет уменьшается сверху вниз по списку.

   Конечная точка запрашивает исправление у назначенных серверов в порядке приоритета. Конечная точка загружает исправление с сервера, где оно находит его первым. Сервер, на котором отсутствует запрошенное исправление, автоматически загрузит его от поставщика, чтобы сделать его доступным для будущих запросов.

Чтобы удалить ненужные серверы, нажмите соответствующую кнопку ⊖Удалить в правой части таблицы.

Выберите параметр **Использовать веб-сайты поставщиков в качестве запасного места для загрузки исправлений** , чтобы убедиться, что ваши конечные точки получают исправления программного обеспечения в случае недоступности серверов кэширования исправлений.

Настройка и установка сканирования исправлений

GravityZone выполняет развертывание исправление в два независимых этапа:

1. Оценка По запросу через консоль управления конечные точки сканируют отсутствующие исправления и сообщают о них.
2. Установка Консоль отправит агентам список исправлений, которые вы хотите установить. Конечная точка загружает исправления с сервера кэширования исправлений, а затем устанавливает их.

Политика предоставляет параметры для автоматизации этих процессов, частично или полностью, чтобы они периодически запускались в соответствии с предпочтительным расписанием.

Чтобы настроить автоматическое сканирование исправлений:

1. Выберите флажок **Автоматическое сканирование исправлений**.
2. Используйте параметры планирования для настройки повторения сканирования. Вы можете настроить сканирование ежедневно или в определенные дни недели, в определенное время.
3. Выберите **Интеллектуальное сканирование при установке нового приложения/программы**, чтобы определить, когда новое приложение было установлено на конечной точке и какие патчи доступны для него.

Чтобы настроить автоматическую установку исправлений:

1. Установите флажок **Установить исправления автоматически после сканирования** .
2. Выберите, какие исправления следует установить: безопасности, иные или все сразу.
3. Используйте параметры планирования для настройки времени запуска задач установки. Вы можете настроить сканирование сразу после завершения сканирования исправлений, ежедневно или в определенные дни недели, в определенное время. Мы рекомендуем устанавливать исправления безопасности сразу после их обнаружения.
4. По умолчанию все продукты имеют право на исправления. Если вы хотите автоматически обновить только набор продуктов, которые вы считаете важными для вашего бизнеса, выполните следующие действия:
   a. Выберите флажок **Особый поставщик и продукт**.

b. Нажмите поле **Поставщик** в верхней части таблицы. Отобразится список всех поддерживаемых поставщиков.

c. Прокрутите список и выберите поставщика для продуктов, которые вы хотите исправить.

d. Нажмите поле **Продукт** в верхней части таблицы. Отобразится список всех продуктов выбранного поставщика.

e. Выберите все продукты, которые вы хотите исправить.

f. Нажмите кнопку ⊕ **Добавить**.

g. Повторите предыдущие шаги для оставшихся поставщиков и продуктов.

Если вы забыли добавить продукт или хотите удалить его, найдите поставщика в таблице, дважды щелкните поле **Продукты** и выберите или отмените выбор продукта в списке.

Чтобы удалить поставщика и все его продукты, найдите его в таблице и нажмите соответственно кнопку ⊖ **Удалить** в правой части таблицы.

5. По различным причинам конечная точка может быть отключена, когда назначена установка исправления. Выберите параметр **Если пропущено, запустите как можно скорее** , чтобы установить исправления сразу после того, как конечная точка вернется в оперативный режим.

6. Некоторые исправления требуют перезагрузки системы после установки. Если вы хотите сделать это вручную, выберите параметр **Отложить перезапуск**.

Важно
Для успешной оценки и установки на конечных точках Windows необходимо убедиться, что выполнены следующие требования:

- **Доверенные корневые центры сертификации** хранит **Сертификат корневого ЦС DigiCert Assured ID**.
- **Промежуточные центры сертификации** включает в себя **центр сертификации подписанного кода DigiCert SHA2**.
- На конечных точках установлены исправления для Windows 7 и Windows Server 2008 R2, упомянутые в этой статье Microsoft: Рекомендации по безопасности Microsoft 3033929

7.2.7. Контроль устройств

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов
- ОС MAK

Модуль управления устройствами позволяет предотвратить утечки данных и проникновение вредоносного ПО через внешние устройства, подключаемые к конечным точкам, применяя с помощью политик правила блокировок и исключений, для широкого спектра типов устройств.

Важно
На macOS Контроль устройств использует расширение ядра или системы. Установка расширения ядра требует подтверждения пользователя на macOS High Sierra (10.13.x). Система уведомляет пользователя о том, что расширение системы от Bitdefender было заблокировано. Пользователь может разрешить это в настройках **Безопасность и конфиденциальность** . Пока пользователь не утвердит расширение системы Bitdefender, этот модуль не будет работать, а пользовательский интерфейс Endpoint Security for Mac покажет критическую проблему, запрашивающую утверждение.
Чтобы исключить вмешательство пользователя, вы можете предварительно утвердить расширение Bitdefender, занеся его в белый список с помощью инструмента управления мобильными устройствами. Подробнее о расширениях Bitdefender см. эту статью базы знаний .

Для использования модуля управления устройствами, необходимо сначала включить его в агент безопасности, устанавливаемый на выбранных конечных точках, затем включить опцию **Контроль устройства** в политике, применяемой к этим конечным точкам. После этого, каждый раз при подключении внешнего устройства к управляемой конечной точке, агент безопасности будет отправлять информацию об этом событии в Control Center, в том числе об имени устройства, классе, ID, дате и времени подключения.

В следующей таблице вы можете найти типы устройств, которые поддерживаются Контролем устройств в системах Windows и macOS:

Тип устройств	Windows	ОС MAK
Bluetooth	Да	Да
CD-ROM Drive	Да	Да (оптический)
Дисковод гибких дисков	Нет	Нет
IEEE 1284.4	Нет	Нет
IEEE 1394 (FireWire)	Нет	Поддерживается в версиях macOS до Big Sur
Образ	Да	Телефоны с подключением PTP, встроенной камерой
Модем	Да	Нет
Ленточный накопитель	Нет	Нет
Портативные Windows-устройства	Нет	Телефоны с MPTсоединением
Порты COM/LPT	Нет	Нет
SCSI Raid	Нет	Нет
Принтеры	Да	Только локально подключенные принтеры
Сетевой адаптер	Да	Да (включая Wi-Fi dongles)
Адаптер беспроводной сети	Да	Да
Внутренние устройства хранения информации	Да	Нет
Внутренние устройства хранения информации	Да	Да (Thunderbolt поддерживался в версиях macOS до Big Sur)

Примечание

- В macOS, если для определенного класса устройств выбрано **Пользователь** разрешение, будут применяться только разрешения, настроенные для подкатегории **Другое**. ,
- Device Control разрешает или запрещает доступ к адаптеру Bluetooth на системном уровне в Windows и macOS в соответствии с политикой. Возможность установки конкретного исключения для каждого сопряженного устройства отсутствует.

Модуль управления устройствами позволяет управлять разрешениями следующим образом:

- Создание правил разрешений
- Создание правил исключений

Правила

Раздел **Правила** позволяет создавать разрешения для устройств, подключаемых к конечным точкам.

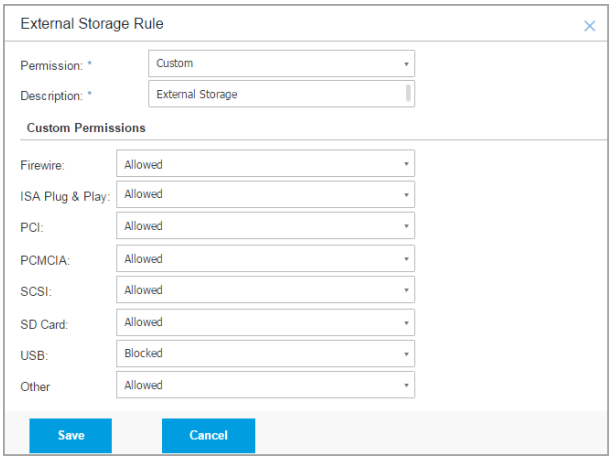
Чтобы задать разрешения определенным типам устройств:

1. Перейдите в **Управление устройством > Правила**.
2. Нажмите на название устройства в представленной таблице.
3. Выберите один тип разрешения из доступных вариантов. Пожалуйста, обратите внимание, что доступно множество разрешений, которые могут варьироваться в зависимости от типа устройства:
   - **Разрешенное**: устройство можно использовать на конечной точке.
   - **Блокированное**: устройство не может быть использовано на конечной точке. В этом случае, каждый раз, когда устройство подключается к конечной точке, агент безопасности покажет уведомление о том, что это устройство заблокировано.

     Важно
     Подключенные устройства, ранее заблокированные, не разблокируются автоматически путем изменения разрешения на **Разрешено** . Пользователь должен перезагрузить систему или повторно подключить устройство, чтобы иметь возможность использовать его.

   - **Только чтение**: может быть использована только функция чтения на данном устройстве.
   - **Пользователь**: позволяет создавать разные разрешения для каждого типа используемого порта, таких как Firewire, ISA Plug & Play, PCI, PCMCIA, USB, т.д. В этом случае, отображается список компонентов, доступных для выбранного устройства, и вы можете установить желаемые разрешения для каждого компонента.

     Например, для внешних накопителей вы можете заблокировать только порты USB и позволить использовать все остальные порты.



Политики - Управление устройствами - Правила

Исключения

После установки правил разрешений для разных типов устройств, вы можете исключить определенные устройства или типы устройств из этих правил.

Вы можете задать исключения для устройств:

- По ID устройства (или аппаратного ID), для обозначения определенных устройств, которые вы хотите исключить.
- По ID модели (или PID), для определения диапазона устройств, произведенных одним производителем.

Чтобы создать правила исключений для устройств:

1. Перейдите в **Управление устройством > Исключения**.
2. Включите опцию **Исключения**.
3. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.
4. Выберите способ, который вы хотите использовать для добавления исключений:
   - **Вручную**. В этом случае, вы должны ввести идентификатор каждого устройства или ID продукта, который вы хотите исключить, если у вас есть под рукой список соответствующих идентификаторов:

a. Выберите тип исключения (по ID модели или по ID устройства).
b. В поле **Исключения**, введите идентификаторы, которые вы хотите исключить.
c. В поле **Описание** введите имя, которое поможет вам определить устройство или набор устройств.
d. Выберите тип разрешения для указанных устройств (**Разрешено** или **Заблокировано**).
e. Нажмите **Сохранить**.

Примечание
Можно вручную настроить исключения подстановочных знаков на основе идентификатора устройства, используя синтаксис `подстановочные знаки: deviceID` . Используйте знак вопроса (?), чтобы заменить один символ, и звездочку (*), чтобы заменить любое количество символов в `идентификаторе устройства` . Например, для `Подстановочные знаки:PCI\VEN_8086*` все устройства, содержащие строку `PCI\VEN_8086` в своих ID будут исключены из правил политики.

- **С обнаруженного устройства**. В этом случае, вы можете выбрать идентификаторы устройств или идентификаторы моделей для исключения из списка всех обнаруженных устройств в вашей сети (в отношении только управляемых конечных точек):
  a. Выберите тип исключения (по ID модели или по ID устройства).
  b. В таблице **Исключения** выберите идентификатор, который вы хотите исключить:
     – Для идентификаторов устройств (Hardware ID), выберите каждое устройство, которое необходимо исключить из списка.
     – Для идентификаторов моделей (PID), выберите одно устройство, чтобы исключить все устройства, имеющие тот же ID модели.
  c. В поле **Описание** введите имя, которое поможет вам определить устройство или набор устройств.
  d. Выберите тип разрешения для указанных устройств (**Разрешено** или **Заблокировано**).
  e. Нажмите **Сохранить**.

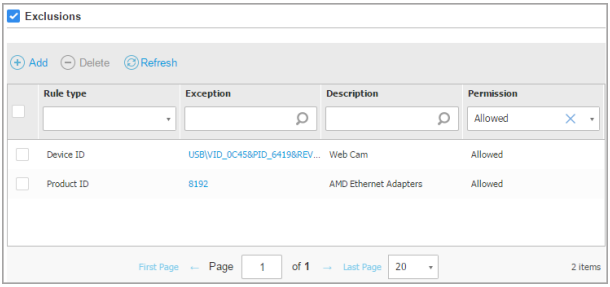
Важно

- Устройства, уже подключеные к конечным точкам, будут обнаружены Bitdefender Endpoint Security Tools только после перезапуска соответствующих конечных точек.
- Подключенные устройства, ранее заблокированные, не разблокируются автоматически путем установки разрешения на **Разрешено** . Пользователь должен перезагрузить систему или повторно подключить устройство, чтобы иметь возможность использовать его.

Все исключенные устройства появятся в таблице **Exclusions**.

Чтобы удалить исключение:

1. Выберите его в таблице.
2. Нажмите кнопку ⊕ **Удалить** в верхней части таблицы.



Политики - Управление устройствами - Исключения

7.2.8. Ретранслятор

Примечание

Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов
- Linux

В этом разделе вы можете задать настройки связи и обновлений для конечных точек с ролью ретранслятора.

Настройки объединены в следующие разделы:

- Коммуникации
- Обновления

Коммуникации

Вкладка **Связь** содержит настройки прокси-сервера для связи между ретрансляторами и компонентами GravityZone.

При необходимости, вы можете самостоятельно настроить связь между выбранными конечными точками-ретрансляторами и облачным сервисом Bitdefender/GravityZone, используя следующие параметры:

- **Сохранить настройки установки**, чтобы использовать параметры прокси-сервера, определенные в установочном пакете.
- **Использовать прокси, определенный в общем разделе**, чтобы использовать параметры прокси-сервера, определенные в текущей политике в разделе **Общее > Настройки**.
- **Не использовать**, когда конечные точки не связываются с конкретными компонентами Bitdefender через прокси-сервер.

Обновления

Этот раздел позволяет настроить параметры обновлений для конечных точек с ролью ретранслятора:

- В разделе **Обновление** вы можете настроить следующие параметры:
  - Интервал времени проверки ретранслятором наличия обновлений.
  - Расположение папки на ретрансляторе, куда обновления продукта и сигнатур будут загружаться и зеркалироваться. Если вы хотите задать конкретную папку загрузки, введите ее полный путь в соответствующем поле.

    Важно
    Рекомендуется задать специальную папку для обновлений продукта и сигнатур. Избегайте выбора папки, содержащей систему или личные файлы.

- Источник обновлений по умолчанию для агентов-ретрансляторов - http://upgrade.bitdefender.com. Вы можете указать другие источники

обновлений, введя IP-адрес или локальное имя хоста одной или нескольких машин-ретрансляторов в сети, а затем настроить их приоритет, используя кнопки вверх и вниз, отображаемые при наведении мыши. Если первый источник обновлений недоступен, будет использован следующий в списке и так далее.

Чтобы задать пользовательское месторасположение обновлений:

1. Включите опцию **Определить пользовательские места обновления**.
2. Введите адрес нового сервера обновлений в поле **Добавить локацию**. Используйте один из следующих вариантов синтаксиса:
   - `update_server_ip:port`
   - `update_server_name:port`

   По умолчанию используется порт 7074.
3. Если конечная точка-ретранслятор общается с локальным сервером обновлений через прокси-сервер, выберите **Использовать прокси**. Настройки прокси-сервера, заданные в разделе **Общее > Настройки**, будут учтены.
4. Нажмите кнопку **Добавить** в верхней части таблицы.
5. Используйте стрелки вверх / вниз в колонке **Действие**, чтобы установить приоритет использования источников обновлений. Если первый источник обновлений недоступен, будет использован следующий в списке и так далее.

Чтобы удалить папку из списка, нажмите соответствующую кнопку **Удалить**. Вы можете удалить источник обновлений по умолчанию (не рекомендуется).

7.2.9. Защита Exchange

Примечание
Этот модуль доступен для Windows для серверов.

Security for Exchange поставляется с очень гибкими настройками, которые позволяют защитить серверы Microsoft Exchange от таких угроз, как вредоносные программы, спам и фишинг. Защита Exchange, установленная на вашем почтовом сервере, позволяет вам также фильтровать сообщения,

содержащие вложения, или если содержание писем считается опасным, в соответствии с политиками безопасности вашей компании.

Чтобы сохранить нормальную производительность сервера, трафик электронной почты обрабатывается фильтрами Security for Exchange в следующем порядке:

1. Фильтрация спама
2. Управление контентом > Фильтрация контента
3. Управление контентом > Фильтрация вложений
4. Фильтрация вредоносных программ

Настройки Security for Exchange организованы в следующих разделах:

- Основные
- Защита от вредоносного ПО
- Антиспам
- Контроль контента

Основные

В этом разделе вы можете создавать и управлять группами учетных записей электронной почты, определять срок хранения объектов в карантине и блокировать определенных отправителей.

Группы пользователей

Control Center позволяет создавать группы пользователей, для которых могут применяться различные политики сканирования и фильтрации. Например, вы можете создать соответствующую политику для ИТ-отдела, отдела продаж или для менеджеров вашей компании.

Чтобы создать пользовательскую группу:

1. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Отобразится окно подробной информации.
2. Введите имя группы, ее описание и адреса электронной почты пользователей.

Примечание

- Для большого количества адресов электронной почты, вы можете скопировать и вставить список из текстового файла.
- Допустимые разделители: пробел, запятая, точка с запятой и ввод.

3. Нажмите **Сохранить**.

Пользовательские группы доступны для редактирования. Нажмите на название группы, чтобы открыть окно настроек, где вы можете изменить данные о группе или отредактировать список пользователей.

Чтобы удалить пользовательскую группу из списка, выберите группу и нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

Настройки

- **Delete quarantined files older than (days).** По умолчанию, файлы в карантине старше 15 дней удаляются автоматически. Для того, чтобы изменить период, введите новое значение в соответствующем поле.
- **Черный список подключений** Если эта опция включена, сервер Exchange отклоняет все письма из черного списка отправителей.

  Чтобы создать черный список:
  1. Нажмите на ссылку **Редактировать элементы в черном списке**.
  2. Введите адрес электронной почты, который вы хотите заблокировать. При редактировании списка вы также можете использовать специальные символы, чтобы задать домен или шаблон для адресов входящей электронной почты:
     - Звездочка (*) заменяет ноль, один или более символов.
     - Вопросительный знак (?) заменяет один любой символ.

     Например, если ввести `*@boohouse.com`, все адреса электронной почты из домена `boohouse.com` будут заблокированы.
  3. Нажмите **Сохранить**.

Проверка IP-адреса домена (Антиспуфинг)

Используйте этот фильтр, чтобы предотвратить подмену спамерами адресов электронной почты отправителей (спуфинг) и принятие электронной почты как доверенной. Вы можете указать IP-адреса, которым вы разрешаете отправку электронной почты в ваши почтовые домены, и, при необходимости, других известных почтовых доменов. Если появится сообщение от одного из перечисленных доменов, но IP-адрес отправителя не совпадет ни с одним из заданных IP-адресов, электронная почта будет отклонена.

Предупреждение
Не используйте этот фильтр, если вы используете смарт-хост, услугу почтовой фильтрации или фильтрующий шлюз электронной почты перед вашим сервером Exchange.

Важно

- Фильтр проверяет только почтовые подключения, не прошедшие проверку подлинности.
- Лучшие практики:
  - Рекомендуется использовать этот фильтр только на серверах Exchange, которые непосредственно используются в Интернет. Например, если у вас есть оба сервера Edge Transport и Hub Transport, настройте этот фильтр только на серверах Edge.
  - Добавьте в ваш список доменов все внутренние IP-адреса, которые могут отправлять почту по SMTP, не проходя проверку подлинности соединения. Это могут быть автоматизированные системы оповещения, сетевое оборудование, такое как принтеры и т.д.
  - На серверах Exchange, использующих Database Availability Groups, также добавьте в список доменов IP-адреса всех серверов с ролью Hub Transport и Mailbox.
  - Будьте осторожны при добавлении в разрешенные IP-адресов внешних почтовых доменов, которые не находятся под вашим управлением. Если вы не будете актуализировать список IP-адресов, сообщения электронной почты из некоторых доменов могут быть отклонены. Если вы используете резервный MX-сервер, вы должны добавить для всех внешних почтовых доменов его IP-адрес, с которого резервный MX-сервер переадресует сообщения электронной почты на ваш основной почтовый сервер.

Чтобы настроить фильтрацию антиспуфинга, выполните действия, описанные ниже:

1. Нажмите на флажок **Domain IP Check (Antispoofing)**, чтобы включить фильтр.
2. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Появится окно конфигурации.
3. Введите домен электронной почты в соответствующем поле.
4. Укажите диапазон доверенных IP-адресов, которые будут использоваться для ранее указанного домена, используя формат CIDR (IP/маска сети).

5. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. IP-адреса будут добавлены в таблицу.
6. Чтобы удалить диапазон IP-адресов из списка, нажмите соответствующую кнопку ⊗ **Удалить** в правой части таблицы.
7. Нажмите **Сохранить**. Домен будет добавлен к фильтру.

Чтобы удалить домен электронной почты из фильтра, выберите его в таблице антиспуфинга и нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

Защита от вредоносного ПО

Модуль защиты от вредоносных программ защищает почтовые сервера Exchange от всех видов вредоносных угроз (вирусов, троянов, шпионских программ, руткитов, рекламного ПО, и т.д.), путем обнаружения зараженных или подозрительных объектов, попытками их лечения или путем изоляции инфицированных объектов, в соответствии с заданными действиями.

Сканирование на предмет вредоносных программ выполняется на двух уровнях:

- Транспортный уровень
- Хранилище Exchange

Сканирование на транспортном уровне

Bitdefender Endpoint Security Tools интегрируется с почтовыми транспортными агентами для сканирования всего почтового трафика.

По умолчанию, сканирование транспортного уровня включено. Bitdefender Endpoint Security Tools фильтрует трафик электронной почты, и, если требуется, информирует пользователей о принятых мерах, добавляя текст в тело сообщения электронной почты.

Используйте флажок **Антивирусная фильтрация**, чтобы отключить или повторно включить эту функцию.

Чтобы настроить текст уведомления, нажмите на ссылку **Настройки**. Доступны следующие опции:

- **Добавить нижний колонтитул в отсканированные письма.** Выберите этот флажок, чтобы добавить сообщение в конце отсканированных писем. Чтобы изменить текст по умолчанию, введите ваше сообщение в текстовом поле ниже.

- **Замена текста.** Для писем, вложения которых были удалены или перемещены в карантин, может быть вложен файл-уведомление. Чтобы изменить текст уведомления по умолчанию, введите ваше сообщение в соответствующее текстовое поле.

Фильтрация вредоносного ПО основана на правилах. Каждое сообщение, доставленное почтовому серверу, проверяется на соответствие правилам фильтрации в порядке их приоритета, пока не будет найдено соответствие правилу. Затем почтовое сообщение обрабатывается в соответствии с действиями, заданными этим правилом.

Управление правилами фильтрации

Вы можете просмотреть все существующие правила в таблице вместе с информацией об их приоритетах, статусах и сферах действия. Правила отсортированы по приоритетности и первое правило обладает наивысшим приоритетом.

Любая antimalware-политика имеет правило по умолчанию, которое становится активным, как только включается фильтрация вредоносного ПО. Что вы должны знать о правиле по умолчанию:

- Это правило нельзя скопировать, удалить или отключить.
- Вы можете изменить только параметры сканирования и действия.
- Приоритет у правила по умолчанию всегда самый низкий.

Создание правил

Существуют два варианта создания правил фильтрации:

- Начните с настроек по умолчанию, выполнив следующие действия:
  1. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы, чтобы открыть окно конфигурации.
  2. Настройте параметры правила. Для получения подробной информации относительно опций, обратитесь к опциям правил.
  3. Нажмите **Сохранить**. Правило будет отображено первым в таблице.
- Используйте клон пользовательского правила в качестве шаблона, выполнив следующие действия:
  1. Выберите из таблицы требуемое правило.
  2. Нажмите кнопку ⧉ **Скопировать** в верхней части таблицы, чтобы открыть окно конфигурации.
  3. Настройте параметры правила в соответствии с вашими потребностями.
  4. Нажмите **Сохранить**. Правило будет отображено первым в таблице.

Редактирование правил

Для редактирования существующего правила:

1. Нажмите на название правила, чтобы открыть окно конфигурации.
2. Задайте новые значения для опций, которые вы хотите изменить.
3. Нажмите **Сохранить**. Изменения вступят в силу после сохранения политики.

Установка приоритетов правил

Чтобы изменить приоритет правил:

1. Выберите правило, которое будет перемещаться.
2. Используйте кнопки **Вверх** или **Вниз** в верхней части таблицы, чтобы увеличить или уменьшить приоритет правила.

Удаление правил

Вы можете удалить одно или несколько пользовательских правил сразу. Все, что вам нужно сделать, это:

1. Отметьте флажками правила, которые будут удалены.
2. Нажмите кнопку **Удалить** в верхней части таблицы. После удаления правило нельзя восстановить.

Опции правил

Доступны следующие опции:

- **Основное.** В этом разделе вы должны задать имя для правила, иначе вы не сможете сохранить его. Выберите флажок **Активен**, если хотите, чтобы правило вступило в силу после сохранения политики.
- **Область действия правила** Вы можете ограничить применение правил только к определенной подгруппе писем, задав следующие параметры:
  - **Применить к (направление).** Выберите направление почтового трафика, к которому будет применяться правило.
  - **Отправители.** Вы можете применять правила для любого отправителя или только для определенных отправителей. Для определенного списка отправителей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Просмотрите выбранные группы в таблице справа.
  - **Получатель** Вы можете применять правила для любого получателя или только для определенных получателей. Для определенного списка получателей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Вы можете просмотреть выбранные группы в таблице справа.

Правило применяется если хотя бы один получатель соответствуют вашему выбору. Если вы хотите применять правило только в том случае, если все получатели находятся в выбранных группах, выберите **Выбрать всех получателей**.

Примечание
Адреса в полях **Cc** и **Bcc** также считаются в качестве получателей.

Важно
Правила, основанные на пользовательских группах, применяются только к серверам с ролями Hub Transport и Mailbox.

- **Параметры** Настройте параметры сканирования для сообщений электронной почты, соответствующих правилу:
  - **Типы отсканированных файлов** Используйте эту опцию, чтобы указать, какие типы файлов вы хотите просканировать. Вы можете сканировать все файлы (независимо от их расширения), только файлы приложений или определенные типы файлов, которые вы считаете опасными. Сканирование всех файлов обеспечивает наилучшую защиту, в то время как сканирование только приложений рекомендуется для быстрого сканирования.

    Примечание
    Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов. Для получения более подробной информации, обратитесь к «Типы файлов приложений» (p. 509).

    Если вы хотите сканировать файлы с определенными расширениями, у вас есть два варианта:
    - **Пользовательские расширения**, где вы должны указать только те расширения, которые будут проверяться.
    - **Все файлы, кроме определенных расширений**, где вы должны ввести только те расширения, которые будут пропущены при сканировании.
  - **Максимальный размер вложения / тела письма (MB).** Установите этот флажок и введите значение в соответствующем поле, чтобы установить максимально допустимый размер прикрепленного файла или тела сообщения электронной почты, которые будут проверяться.
  - **Максимальная глубина архива (уровней).** Установите флажок и выберите максимальную глубину архива из соответствующего поля.

Чем ниже уровень глубины, тем выше производительность и ниже степень защиты.

- **Сканирование на наличие потенциально нежелательных приложений(PUA).** Установите этот флажок, чтобы просканировать возможность проникновения вредоносных или нежелательных приложений, таких как программы показа рекламы, которые могут установиться на системах без согласия пользователя, изменить поведение различных программных продуктов и снизить производительность системы.

- **Действия** Вы можете указать различные автоматические действия агента безопасности для файлов, в зависимости от типа обнаружения.

  Тип обнаружения делит файлы на три категории:

  - **Зараженных файлов.** Bitdefender определяет файлы как зараженные с помощью различных передовых механизмов, которые включают сигнатуры вредоносного ПО, технологии машинного обучения и искусственного интеллекта (ИИ).
  - **Подозрительные файлы.** Эти файлы опредеояются, как подозрительные с помощью эвристического анализа и других технологий Bitdefender. Такой подход обеспечивает высокий уровень обнаружения, но в некоторых случаях пользователь должен знать о случаях ложных сигналов (чистые файлы, определенные как подозрительные).
  - **Не сканируемые файлы** Эти файлы не могут быть просканированы. Это могут быть файлы защищенные паролем, зашифрованные, перепакованные и другие.

  Для каждого типа обнаружения, вы можете выбрать действия по умолчанию или основные и альтернативные действия, если основные не выполняются. Хотя это и не рекомендуется, можно изменить эти действия в соответствующих меню. Выберите действие, которое будет принято:

  - **Дезинфицировать** Удаляет вредоносный код из инфицированных файлов и восстанавливает исходный файл. В случае определенных типов вредоносных программ лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов. Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.
  - **Отклонить / удалить письмо.** На серверах с ролью пограничного транспорта (Edge Transport), обнаруженная электронная почта будет отклонена с ошибкой SMTP 550. Во всех других случаях электронная

почта удаляется без предупреждения. Желательно избегать использование этого действия.
- **Удалить файл** Удаляет проблемные вложения без предупреждения. Желательно избегать использование этого действия.
- **Заменить файл.** удаляет проблемные файлы и вставляет текстовый файл, который уведомляет пользователя о принятых мерах.
- **Переместить файл в карантин.** Перемещает обнаруженные файлы в карантин и вставляет текстовый файл, который уведомляет пользователя о принятых мерах. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает риск заражения. Вы можете управлять файлами в карантине на странице **Карантин**.

> **Примечание**
> Пожалуйста, обратите внимание, что карантин для серверов Exchange требует дополнительное дисковое пространство на разделе, где установлен агент безопасности. Размер карантина зависит от количества хранящихся элементов и их размера.

- **Не предпринимать никаких действий** Никаких действий не будет предпринято в отношении обнаруженных файлов. Эти файлы будут отображаться только в журнале сканирования. По умолчанию, задачи сканирования настроены игнорировать подозрительные файлы. Вы можете изменить действие по умолчанию, чтобы перемещать подозрительные файлы в карантин.
- По умолчанию, когда почта соответствует одному правилу, она обрабатывается исключительно только им, без проверки любых других оставшихся правил. Если вы хотите продолжить проверку другими правилами, снимите флажок **Если условия правила совпадают, прекратить обработку другими правилами**

Исключения

Если вы хотите, чтобы определенный трафик электронной почты был проигнорирован любыми правилами фильтрации, вы можете задать исключения из сканирования. Чтобы создать исключение:

1. Раскройте раздел **Исключения для правил защиты от вредоносных программ**.
2. Нажмите кнопку ⊖ **Добавить** в этом разделе на панели инструментов, которая открывает окно конфигурации.

3. Настройте параметры исключения. Для получения подробной информации относительно опций, обратитесь к опциям правил.
4. Нажмите **Сохранить**.

Сканирование хранилища Exchange

Защита Exchange использует службу Exchange Web Services (EWS) компании Microsoft, чтобы сканировать почтовые ящики Exchange и базы данных общих папок. Вы можете настроить модуль защиты от вредоносного ПО для регулярного запуска задач сканирования по запросу нужных баз данных, в соответствии с заданным графиком.

Примечание

- Сканирование по запросу доступно только для серверов Exchange, на которых установлена роль сервера почтовых ящиков (Mailbox).
- Пожалуйста, обратите внимание, что сканирование по запросу увеличивает потребление ресурсов и, в зависимости от опций сканирования и числа проверяемых объектов, может занимать значительное время.

Сканирование по запросу требует учетной записи администратора сервера Exchange (учетной записи службы), чтобы подменять пользователей Exchange и для получения доступа к целевым объектам, для сканирования почтовых ящиков и общих папок пользователей. Рекомендуется создать отдельную учетную запись для этой цели.

Учетная запись администратора Exchange должна соответствовать следующим требованиям:

- Она является членом группы Organization Management (Exchange 2016, 2013 и 2010)
- Она является членом группы Exchange Organization Administrators (Exchange 2007)
- Она имеет выделенный почтовый ящик.

Включение сканирования по запросу

1. В разделе **Сканировать задачи** нажмите на ссылку **Добавить учетные данные**.
2. Введите имя пользователя и пароль учетной записи службы.
3. Если электронная почта отличается от имени пользователя, необходимо также указать адрес электронной почты учетной записи службы.

4. Введите адрес (URL) Exchange Web Services (EWS) если автообнаружение Exchange не работает.

Примечание

- Имя пользователя должно включать имя домена, например, `user@domain` или `domain\user`.
- Не забудьте обновлять учетные данные в Control Center если они были изменены.

Управление задачами сканирования

В таблице задач сканирования отображаются все запланированные задачи и предоставляется информация об их назначении и периодичности.

Для создания задачи сканирования хранилища Exchange:

1. В разделе **Сканировать задачи**, нажмите кнопку ⊕ **Добавить** в верхней части таблицы, чтобы открыть окно конфигурации.
2. Настройте параметры задачи, как описано в следующем разделе.
3. Нажмите **Сохранить**. Задача будет добавлена в список и она вступит в силу сразу после сохранения политики.

Вы можете отредактировать задачу в любое время, нажав на имя задачи.

Чтобы удалить задачу из списка, выберите его и нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

Параметры задачи сканирования

Задачи имеют ряд параметров, описание которых вы можете найти ниже:

- **Общее** Введите подходящее имя задачи.

  Примечание
  Вы можете просмотреть имя задачи во временной шкале Bitdefender Endpoint Security Tools.

- **Планировщик.** Используйте параметры планирования для настройки расписания сканирования. Вы можете установить время запуска задачи сканирования каждые несколько часов, дней или недель, начиная с указанной даты и времени. Для больших баз данных задача сканирования может занимать много времени и может повлиять на производительность

сервера. В таких случаях вы можете настроить задачу остановки после определенного времени работы.

- **Цель** Выберите контейнеры и объекты, которые будут проверяться. Вы можете выбрать для сканирования: почтовые ящики, общие папки или и то, и другое. Кроме электронной почты, вы можете выбрать для сканирования другие объекты, такие, как **Контакты**, **Задачи**, **Фурнитура** и **Опубликовать элементы**. Кроме того, вы можете установить следующие ограничения на содержимое, которое будет проверяться:
  - Только непрочитанные сообщения
  - Только элементы с вложениями
  - Только новое, полученное в указанный промежуток времени

  Например, вы можете выбрать для сканирования только письма почтовых пользователей, принятые за последние семь дней.

  Выберите флажок **Исключения**, если вы хотите определить исключения при сканировании. Чтобы создать исключение, используйте поля из заголовков таблицы следующим образом:
  1. Выберите тип репозитория из меню.
  2. В зависимости от типа хранилища укажите объекты, которые должны быть исключены:

Тип хранилища	Формат объекта
Почтовый ящик	Адрес электронной почты
Общая папка	Путь к папке, начиная с корня каталога
База данных	Идентификатор базы данных

     Примечание
     Для получения идентификатора базы данных, используйте команду оболочки Exchange:
     ```
     Get-MailboxDatabase | fl name,identity
     ```

     Вы можете ввести только одну команду за один раз. Если у вас есть несколько объектов одного типа, вы должны задать столько правил, сколько элементов.
  3. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы, чтобы сохранить исключение и добавить его в список.

Чтобы удалить правило исключения из списка, нажмите соответствующую кнопку ⊖ **Удалить**.

- **Параметры** Настройте параметры сканирования для сообщений электронной почты, соответствующих правилу:
  - **Типы отсканированных файлов** Используйте эту опцию, чтобы указать, какие типы файлов вы хотите просканировать. Вы можете сканировать все файлы (независимо от их расширения), только файлы приложений или определенные типы файлов, которые вы считаете опасными. Сканирование всех файлов обеспечивает наилучшую защиту, в то время как сканирование только приложений рекомендуется для быстрого сканирования.

    Примечание
    Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов. Для получения более подробной информации, обратитесь к «Типы файлов приложений» (p. 509).

    Если вы хотите сканировать файлы с определенными расширениями, у вас есть два варианта:
    - **Пользовательские расширения**, где вы должны указать только те расширения, которые будут проверяться.
    - **Все файлы, кроме определенных расширений**, где вы должны ввести только те расширения, которые будут пропущены при сканировании.
  - **Максимальный размер вложения / тела письма (MB).** Установите этот флажок и введите значение в соответствующем поле, чтобы установить максимально допустимый размер прикрепленного файла или тела сообщения электронной почты, которые будут проверяться.
  - **Максимальная глубина архива (уровней).** Установите флажок и выберите максимальную глубину архива из соответствующего поля. Чем ниже уровень глубины, тем выше производительность и ниже степень защиты.
  - **Сканирование на наличие потенциально нежелательных приложений(PUA).** Установите этот флажок, чтобы просканировать возможность проникновения вредоносных или нежелательных приложений, таких как программы показа рекламы, которые могут установиться на системах без согласия пользователя, изменить поведение различных программных продуктов и снизить производительность системы.

- **Действия** Вы можете указать различные автоматические действия агента безопасности для файлов, в зависимости от типа обнаружения.

  Тип обнаружения делит файлы на три категории:
  - **Зараженных файлов.** Bitdefender определяет файлы как зараженные с помощью различных передовых механизмов, которые включают сигнатуры вредоносного ПО, технологии машинного обучения и искусственного интеллекта (ИИ).
  - **Подозрительные файлы.** Эти файлы опредеояются, как подозрительные с помощью эвристического анализа и других технологий Bitdefender. Такой подход обеспечивает высокий уровень обнаружения, но в некоторых случаях пользователь должен знать о случаях ложных сигналов (чистые файлы, определенные как подозрительные).
  - **Не сканируемые файлы** Эти файлы не могут быть просканированы. Это могут быть файлы защищенные паролем, зашифрованные, перепакованные и другие.

  Для каждого типа обнаружения, вы можете выбрать действия по умолчанию или основные и альтернативные действия, если основные не выполняются. Хотя это и не рекомендуется, можно изменить эти действия в соответствующих меню. Выберите действие, которое будет принято:
  - **Дезинфицировать** Удаляет вредоносный код из инфицированных файлов и восстанавливает исходный файл. В случае определенных типов вредоносных программ лечение невозможно, поскольку обнаруженный файл является полностью вредоносным. Рекомендуется всегда держать это действие в качестве первого, чтобы быть в курсе зараженния файлов. Лечение подозрительных файлов невозможно, поскольку процедура лечения недоступна.
  - **Отклонить/ удалить электронную почту** Электронная почта удаляется без предупреждения. Желательно избегать использование этого действия.
  - **Удалить файл** Удаляет проблемные вложения без предупреждения. Желательно избегать использование этого действия.
  - **Заменить файл.** удаляет проблемные файлы и вставляет текстовый файл, который уведомляет пользователя о принятых мерах.
  - **Переместить файл в карантин.** Перемещает обнаруженные файлы в карантин и вставляет текстовый файл, который уведомляет пользователя о принятых мерах. Файлы, помещенные в карантин, не могут быть выполнены или открыты; таким образом, не возникает

риск заражения. Вы можете управлять файлами в карантине на странице **Карантин**.

> **Примечание**
> Пожалуйста, обратите внимание, что карантин для серверов Exchange требует дополнительное дисковое пространство на разделе, где установлен агент безопасности. Размер карантина зависит от количества и размера хранящихся писем.

- **Не предпринимать никаких действий** Никаких действий не будет предпринято в отношении обнаруженных файлов. Эти файлы будут отображаться только в журнале сканирования. По умолчанию, задачи сканирования настроены игнорировать подозрительные файлы. Вы можете изменить действие по умолчанию, чтобы перемещать подозрительные файлы в карантин.
- По умолчанию, когда почта соответствует одному правилу, она обрабатывается исключительно только им, без проверки любых других оставшихся правил. Если вы хотите продолжить проверку другими правилами, снимите флажок **Если условия правила совпадают, прекратить обработку другими правилами**

Антиспам

Модуль антиспама предлагает несколько защитных слоев против спама и фишинга, используя комбинации различных фильтров и механизмов, чтобы определить являются ли письма спамом или нет.

> **Примечание**
> - Антиспам-фильтрация доступна для:
>   - Exchange Server 2016/2013 с ролями Edge Transport или Mailbox
>   - Exchange Server 2010/2007 с ролями Edge Transport или Hub Transport
> - Если у вас есть обе роли Edge и Hub в вашей структуре Exchange, рекомендуется включить антиспам-фильтрацию на сервере с ролью Edge Transport.

Фильтрация спама автоматически включена для входящих сообщений электронной почты. Используйте флажок **Антиспамовая фильтрация**, чтобы отключить или повторно включить эту функцию.

Антиспам-фильтры

Электронная почта проверяется на соответствие правилам фильтрации спама на основе групп отправителей и получателей, в порядке приоритета, до совпадения правила. Затем электронная почта обрабатывается в соответствии с параметрами правил и действия применяются над обнаруженным спамом.

Некоторые антиспам-фильтры настраиваются и вы можете контролировать их использование. Список дополнительных фильтров:

- **Charset Filter.** Многие спам-письма написаны на кириллице или иероглифами. Фильтр кодировки определяет подобные сообщения и отмечает их как SPAM.
- **Sexually Explicit Tagged Content.** Спам, который содержит информацию сексуального характера, будет содержать предупреждение SEXUALLY-EXPLICIT: в строке темы. Этот фильтр обнаруживает письма, помеченные как SEXUALLY-EXPLICIT: в строке темы, и помечает их как спам.
- **URL Filter.** Практически все спам-сообщения содержат ссылки на различные ресурсы. Как правило, эти ресурсы содержат еще больше рекламы и предлагают возможность купить вещи. Иногда они также используются для фишинга.

  Bitdefender имеет базу данных подобных ссылок. Фильтр URL-адреса сверяет каждую ссылку в сообщениях электронной почты с этой базой данных. Если обнаружено совпадение, сообщение помечается как спам.
- **Realtime Blackhole List (RBL).** Этот фильтр позволяет проверять почтовый сервер отправителя на сторонних RBL-серверах. Фильтр использует протокол DNSBL и серверы RBL для фильтрации спама на основе репутации почтовых серверов отправителей спама.

  Адрес почтового сервера извлекается из заголовка электронной почты и проверяется его достоверность. Если адрес принадлежит частному классу (`10.0.0.0`, `172.16.0.0` до `172.31.0.0` или `192.168.0.0` до `192.168.255.0`), он игнорируется.

  Проверка DNS выполняется в домене `d.c.b.a.rbl.example.com`, где `d.c.b.a` это обратный IP-адрес сервера и `rbl.example.com` это сервер RBL. Если DNS-сервер отвечает, что домен является действительным, значит IP-адрес указан на сервере RBL и серверу присваивается

определенный рейтинг. Этот рейтинг колеблется между 0 и 100, в зависимости от уровня доверия, который присваивается серверу.

Запрос отправляется для каждого RBL-сервера списком, и рейтинг, возвращаемый каждым из этих серверов, добавляется к промежуточному рейтингу. Когда рейтинг достигает 100, запросы больше не выполняются.

Если оценка RBL-фильтра 100 или выше, электронная почта считается спамом и применяются соответствующие меры. В противном случае, оценка спама вычисляется из результата RBL-фильтра и добавляется к глобальной спам-оценке электронной почты.

- **Heuristic Filter.** Разработанный Bitdefender, эвристический фильтр обнаруживает новые и неизвестные спам-угрозы. Фильтр автоматически обучается на больших объемах спама внутри антиспам-лаборатории Bitdefender. Во время обучения он учится различать спам и легитимные сообщения, распознавать новый спам на основе очень тонкого сходства, используя уже рассмотреную электронную почту. Этот фильтр предназначен для улучшения обнаружения спама на основаннии сигнатур при очень низком количестве ложных срабатываний.
- **BitdefenderОблачный запрос.** Bitdefender поддерживает постоянно развивающуюся базу данных "отпечатков" спам-почты в облаке. Запросы, содержащие характерные признаки, отправляются на облачные серверы и мгновенно проверяются, являются ли эти сообщения спамом. Даже если характерные признаки не найдены в базе данных, они сверяются с другими недавно полученными запросами, и при выполнении определенных условий, электронное сообщение может быть помечено как спам.

Управление правилами антиспама

Вы можете просмотреть все существующие правила в таблице вместе с информацией об их приоритетах, статусах и сферах действия. Правила отсортированы по приоритетности и первое правило обладает наивысшим приоритетом.

Любая антиспам-политика имеет правило по умолчанию, которое становится активным, как только включается антиспам-фильтрация. Что вы должны знать о правиле по умолчанию:

- Это правило нельзя скопировать, удалить или отключить.
- Вы можете изменить только параметры сканирования и действия.
- Приоритет у правила по умолчанию всегда самый низкий.

Создание правил

Чтобы создать правило:

1. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы, чтобы открыть окно конфигурации.
2. Настройте параметры правила. Для получения подробной информации относительно опций, обратитесь к «Опции правил» (р. 275).
3. Нажмите **Сохранить**. Правило будет отображено первым в таблице.

Редактирование правил

Для редактирования существующего правила:

1. Нажмите на название правила, чтобы открыть окно конфигурации.
2. Задайте новые значения для опций, которые вы хотите изменить.
3. Нажмите **Сохранить**. Изменения вступят в силу сразу после сохранения политики.

Установка приоритетов правил

Чтобы изменить приоритет правил, выберите правило, которое вы хотите изменить, и используйте стрелки ▲ **Вверх** и ▼ **Вниз** в верхней части таблицы. Вы можете переместить только одно правило за один раз.

Удаление правил

Если вы не хотите больше использовать правило, выберите правило и нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

Опции правил

Доступны следующие опции:

- **Основное.** В этом разделе вы должны задать имя для правила, иначе вы не сможете сохранить его. Выберите флажок **Активен**, если хотите, чтобы правило вступило в силу после сохранения политики.
- **Область действия правила** Вы можете ограничить применение правил только к определенной подгруппе писем, задав следующие параметры:
  - **Применить к (направление).** Выберите направление почтового трафика, к которому будет применяться правило.
  - **Отправители.** Вы можете применять правила для любого отправителя или только для определенных отправителей. Для определенного списка отправителей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Просмотрите выбранные группы в таблице справа.
  - **Получатель** Вы можете применять правила для любого получателя или только для определенных получателей. Для определенного списка получателей нажмите кнопку **Специальные** и выберите нужные группы

из таблицы слева. Вы можете просмотреть выбранные группы в таблице справа.

Правило применяется если хотя бы один получатель соответствуют вашему выбору. Если вы хотите применять правило только в том случае, если все получатели находятся в выбранных группах, выберите **Выбрать всех получателей**.

Примечание
Адреса в полях **Cc** и **Bcc** также считаются в качестве получателей.

Важно
Правила, основанные на пользовательских группах, применяются только к серверам с ролями Hub Transport и Mailbox.

- **Настройки.** Выберите уровень безопасности, который лучше всего соответствует вашим потребностям (**Интенсивный**, **Нормальный** или **Рекомендуемый**) Используйте описание справа от шкалы, чтобы выбрать необходимый уровень.

  Кроме того, вы можете включить различные фильтры. Для получения более подробной информации об этих фильтрах, обратитесь к «Антиспам-фильтры» (p. 273).

  Важно
  RBL фильтр требует дополнительных настроек. Вы можете настроить фильтр после создания или редактирования правила. Для получения более подробной информации, обратитесь к«Настройка фильтра RBL» (p. 278)

  Для соединений, прошедших проверку подлинности, вы также можете выбрать сканированировать функцией антиспама или нет.
- **Действия.** Есть несколько действий, которые вы можете применить при обнаружении писем. Каждое действие, в свою очередь, имеет несколько возможных вариантов или вторичных действий. Их описание приведено ниже:

  Основные действия:
  - **Доставить электронную почту.** Спам-почта будет достигать почтовых ящиков получателей.
  - **Карантинная электронная почта** Электронная почта будет зашифрована и сохранена в папке карантина на сервере Exchange

и не будет доставлена получателям. Вы можете управлять помещенной в карантин электронной почтой на странице **Карантин**.

- **Перенаправить письмо на.** Почта не будет доставлена оригинальному получателю, но будет доставлена на адрес, указанный в соответствующем поле.
- **Отклонить / удалить письмо.** На серверах с ролью пограничного транспорта (Edge Transport), обнаруженная электронная почта будет отклонена с ошибкой SMTP 550. Во всех других случаях электронная почта удаляется без предупреждения. Желательно избегать использование этого действия.

Вторичные действия:

- **Интеграция с Exchange SCL.** Добавляет заголовок к спаму, позволяя серверу Exchange или Microsoft Outlook осуществлять действия в соответствии с механизмом - Уровень доверия спаму (SCL).
- **Отметьте тему письма как.** Вы можете добавить метку в тему письма, чтобы помочь пользователям фильтровать письма, обнаруженные в почтовом клиенте.
- **Добавить заголовок письма.** Добавляет заголовок к электронной почте, определенной как спам. Вы можете изменить имя заголовка и содержание, введя необходимые значения в соответствующих полях. Кроме того, вы можете использовать этот заголовок электронной почты, чтобы создать дополнительные фильтры.
- **Сохранить письмо на диск.** Копия спама сохраняется в виде файла в указанную папку. Укажите абсолютный путь к папке в соответствующем поле.

  Примечание
  Эта опция поддерживает только электронные письма в формате MIME.

- **Архив к аккаунту** Копия обнаруженной электронной почты доставляется по указанному адресу электронной почты. Это действие добавляет указанный адрес электронной почты в СК (Bcc) список адресов электронной почты.

- По умолчанию, когда почта соответствует одному правилу, она обрабатывается исключительно только им, без проверки любых других оставшихся правил. Если вы хотите продолжить проверку другими

правилами, снимите флажок **Если условия правила совпадают, прекратить обработку другими правилами**

Настройка фильтра RBL

Если вы хотите использовать фильтр RBL, вы должны указать список серверов RBL.

Чтобы настроить фильтр:

1. На странице **Антиспам**, нажмите на ссылку **Настройки**, чтобы открыть окно конфигурации.
2. Укажите в соответствующих полях IP-адрес DNS-сервера для отправки запроса, а также интервал тайм-аута для запроса. Если адрес DNS-сервера не настроен или DNS-сервер недоступен, фильтр RBL использует DNS-серверы системы.
3. Для каждого сервера RBL:
   a. Введите имя сервера или IP-адрес и уровень доверия, назначенный серверу, в полях заголовка таблицы.
   b. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.
4. Нажмите **Сохранить**.

Настройка белого списка отправителей

Вы можете снизить потребление ресурсов сервера, добавив известных отправителей электронной почты в списки надежных или ненадежных отправителей. Таким образом, почтовый сервер всегда будет принимать или отклонять письма, поступающие от этих отправителей. Например, у вас есть интенсивные связи по электронной почте с бизнес-партнером и чтобы быть уверенным, что вы получите все письма от него, вы можете добавить партнера в белый список.

Чтобы построить белый список надежных отправителей:

1. Нажмите ссылку **Белый список**, чтобы открыть окно конфигурации.
2. Выберите флажок **Отправитель Белый список**.
3. Введите адреса электронной почты в соответствующем поле. При редактировании списка вы также можете использовать специальные символы, чтобы задать домен или шаблон для адресов входящей электронной почты:
   - Звездочка (*) заменяет ноль, один или более символов.
   - Вопросительный знак (?) заменяет один любой символ.

Например, если вы введете `*.gov`, все письма, поступающие от домена `.gov`, будут приняты.

4. Нажмите **Сохранить**.

Примечание
Используйте опцию **Черный список подключений** из раздела **безопасность электронной почты > Основное > Настройки**, чтобы добавить известных отправителей спама в черный список.

Контроль контента

Используйте модуль управления контентом для усиления защиты электронной почты, отфильтровав весь почтовый трафик, несовместимый с политикой компании (нежелательный или потенциально опасный).

Для общего контроля содержимого электронной почты, модуль включает в себя два варианта фильтрации электронной почты:

- Фильтрацию контента
- Фильтрацию вложений

Примечание
Фильтрация контента и Фильтрация вложений доступна для:

- Exchange Server 2016/2013 с ролями Edge Transport или Mailbox
- Exchange Server 2010/2007 с ролями Edge Transport или Hub Transport

Управление правилами фильтрации

Фильтры управления контентом основаны на правилах. Вы можете задать различные правила для различных пользователей и групп пользователей. Каждое сообщение, достигающее почтового сервера, сверяется с правилами фильтрации в порядке приоритета, пока не будет найдено соответствие правилу. Затем почтовое сообщение обрабатывается в соответствии с действиями, заданными этим правилом.

Правила фильтрации содержимого предшествует правилам фильтрации вложений.

Правила фильтрации контента и вложений расположены в соответствующих таблицах, упорядоченных по приоритету, и первое правило имеет наивысший приоритет. Для каждого правила отображается следующая информация:

- Приоритет

- Имя
- Направление трафика
- Группы отправителей и получателей

Создание правил

Существуют два варианта создания правил фильтрации:

- Начните с настроек по умолчанию, выполнив следующие действия:
  1. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы, чтобы открыть окно конфигурации.
  2. Настройте параметры правила. Для получения подробной информации об опциях фильтрации конкретного контента и вложения, обратитесь к:
     - Опции правил фильтрации контента
     - Опции правил фильтрации вложений.
  3. Нажмите **Сохранить**. Правило будет отображено первым в таблице.
- Используйте клон пользовательского правила в качестве шаблона, выполнив следующие действия:
  1. Выберите нужное правило из таблицы.
  2. Нажмите кнопку ⧉ **Скопировать** в верхней части таблицы, чтобы открыть окно конфигурации.
  3. Настройте параметры правил в соответствии с вашими потребностями.
  4. Нажмите **Сохранить**. Правило будет отображено первым в таблице.

Редактирование правил

Для редактирования существующего правила:

1. Нажмите на название правила, чтобы открыть окно конфигурации.
2. Задайте новые значения для опций, которые вы хотите изменить.
3. Нажмите **Сохранить**. Изменения вступят в силу после сохранения политики.

Установка приоритетов правил

Чтобы изменить приоритет правил:

1. Выберите правило, которое будет перемещаться.
2. Используйте кнопки ▲ **Вверх** или ▼ **Вниз** в верхней части таблицы, чтобы увеличить или уменьшить приоритет правила.

Удаление правил

Вы можете удалить одно или несколько пользовательских правил одновременно. Все, что вам нужно сделать, это:

1. Выберите правило, которое будет удалено.
2. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы. После удаления правило нельзя восстановить.

Фильтрация контента

Фильтрация контента позволяет фильтровать почтовый трафик на основе символьных строк, которые вы определили ранее. Эти строки сравниваются с темой письма или текстовым содержимым тела электронного письма. Фильтрация контента выполняет следующие задачи:

- Предотвращает поступление нежелательного содержимого электронной почты в почтовые ящики серверов Exchange.
- Блокирует исходящие сообщения электронной почты, содержащие данные конфиденциального характера.
- Архивирует электронную почту, удовлетворяющую заданным условиям, и доставляет ее на другой аккаунт электронной почты или сохраняет на диск. Например, вы можете сохранить письма, отправленные на адрес электронной почты поддержки вашей компании в папку на локальном диске.

Включение фильтрации контента

Если вы хотите использовать фильтрацию контента, выберите флажок **Контентная фильтрация**.

Для создания и управления правилами фильтрации контента, обратитесь к «Управление правилами фильтрации» (p. 279).

Опции правил

- **Основное.** В этом разделе вы должны задать имя для правила, иначе вы не сможете сохранить его. Выберите флажок **Активен**, если хотите, чтобы правило вступило в силу после сохранения политики.
- **Область действия правила** Вы можете ограничить применение правил только к определенной подгруппе писем, задав следующие параметры:
  - **Применить к (направление).** Выберите направление почтового трафика, к которому будет применяться правило.
  - **Отправители.** Вы можете применять правила для любого отправителя или только для определенных отправителей. Для определенного списка отправителей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Просмотрите выбранные группы в таблице справа.

– **Получатель** Вы можете применять правила для любого получателя или только для определенных получателей. Для определенного списка получателей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Вы можете просмотреть выбранные группы в таблице справа.

  Правило применяется если хотя бы один получатель соответствуют вашему выбору. Если вы хотите применять правило только в том случае, если все получатели находятся в выбранных группах, выберите **Выбрать всех получателей**.

  Примечание
  Адреса в полях **Cc** и **Bcc** также считаются в качестве получателей.

  Важно
  Правила, основанные на пользовательских группах, применяются только к серверам с ролями Hub Transport и Mailbox.

- **Настройки.** Настройте выражения для поиска в сообщениях электронной почты, как описано ниже:
  1. Выберите часть электронной почты, которая должна быть проверена:
     – Тема электронной почты, отметив флажок проверки **Фильтровать по теме**. Все письма, которые содержат любое из выражений, введенное в соответствующей таблице, будут отфильтрованы.
     – Тело письма, выбрав флажок **Фильтровать по содержанию тела**. Все письма, которые содержат в теле письма любое из заданных выражений, будут отфильтрованы.
     – И тема, и тело письма, отметив оба флажка. Все письма, тема которых соответствует любому правилу из первой таблицы и тело письма, содержащее любое выражение из второй таблицы, будут отфильтрованы. Например:

       Первая таблица содержит выражения: `Новостная рассылка` и `Еженедельный`. Вторая таблица содержит выражения: `Покупки`, `Цена` и `Предложение`.

       Письмо с темой "Ежемесячное **новостная рассылка** от вашего любимого продавца часов" и телом письма, содержащим фразу "Мы рады представить вам наши новинки **Предложения** содержащие сенсационные часы в неотразимой **Ценой**.", совпадет с правилами и письмо будет отфильтровано. Если тема письма содержит

"Новости от вашего продавца часов", электронное письмо не будет отфильтровано.

2. Создайте списки условий, используя поля в заголовках таблицы. Для каждого условия выполните следующие действия:
   a. Выберите тип выражения, которое будет использовано в поиске. Вы можете ввести точный текст или построить текстовые шаблоны с использованием регулярных выражений.

      Примечание
      Синтаксис регулярных выражений соответствует грамматике ECMAScript.

   b. Введите строку для поиска в поле **Expression**.

      Например:

      i. Выражение `5[1-5]\d{2}([\s\-]?\d{4}){3}` соответствует банковским картам с номерами, которые начинаются с цифр от 51 до 55, состоят из шестнадцати цифр в группах по четыре и группы могут разделяться пробелом или тире. Таким образом, любое письмо, содержащее номер карты в одном из следующих форматов: `5257-4938-3957-3948`, `5257 4938 3957 3948` или `5257493839573948`, будет отфильтровано.

      ii. Это выражение обнаруживает письма со словами `Лотерея`, `Наличные` и `награда`, найденными в этом порядке:

      ```
      (lottery)((.|\n|\r)*)( cash)((.|\n|\r)*)( prize)
      ```

      Чтобы обнаружить электронные письма, содержащие каждое из трех слов независимо от их порядка следования, добавьте три регулярных выражения с разным порядком слов.

      iii. Это выражение обнаруживает электронные письма, которые включают три и более вхождений слова `Награда`:

      ```
      (prize)((.|\n|\r)*)( prize)((.|\n|\r)*)( prize)
      ```

   c. Если вы хотите дифференцировать заглавные и маленькие буквы в письме при сравнении текста, выберите флажок **Учитывать**

регистр. Например, если отметить этот флажок, то `новостная рассылка` и `новостная рассылка` будут разными словами.

d. Если вы не хотите, чтобы выражение было частью других слов, выберите флажок **Целый мир**. Например, с выбранным флажком, выражение `Зарплата Анны` не будет совпадать с `Зарплата Марианы`.

e. Нажмите кнопку ⊕ **Добавить** в заголовке столбца **Действие**, чтобы добавить условие в список.

- **Действия.** Есть несколько действий, которые могут быть предприняты при обнаружении писем. Каждое действие, в свою очередь, имеет несколько возможных вариантов или вторичных действий. Их описание приведено ниже:

  Основные действия:

  - **Добавить электронную почту.** Обнаруженная электронная почта будет доставлена в почтовые ящики получателей.
  - **Карантин.** Электронная почта будет зашифрована, сохранена в папке карантина на сервере Exchange и не будет доставлена получателям. Вы можете управлять помещенной в карантин электронной почтой на странице **Карантин**.
  - **Отклонить.** Почта не будет доставлена оригинальным получателям, но будет доставлена на адрес, указанный в соответствующем поле.
  - **Отклонить / удалить письмо.** На серверах с ролью пограничного транспорта (Edge Transport), обнаруженная электронная почта будет отклонена с ошибкой SMTP 550. Во всех других случаях электронная почта удаляется без предупреждения. Желательно избегать использование этого действия.

  Вторичные действия:

  - **Отметьте тему письма как** Вы можете добавить метку в тему письма, чтобы помочь пользователям отфильтровать обнаруженые письма в почтовом клиенте.
  - **Добавьте заголовок к сообщениям электронной почты.** Вы можете добавить сообщению заголовок и значение обнаруженной почте, набрав желаемые значения в соответствующем поле.
  - **Сохранить почту на диск.** Копия обнаруженной электронной почты сохраняется в виде файла в специальной папке на сервере Exchange. Если папка на сервере не существует, то она будет создана. Укажите абсолютный путь к папке в соответствующем поле.

Примечание
Эта опция поддерживает только электронные письма в формате MIME.

- **Архив к аккаунту** Копия обнаруженной электронной почты доставляется по указанному адресу электронной почты. Это действие добавляет указанный адрес электронной почты в СК (Bcc) список адресов электронной почты.

- По умолчанию, если сообщение соответствует условиям одного правила, его дальнейшая проверка на соответствие другим правилам не производится. Чтобы продолжить обработку другими правилами, снимите флажок **Если условия правила совпадают, прекратите обработку большего количества правил**.

Исключения

Если вы хотите, чтобы почтовый трафик для определенных отправителей или получателей доставлялся с любыми вложениями, вне зависимости от правил фильтрации, вы можете задать исключения в фильтрах.

Чтобы создать исключение:

1. Нажмите ссылку **Исключения** рядом с флажком **Фильтрация контента**. Это действие откроет окно конфигурации.
2. Введите адреса электронной почты доверенных отправителей и/или получателей в соответствующих полях. Любое письмо, приходящее от доверенного отправителя или отправляющееся доверенному получателю, будет исключено из фильтрации. При редактировании списка вы также можете использовать специальные символы, чтобы задать домен или шаблон для адресов входящей электронной почты:
   - Звездочка (*) заменяет ноль, один или более символов.
   - Вопросительный знак (?) заменяет один любой символ.

   Например, если вы введете `*.gov`, все письма, поступающие от домена `.gov`, будут приняты.
3. Для писем с несколькими получателями, можно выбрать флажок **Исключить электронную почту из фильтрации, только если все получатели являются доверенными**, чтобы применять исключение, только если все получатели электронной почты присутствуют в списке доверенных.
4. Нажмите **Сохранить**.

Фильтрация вложений

Модуль фильтрации вложений предоставляет функции фильтрации вложений электронной почты. Он может обнаружить вложения с определенными шаблонами имен или определенного типа. С помощью фильтрации вложений вы можете:

- Блокировать потенциально опасные вложения, такие как `.vbs` или `.exe` файлы или письма содержащие их.
- Блокировать вложения, имеющие оскорбительные выражения или электронные письма содержащие их.

Включение фильтрации вложений

Если вы хотите использовать фильтрацию содержимого, выберите флажок **Фильтрация вложений**.

Для создания и управления правилами фильтрации содержимого, обратитесь к «Управление правилами фильтрации» (p. 279).

Опции правил

- **Основное.** В этом разделе вы должны задать имя для правила, иначе вы не сможете сохранить его. Выберите флажок **Активен**, если хотите, чтобы правило вступило в силу после сохранения политики.
- **Область действия правила** Вы можете ограничить применение правил только к определенной подгруппе писем, задав следующие параметры:
  - **Применить к (направление).** Выберите направление почтового трафика, к которому будет применяться правило.
  - **Отправители.** Вы можете применять правила для любого отправителя или только для определенных отправителей. Для определенного списка отправителей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Просмотрите выбранные группы в таблице справа.
  - **Получатель** Вы можете применять правила для любого получателя или только для определенных получателей. Для определенного списка получателей нажмите кнопку **Специальные** и выберите нужные группы из таблицы слева. Вы можете просмотреть выбранные группы в таблице справа.

    Правило применяется если хотя бы один получатель соответствуют вашему выбору. Если вы хотите применять правило только в том случае, если все получатели находятся в выбранных группах, выберите **Выбрать всех получателей**.

Примечание
Адреса в полях **Cc** и **Bcc** также считаются в качестве получателей.

Важно
Правила, основанные на пользовательских группах, применяются только к серверам с ролями Hub Transport и Mailbox.

- **Настройки.** Перечислите файлы, которые разрешены или запрещены во вложениях электронной почты.

  Вы можете фильтровать вложения электронной почты по типу или по имени файла.

  Чтобы отфильтровать вложения по типу файла, выполните следующие действия:
  1. Выберите флажок **Определить по типу контента**.
  2. Выберите опцию обнаружения, которая больше всего подходит для ваших потребностей:
     - **Only the following categories**, когда у вас есть ограниченный перечень запрещенных типов файлов.
     - **Все, кроме следующих категорий**, когда у вас есть ограниченный перечень разрешенных типов файлов.
  3. Выберите интересующие вас категории типов файлов из списка доступных. Для получения подробной информации о расширениях каждой категории, обратитесь к «Фильтрация вложений по типу файлов» (p. 510).

     Если вам необходимы только некоторые конкретные типы файлов, выберите флажок **Пользовательские расширения** и введите список расширений в соответствующем поле.
  4. Выберите флажок **Включить определение истинного типа**, чтобы проверять заголовки файлов и правильно определять тип файла вложения при сканировании запрещенных расширений. Это означает, что расширение не может быть просто переименовано для обхода политики фильтрации вложений.

     Примечание
     Точное определение типа может быть ресурсоемким.

Чтобы отфильтровать вложения по имени, выберите флажок **Detect by Filename** и введите имена файлов, которые вы хотите отфильтровать, в соответствующем поле. При редактировании списка вы также можете использовать специальные символы, чтобы задать шаблоны:

- Звездочка (*) заменяет ноль, один или более символов.
- Вопросительный знак (?) заменяет один любой символ.

Например, если вы введете `database.*`, все файлы с именем `database`, независимо от их расширения, будут обнаружены.

Примечание
Если вы включите и определение типа содержимого, и имя файла (без точного определения типа), файл должен одновременно удовлетворять обоим условиям одновременно. Например, вы выбрали категорию **Мультимедиа** и ввели имя файла `test.pdf`. В этом случае любое письмо будет пропущено правилом, потому что файл PDF не является мультимедийным файлом.

Выберите флажок **Сканирование внутри архивов**, чтобы предотвратить сокрытие заблокированных файлов в простых архивах, таким образом обходя правило фильтрации.

Рекурсивное сканирование ведется внутри архивов и по умолчанию осуществляется до четвертого уровня глубины архива. Вы можете оптимизировать проверку, как описано ниже:

1. Выберите флажок **Максимальная глубина архива (уровни)**.
2. Выберите другое значение из соответствующего меню. Для лучшей производительности выберите наименьшее значение, для максимальной защиты выберите наибольшее значение.

Примечание
Если вы выбрали опцию **Сканирование внутри архивов**, проверяться будут все архивы.

- **Действия.** Есть несколько действий, которые вы можете предпринять при обнаружении вложений или электронной почты, содержащую их. Каждое действие, в свою очередь, имеет несколько возможных вариантов или вторичных действий. Их описание приведено ниже:

Основные действия:

- **Заменить файл.** Удаляет обнаруженные файлы и вставляет текстовый файл, который уведомляет пользователя о совершенных действиях.

  Чтобы настроить текст уведомлений:
  1. Нажмите **Настройки** рядом с флажком **Attachment filtering**.
  2. Введите текст уведомления в соответствующем поле.
  3. Нажмите **Сохранить**.
- **Удалить файл.** Удаляет обнаруженные файлы без предупреждения. Желательно избегать использование этого действия.
- **Отменить/Удалить электронную почту.** На серверах с ролью пограничного транспорта (Edge Transport) обнаруженная электронная почта будет отклонена с ошибкой SMTP 550. Во всех других случаях электронная почта удаляется без предупреждения. Желательно избегать использование этого действия.
- **Карантинная электронная почта** Электронная почта будет зашифрована и сохранена в папке карантина на сервере Exchange и не будет доставлена получателям. Вы можете управлять помещенной в карантин электронной почтой на странице **Карантин**.
- **Перенаправить письмо на.** Почта не будет доставлена оригинальному получателю, но будет доставлена на адрес указанный в соответствующем поле.
- **Доставить электронную почту.** Позволяет проходить электронной почте.

Вторичные действия:

- **Отметьте тему письма как** Вы можете добавить метку в тему письма, чтобы помочь пользователям отфильтровать обнаруженые письма в почтовом клиенте.
- **Добавьте заголовок электронной почты..** Вы можете добавить сообщению заголовок и значение обнаруженной почте, набрав желаемые значения в соответствующем поле.
- **Сохранить письмо на диск.** Копия обнаруженной электронной почты сохраняется в виде файла в специальной папке на сервере Exchange. Если папка на сервере не существует, то она будет создана. Укажите абсолютный путь к папке в соответствующем поле.

Примечание
Эта опция поддерживает только электронные письма в формате MIME.

- **Архив к аккаунту** Копия обнаруженной электронной почты доставляется по указанному адресу электронной почты. Это действие добавляет указанный адрес электронной почты в СК (Bcc) список адресов электронной почты.

- По умолчанию, когда почта соответствует одному правилу, она обрабатывается исключительно только им, без проверки любых других оставшихся правил. Если вы хотите продолжить проверку другими правилами, снимите флажок **Если условия правила совпадают, прекратить обработку другими правилами**

Исключения

Если вы хотите, чтобы почтовый трафик для определенных отправителей или получателей доставлялся с любыми вложениями, вне зависимости от правил фильтрации, вы можете задать исключения в фильтрах.

Чтобы создать исключение:

1. Нажмите **Исключния** рядом с флажком **Фильтрация вложений**. Это действие откроет окно конфигурации.
2. Введите адреса электронной почты доверенных отправителей и/или получателей в соответствующих полях. Любое письмо, приходящее от доверенного отправителя или отправляющееся доверенному получателю, будет исключено из фильтрации. При редактировании списка вы также можете использовать специальные символы, чтобы задать домен или шаблон для адресов входящей электронной почты:
   - Звездочка (*) заменяет ноль, один или более символов.
   - Вопросительный знак (?) заменяет один любой символ.

   Например, если вы введете `*.gov`, все письма, поступающие от домена `.gov`, будут приняты.
3. Для писем с несколькими получателями, можно выбрать флажок **Исключить электронную почту из фильтрации, только если все получатели являются доверенными**, чтобы применять исключение, только если все получатели электронной почты присутствуют в списке доверенных.
4. Нажмите **Сохранить**.

7.2.10. Шифрование

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов
- ОС MAK

Модуль Encryption управляет полным шифрованием диска на конечных точках, используя BitLocker в Windows и FileVault и утилиту командной строки diskutil в macOS, соответственно.

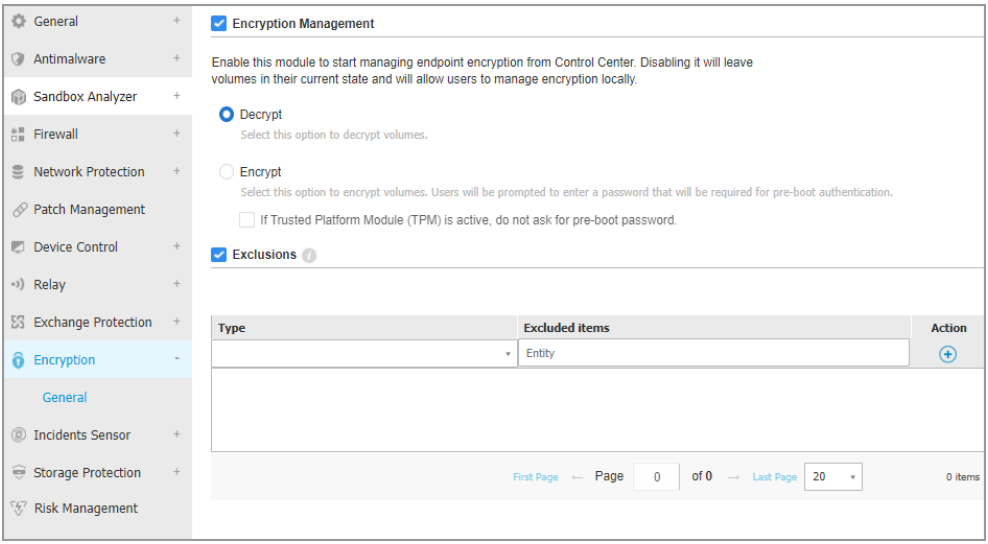
При таком подходе GravityZone может обеспечить некоторые постоянные преимущества:

- Данные защищены в случае утери или кражи устройства.
- Обширная защита для самых популярных компьютерных платформ в мире, благодаря использованию рекомендуемых стандартов шифрования с полной поддержкой Microsoft и Apple.
- Минимальное влияние на производительность конечных точек благодаря встроенным средствам шифрования.

Модуль шифрования использует следующие решения:

- BitLocker версии 1. 2 и позднее на конечных точках Windows с доверенным платформенным модулем (TPM) для загрузочных и незагрузочных томов.
- BitLocker версии 1. 2 и позднее на конечных точках Windows без TPM для загрузочных и незагрузочных томов.
- FileVault на конечных точках macOS, для загрузочных томов.
- diskutil на конечных точках macOS, для незагрузочных томов.

Список операционных систем, поддерживаемых модулем шифрования, см. в Руководстве по установке GravityZone.



Страница шифрования

Чтобы начать управление шифрованием конечной точки из Control Center, установите флажок **Управление шифрованием** . Пока этот параметр включен, пользователи конечных точек не могут управлять шифрованием локально, а все их действия будут отменены. Отключение этого параметра оставит тома конечной точки в их текущем состоянии (зашифрованном или незашифрованном), и пользователи смогут управлять шифрованием на своих компьютерах.

Для управления процессами шифрования и дешифрования доступны три варианта:

- **Расшифровать** - расшифровывает тома и сохраняет их незашифрованными, когда политика активна на конечных точках.
- **Шифровать** - шифрует тома и сохраняет их в зашифрованном виде, когда политика активна на конечных точках.

  В разделе «Шифрование» можно установить флажок **Если доверенный платформенный модуль (TPM) активен, не запрашивать пароль для шифрования** . Этот параметр обеспечивает шифрование на конечных точках Windows с TPM, не требуя пароль шифрования от пользователей. Подробнее см: «Шифрование томов» (p. 293).

- **Исключения**

GravityZone поддерживает метод шифрования Advanced Encryption Standard (AES) с 128 и 256-битными ключами в Windows и macOS. Фактический алгоритм шифрования зависит от конфигурации каждой операционной системы.

Примечание
GravityZone обнаруживает и управляет томами, зашифрованными вручную, с помощью BitLocker, FileVault и diskutil. Для того, чтобы начать управлять этими томами, агент безопасности предложит пользователям конечных точек изменить свои ключи восстановления. В случае использования других решений для шифрования, тома должны быть расшифрованы перед применением политики GravityZone.

Шифрование томов

Чтобы зашифровать тома:

1. Установите флажок **Управление шифрованием** .
2. Выберите опцию **Шифрование** .

Процесс шифрования начинается после того, как политика становится активной на конечных точках, с некоторыми особенностями в Windows и Mac.

Для Windows

По умолчанию агент безопасности предложит пользователям настроить пароль для запуска шифрования. Если на машине установлен функциональный TPM, агент безопасности предложит пользователям настроить персональный идентификационный номер (PIN) для начала шифрования. На экране предварительной загрузки и проверки подлинности пользователи должны вводить пароль или ПИН-код, настроенные на этом этапе, каждый раз, когда запускается конечная точка.

Примечание
Агент безопасности позволяет настраивать требования к сложности ПИН-кода, а также привилегии пользователей на изменение их ПИН-кода с помощью параметров групповой политики BitLocker (GPO).

Чтобы запустить шифрование без ввода пароля от пользователей конечной точки, установите флажок **Если модуль доверенной платформы**

(TPM) активен, не запрашивать пароль перед загрузкой Этот параметр совместим с конечными точками Windows, которые имеют TPM и UEFI.

Когда флажок **Если модуль доверенной платформы (TPM) активен, не запрашивать пароль перед загрузкой** включен:

- На незашифрованной конечной точке:
  - Процесс шифрования без пароля.
  - Экран предварительной загрузки не появляется при запуске машины.
- На конечной точке зашифровано паролем:
  - Пароль удален.
  - Тома остаются зашифрованными
- Зашифрованная или незашифрованная конечная точка с TPM или без TMP не обнаружена или не работает:
  - Пользователю предлагается ввести пароль для шифрования.
  - Экран проверки подлинности перед загрузкой появляется при запуске машины.

Когда флажок **Если модуль доверенной платформы (TPM) активен, не запрашивать пароль перед загрузкой** отключен:

- Пользователь должен ввести пароль для шифрования.
- Тома остаются зашифрованными

На ОС Mac

Для того, чтобы запустить шифрование на загрузочных томах, агент безопасности предложит пользователям ввести свои системные учетные данные. Только пользователи, имеющие локальные учетные записи с правами администратора, могут включить шифрование.

Чтобы запустить шифрование на незагрузочных томах, агент безопасности предложит пользователям настроить пароль шифрования. Этот пароль будет необходим для разблокировки незагружаемого тома при каждом запуске компьютера. Если на компьютере несколько загрузочных томов, пользователи должны настроить пароль шифрования для каждого из них.

Дешифровка томов

Чтобы дешифровать тома на конечных точках:

1. Установите флажок **Управление шифрованием** .
2. Выберите опцию **Дешифровка** .

Процесс расшифровки начинается после того, как политика становится активной на конечных точках, с некоторыми особенностями в Windows и Mac.

Для Windows

Тома расшифровываются без взаимодействия с пользователями.

На ОС Mac

Для загрузочных томов пользователи должны ввести свои системные учетные данные. Для незагрузочных томов пользователи должны ввести пароль, настроенный во время процесса шифрования.

В случае, если пользователи конечной точки забывают свои пароли шифрования, им нужны ключи восстановления для разблокировки компьютеров. Подробнее о получении ключей восстановления см. «Использование Менеджер восстановления (Recovery Manager) для зашифрованных томов» (p. 121).

Исключение разделов

Вы можете создать список исключений из шифрования, добавив определенные буквы дисков, метки и имена разделов и GUID раздела. Вы не можете исключить из шифрования раздел, на котором установлена операционная система.

Чтобы создать правило для исключения разделов из шифрования:

1. Установите флажок **Исключения**.
2. Нажмите **Тип** и выберите тип диска в выпадающем меню.
3. Введите значение диска в поле **Исключенные элементы** и примите во внимание следующие условия:
   - Чтобы ввести **Букву диска**, введите `D:` или вашу букву диска с двоеточием.
   - Для **Метки/имени** вы можете ввести любую метку, например `Работа`.
   - Для раздела **GUID** введите значение следующим образом: `\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\`.
4. Нажмите **Добавить**⊕, чтобы добавить исключение в список.

Чтобы удалить исключение, выберите и добавьте элемент и нажмите **Удалить** ⊗.

7.2.11. Защита хранилища

Примечание
Защита хранилищ доступна для защиты устройств сетевого хранилища (NAS) и систем обмена файлами, совместимых с протоколом адаптации контента Интернета (ICAP).

В данном разделе вы можете настроить Security Server как службу сканирования устройств NAS и систем обмена файлами, совместимых с ICAP, таких как Nutanix Files и Citrix ShareFile.

Security Server сканирует любые файлы, включая архивы, по запросу устройств хранения. В зависимости от настроек Security Server выполняет соответствующие действия с зараженными файлами, например, лечит или запрещает доступ.

Настройки объединены в следующие разделы:

- ICAP
- Исключения

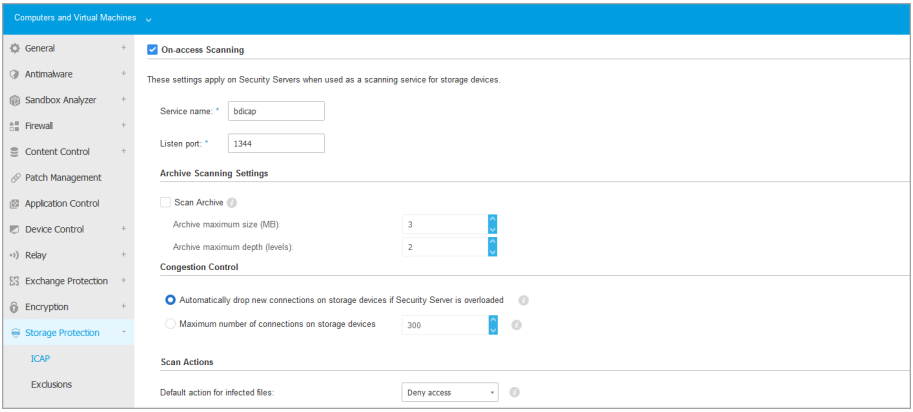
ICAP

Вы можете настроить следующие параметры для Security Server:

- Установите флажок **Сканирование при доступе** , чтобы включить модуль защиты хранилища. Необходимые настройки для связи между Security Server и устройствами хранения предварительно определены следующим образом:
  - Сервисное имя: `bdicap`.
  - Порт прослушивания: `1344`.
- В разделе **Настройки сканирования архива** установите флажок **Сканировать архив** , чтобы включить сканирование архива. Настройте максимальный размер и максимальную глубину сканируемых архивов.

  Примечание
  Если вы установите максимальный размер архива 0 (ноль), Security Server сканирует архивы независимо от их размера.

- В разделе **Контроль перегрузки** выберите предпочтительный способ управления соединениями на устройствах хранения в случае перегрузки Security Server:
  - **Автоматически сбрасывать новые подключения на устройствах хранения, если Security Server перегружен**. Когда один Security Server достиг максимального количества соединений, устройство хранения перенаправит избыток на второй Security Server.
  - **Максимально количество подключений на устройствах хранения**. По умолчанию установлен лимит в 300 подключений.
- В разделе **Действия сканирования** доступны следующие опции:
  - **Запретить доступ** – при обнаружении вредоносного ПО Security Server отправляет событие клиенту ICAP, который запрещает доступ к зараженному файлу.
  - **Disinfect** – при обнаружении вредоносного ПО Security Server отправляет событие клиенту ICAP, который удаляет заражённую часть файла.



Политика - Защита хранилищ - ICAP

Исключения

Если вы хотите удалить определенные объекты из сканирования, установите флажок **Исключения**.

Вы можете определить исключения:

- По хэш - вы определяете исключаемый файл хэшем SHA-256.
- Подстановочным знаком - вы указываете исключенный файл по пути.

Настройка исключений

Чтобы добавить исключение:

1. Выберите тип исключения из меню.
2. В зависимости от типа исключения, укажите объект, который будет исключен, следующим образом:
   - **Хэш** - введите хэши SHA-256 через запятую.
   - **Подстановочный знак** - уточните абсолютный или относительный путь, используя подстановочные знаки. Символ звездочки (*) соответствует любому файлу в директории. Вопросительный знак (?) соответствует только одному символу.
3. Добавить описание для исключения.
4. Нажмите кнопку ⊕ **Добавить**. Новое исключения будут добавлены в список.

Чтобы удалить правило из списка, нажмите соответствующую кнопку ⊗ **Удалить**.

Импорт и экспорт исключений

Если вы намерены повторно использовать исключения в других политиках, вы можете выбрать их экспорт и импорт.

Чтобы экспортировать исключения:

1. Нажмите **Экспорт** в верхней части таблицы исключений.
2. Сохраните файл CSV на вашем компьютере. В зависимости от настроек вашего браузера, файл может автоматически загрузится или вам будет предложено сохранить его в определенное место.

Каждая строка в CSV-файле соответствует одному исключению, имеющему поля в следующем порядке:

```
<exclusion type>, <object to be excluded>, <description>
```

Доступные значения для полей в файле CSV:

Тип исключения:

`1`, для SHA-256 hash

`2`, для подстановочных

Исключаемый объект:

Хеш-значение или путь

Описание

Текст, помогающий определить исключение.

Пример исключений в файле CSV:

```
2,*/file.txt,text
2,*/image.jpg,image
1,e4b0c44298fc1c19afbf4c8996fb9227ae41e4649b934ca991b7852b855,hash
```

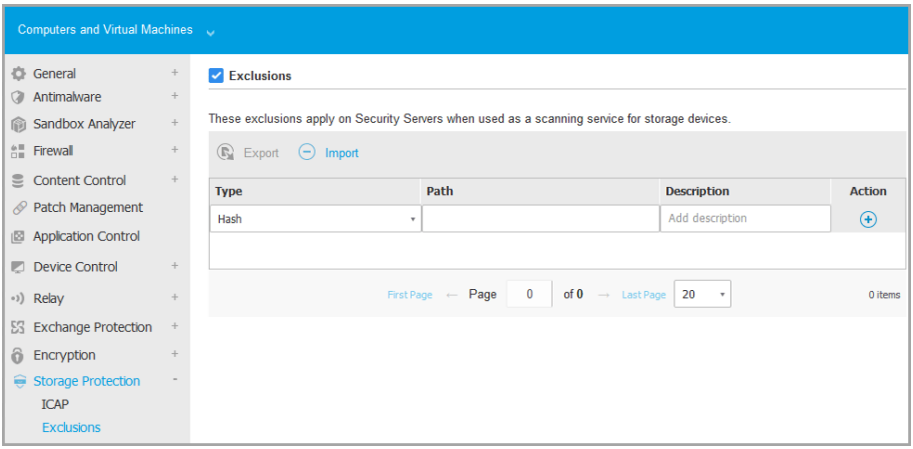
Чтобы импортировать исключения:

1. Нажмите **Импорт**. Откроется окно **Import Policy Exclusions**.
2. Нажмите **Добавить** и затем выберите файл CSV.
3. Нажмите **Сохранить**. Таблица заполняется корректными исключениями. Если файл CSV содержит недопустимые исключения, предупреждение информирует вас о соответствующих номерах строк.

Редактирование исключений

Чтобы редактировать исключение:

1. Кликните имя исключения в колонке **Путь** или в описании.
2. Редактируйте исключения
3. Нажмите `Выход` когда закончите.

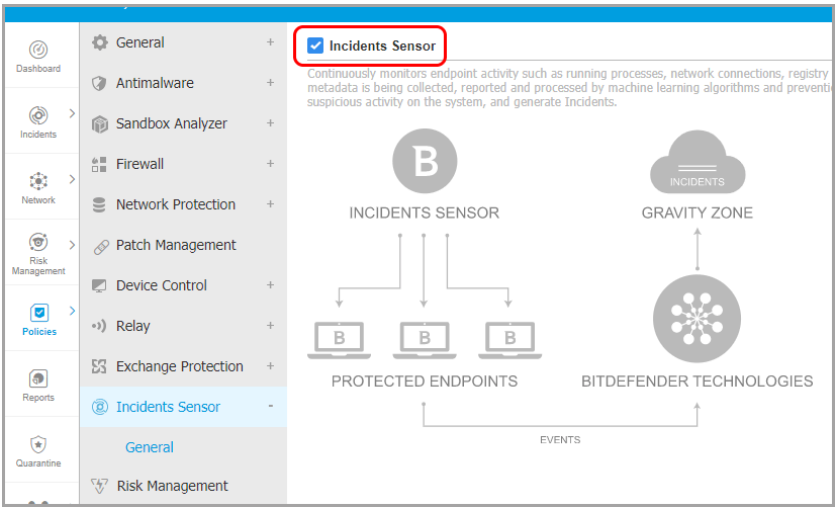


Политика - Защита хранилищ - ICAP

7.2.12. Инциденты Sensor

Постоянный контроль конечных точек, текущих процессов, подключения к сети, изменения реестра. Эти метаданные находятся в процессе сбора, предоставления и обработки при помощи алгоритмов машинного обучения и технологий предотвращения, позволяющих выявить подозрительное поведение.

Проверьте работу датчика инцидентов, чтобы сделать данный модуль доступным.



Инциденты Sensor

7.2.13. Управление рисками

Примечание
Данный модуль доступен для:

- Windows для рабочих станций
- Windows для серверов

Модуль Управление рисками конечной точки помогает выявлять и устранять большое количество сетевых и операционных рисков на уровне конечных точек с помощью задач сканирования рисков, которые можно настроить в политике для периодического выполнения на целевых конечных точках.

Вы можете выбрать нужные индикаторы из большого списка индикаторов рисков для сканирования ваших конечных точек и определить, являются ли они уязвимыми. Для получения дополнительной информации об индикаторах риска GravityZone см. эту статью Базы Знаний.

Чтобы настроить ERA:

- Установите флажок, чтобы включить функции **Управление рисками** и начать настройку политик, определяющих, как запускать задачу **Сканирование рисков**.
- **Планировщик**: определите расписание сканирования рисков для целевых конечных точек:
  1. Укажите дату и время начала запланированного сканирования рисков.
  2. Выберите тип проведения повторного сканирования:
     - Периодически, по указанному количеству часов / дней / недель.
     - По дням недели

     Важно
     Конечные точки должны быть включены по графику. Запланированное сканирование не будет запущено в установленный срок, если аппарат выключен, находится в режиме гибернации или в спящем режиме. В таких ситуациях, проверка будет отложена до следующего раза.
     Проверка по расписанию будет работать на выбранных конечных точках с учетом местного времени. Например, если запланирована задача сканирования, которая должна начаться в 6:00, и конечная точка находится в другом часовом поясе с Control Center, задача сканирования начнется в 6:00 (по времени конечной точки).

  3. При желании вы можете указать, что происходит, когда задача проверки не может быть запущена в запланированное время (конечная точка была отключена или отключена).

     Используйте **Если запланированное время выполнения пропущено, запустить задачу как можно скорее** в соответствии с вашими потребностями:
     - Если вы оставите этот флажок выключенным, задача проверки будет выполняться снова в следующий запланированный момент времени.
     - Когда вы выбираете опцию, вы запускаете сканирование как можно скорее. Чтобы настроить оптимальное время выполнения сканирования и не беспокоить пользователя в рабочее время, выберите **Пропустить, если следующее запланированное сканирование должно начаться менее чем через**, затем укажите интервал, который вы хотите.

Сканирование на наличие рисков запускается при всех показателях, которые активируются по умолчанию.

После успешного завершения операции Вы можете перейти на вкладкуНеправильная настройка страницы **Рисков безопасности**, проанализировав их, и выбрать показатели, которые следует проигнорировать.

Оценка всех рисков компании будет пересмотрена в связи с оставленными без внимания индикаторами риска.

Примечание
Чтобы просмотреть полный список индикаторов рисков и их описание, см. эту статью Базы Знаний.

8. ИНФОРМАЦИОННАЯ ПАНЕЛЬ МОНИТОРИНГА

Правильный анализ сетевой безопасности требует наличия доступа к данным и их корреляции. Наличие централизованной информации о безопасности позволяет контролировать и обеспечивать соблюдение политик безопасности организации, быстро выявлять проблемы, анализировать угрозы и уязвимости.

GravityZone раздел изучения состоит из:

- **Панель управления**
- **Управляющее резюме**

8.1. Панель управления

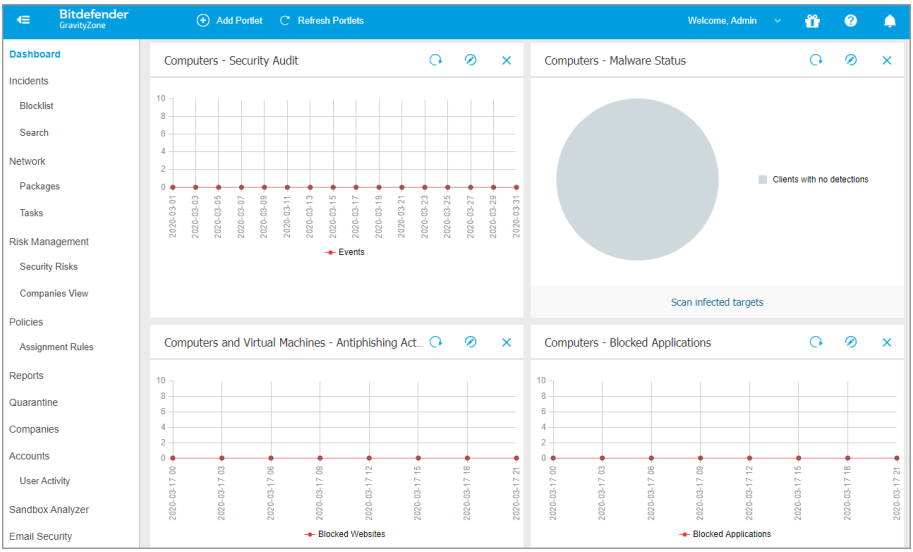
Панель Control Center - настраиваемый визуальный дисплей, обеспечивающий быстрый обзор всех конечных точек и статуса сети.

Она состоит из двух разделов:

- Панель состояния сети приборной панели
- Портлеты панели инструментов

Строка состояния сети панели инструментов информирует вас о количестве открытых или незавершенных инцидентов, находящихся под угрозой активов (конечных точек) и обнаруженных угроз в вашей сети. Используйте эту информацию для того, чтобы просматривать неразрешенные элементы сети. Нажмите **Просмотр** чтобы просмотреть страницу **Инциденты**. Для получения более подробной информации, обратитесь к «Расследование происшествий» (p. 320).

Портлеты информационной панели отображают различную информацию о состоянии безопасности в реальном времени, используя простые графики, которые позволяют вам быстро выявить все проблемы, которые могут потребовать вашего вмешательства.



Информационная панель

Вот что вам нужно знать о портлетах информационной панели:

- Control Center поставляется с несколькими предопределенными портлетами информационной панели.
- Каждый портлет информационной панели включает в себя подробный отчет, создаваемый в фоновом режиме и доступный одним щелчком на графике.
- Есть несколько типов портлетов, которые содержат различную информацию о состоянии защиты конечных точек, такие как состояние обновлений, активность вредоносного ПО, активность файрвола.

> **Примечание**
> По умолчанию, портлеты получают данные за текущий день и, в отличие от отчетов, не могут быть установлены на более длительные промежутки времени, более чем один месяц.

- Информация, отображаемая с помощью портлетов, относится к конечным точкам только под вашей учетной записью. Вы можете настроить объекты каждого портлета и параметры с помощью команды **Изменить портлет**.

- Нажмите на нужной записи легенды диаграммы, в случае доступности, чтобы скрыть или отобразить соответствующие данные на графике.
- Портлеты отображаются в группах по четыре. Используйте вертикальную полосу прокрутки или клавиши со стрелками вверх и вниз для перемещения между группами портлетов.
- Для ряда типов отчетов, у вас есть возможность одновременно запускать нужные задачи на требуемых конечных устройствах, без необходимости переходить к разделу **Network**, чтобы запустить задачу (например, сканировать зараженные конечные точки или обновить конечные точки). Используйте кнопку выполнения доступных действий в нижней части портлета.

Информационную панель очень просто настроить с учетом индивидуальных предпочтений. Вы можете изменить настройки портлета, добавить дополнительные портлеты, удалить или отсортировать существующие портлеты.

8.1.1. Обновление данных портлета

Чтобы убедиться, что портлет отображает последнюю информацию, нажмите на кнопку **Обновить** в его заголовке.

Чтобы обновить информацию обо всех портлетах одновременно, нажмите кнопку **Обновить портлеты** в верхней части панели инструментов.

8.1.2. Редактирование настроек портлета

Некоторые портлеты содержат информацию о текущем статусе, в то время как другие содержат отчеты о событиях безопасности за последний период. Вы можете проверить и настроить периодичность отчетов портлета нажав значок в его заголовке.

8.1.3. Добавление нового портлета

Вы можете добавить другие портлеты для получения необходимой информации.

Чтобы добавить новый портлет:

1. Перейдите на страницу **Панель инструментов**.
2. Нажмите кнопку **Добавить портлет** в верхней части кансоли. Появится окно конфигурации.

3. В разделе **Подробная информация**, настройте детали портлета:
   - Тип фонового отчета
   - Подходящее имя портлета
   - Интервал времени для событий, которые будут отображаться

   Для получения более подробной информации о доступных типах отчетов, обратитесь к «Типы отчетов» (p. 434).
4. В разделе **Цели** выберите сетевые объекты и группы для включения.
5. Нажмите **Сохранить**.

8.1.4. Удаление портлета

Вы можете легко удалить любой портлет, нажав значок ⊗ **Удалить** в его заголовке. После того как вы удалите портлет, вы не сможете его восстановить. Тем не менее, вы сможете создать другой портлет с теми же настройками.

8.1.5. Расположение портлетов

Вы можете расположить портлеты информационной панели по вашему усмотрению. Чтобы изменить расположение портлетов:

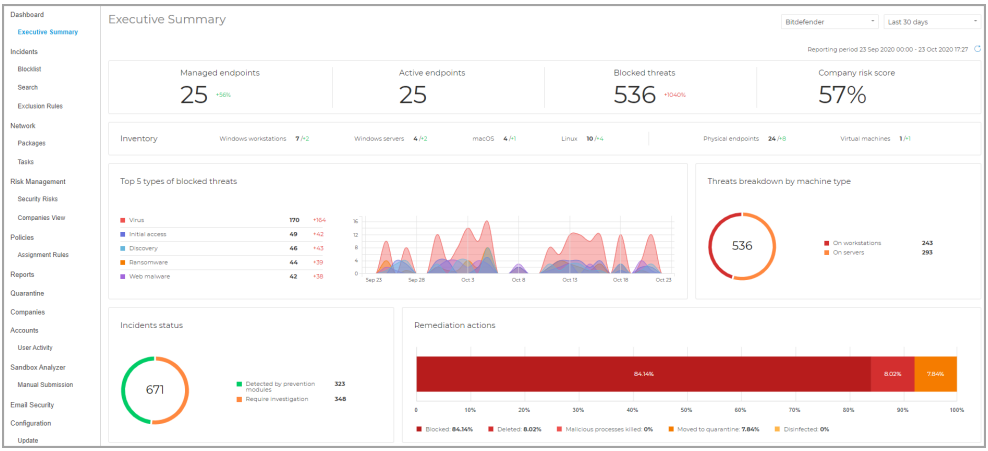
1. Перейдите на страницу **Панель инструментов**.
2. Перетащите любой портлет в нужную позицию. Все остальные портлеты распределятся между новой и старой позицией, сохраняя свой порядок.

> **Примечание**
> Вы можете перемещать портлеты только в имеющиеся позиции.

8.2. Управляющее резюме

Executive Summary представляет собой краткий обзор безопасности всех защищенных конечных точек в Вашей сети и специально разработан, чтобы помочь Вам контролировать, анализировать и предоставлять исполнительному руководству простые в интерпретации данные.

Состоит в основном из виджетов, повышает видимость, предлагая подробную информацию о конечных модулях, обнаружениях и принятых действиях, типах угроз и методах, оценке риска Вашей компании и других.



Управляющее резюме

Важно

- Вся предоставленная статистика основана на данных, собранных после включения этой функции. Первые события не включены в процесс.

Начальные разделы, расположенные в верхней части страницы, следующие::

Управляемые конечные точки

В этом разделе представлены все компьютеры в Вашей сети, на которых установлен агент безопасности.

Активные конечные точки

Этот раздел информирует Вас обо всех конечных точках, которые были подключены к сети в выбранном периоде или находятся в сети на момент составления отчета.

Заблокированные угрозы

В этом разделе представлено общее число заблокированных угроз на Ваших конечных точках.

Инвентаризация

В этом разделе приведены подробные сведения о типах конечных точек и их операционных системах.

Общая оценка риска

В этом разделе Вы можете найти информацию об уровне риска Вашей компании.

В правом верхнем углу страницы можно ввести название компании или выбрать из выпадающего меню интересующую компанию. Пожалуйста, имейте в виду, что в сводке приводятся статистические данные по одной компании за раз, а не по всем.

Вы также можете выбрать заранее определенный период относительно текущего времени.

- **Последние 24 часа**
- **Последние 7 дней**
- **Последние 30 дней**

Примечание

- Все представленные данные напрямую коррелируют с выбранным периодом и компанией.
- Чтобы убедиться, что консоль отображает самую свежую информацию, используйте кнопку **Обновить** в правом верхнем углу страницы.

В зависимости от выбранного интервала Вы можете наблюдать разницу (дельту), показанную в процентах в некоторых разделах.

Дельта значения указывают на различия в Вашей сети, которые произошли между двумя конкретными периодами:

- Период, предшествующий выбранному интервалу, с тем же количеством дней или часов.
- Выбранный Вами интервал.

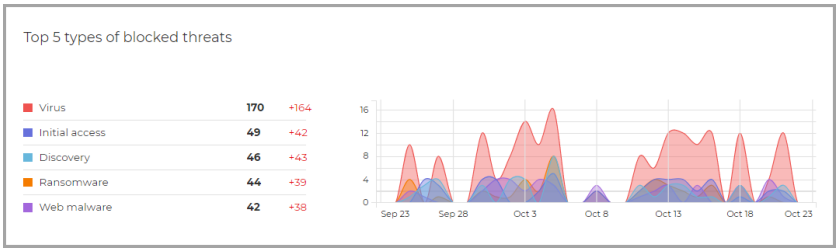
Например, на рисунке ниже общее количество заблокированных угроз в Вашей сети уменьшилось на **6%** за **последние 30 дней** . Этот процент был получен после сравнения значений за 30 дней до выбранного интервала со значениями за последние 30 дней.

Резюме - Delta

Основными виджетами сводки являются:

5 основных типов заблокированных угроз

Виджет предоставляет информацию о наиболее частых типах угроз в зависимости от количества обнаружений на Ваших конечных точках. В столбце слева отображаются типы угроз, а в коррелированном правом столбце можно найти количество обнаружений для каждого типа, а также Дельта-значения.



Резюме - для 5 типов заблокированных угроз

Разбивка угроз по типу конечных точек

В этом виджете представлены типы конечных точек, рабочих станций и серверов, а также количество обнаружений на каждом из них.

Статус инцидентов

Этот виджет детализирует инциденты безопасности по всей сети компании.

Категории данного инцидента описываются как следующие:

- **Обнаружены модулями предотвращения**: события безопасности, идентифицированные как угрозы модулями предотвращения GravityZone.
- **Требуемое изучение**: отображает все подозрительные инциденты, по которым еще не было предпринято никаких действий, и требуется изучение.

Восстановительные действия

В этом разделе описываются действия, которые были предприняты в отношении заблокированных элементов на основе применяемых параметров политики.

Состояние модулей конечной точки

Содержит обзор охвата модулей защиты для Ваших конечных точек. На диаграмме представлены модули и их состояние на текущий период, а также отношение к конечным точкам.

Общая оценка риска

Этот виджет отображает уровень риска, которому подвергается Ваша организация из-за некорректно настроенных параметров системы и известных уязвимостей установленных в настоящее время приложений, а также из-за рисков, вызванных поведением или активностью пользователей.

Обнаружения политики на основе правил

В этом разделе подробно описывается количество обнаружений и их типы на основе правил, настроенных администратором в политике.

Данные типы обнаружения включают в себя:

- **Заблокированные устройства**: количество обнаружений основано на**Контроль устройств** правилах.
- **Заблокированные соединения**: число обнаружений основано на**Firewall** правилах.
- **Заблокированные приложения**: число обнаружений основано на**черный список** правилах.
- **Заблокированные веб-сайты**: количество обнаружений основано на**Контроль веб-сайтов** правилах.

Заблокированные сайты

Этот виджет представляет количество обнаружений, организованных по типам угроз и идентифицированных на Ваших конечных точках с помощью **Сетевой защиты**.

Заблокированные методы сетевых атак

В этом разделе представлена информация о заблокированных методах атаки, обнаруженных в Вашей сети.

8.2.1. Изучение Многомерных Данных

Краткое изложение теперь дает Вам возможность исследовать многомерные данные, переходя от статистического уровня к более детальному и подробному представлению. Новая возможность детализации помогает мгновенно переходить от виджетов к определенным разделам Центра управления.

Для навигации по каждому виджету:

1. Перейдите на страницу **Панель мониторинга** и выберите **Краткое описание**.
2. Найдите интересующий Вас виджет.
3. Нажмите на заголовок или содержимое виджета в зависимости от Вашего выбора. Например, если Вы хотите просматривать только угрозы, обнаруженные на рабочих станциях, напрямую, щелкните **На рабочих станциях** вместо заголовка виджета.

   После выбора вы автоматически перенаправляетесь в соответствующую область Центра управления. В каждом разделе будет отображаться сложная информация в индивидуальной форме, чтобы вы могли легко идентифицировать и анализировать интересующие вас аспекты.

Чтобы перейти в раздел **Угрозы Xplorer**, где вы можете подробно просмотреть обнаруженные угрозы в вашей сети, используйте следующие виджеты:

- **Заблокированные угрозы**
- **5 основных типов заблокированных угроз**
- **Разбивка угроз по типу конечных точек**
- **Восстановительные действия**
- **Обнаружения политики на основе правил**
- **Заблокированные сайты**

- **Заблокированные методы сетевых атак**

Чтобы перейти в область **Сеть**, где Вы можете просмотреть список конечных точек, соответствующие операционные системы и версии, типы конечных точек и др., используйте следующие виджеты:

- **Управляемые конечные точки**
- **Активные конечные точки**
- **Инвентаризация**

Виджет **Оценка рисков компании** перенаправляет Вас в раздел **Управление рисками**, где Вы можете найти информацию об уровне риска, которому подвергается Ваша организация из-за некорректных системных настроек, известных уязвимостей, установленных в настоящее время приложений и потенциальных рисков, вызванных поведением пользователей.

Виджет **Статус инцидентов** перенаправляет Вам в раздел **Инциденты**, в котором содержатся подробные сведения обо всех событиях безопасности, обнаруженных датчиком **Инцидентов**.

Виджет **Состояние модулей конечных точек** автоматически создает отчет **Состояние модулей конечных точек** при доступе. В отчете содержится подробная информация о покрытии модулей защиты для Ваших конечных точек.

Важно

- Разделы, на которые Вы перенаправлены, автоматически фильтруются в соответствии с выбранным Вами виджетом.

Например, когда Вы нажимаете виджет **Заблокированные угрозы** и перенаправляетесь на страницу **Угрозы Xplorer**, в следующих столбцах будут предварительно выбранные и активные фильтры:

- **Тип конечной точки**

  Активные фильтры: **Рабочая станция** и **Сервер**

- **Модуль обнаружения**

  Активные фильтры: **Защита от вредоносных программ**, **Защита сети**, **Защита хранилища**, **Защита от обмена**

- **Выполненное действие**

Активные фильтры (только действия по исправлению): **Заблокировано**, **Удалено**, **Помещено на карантин**, **Вылечено**, **Вредоносный процесс уничтожен**, **Заменено вложение**, **Отклонено/удалено электронное письмо**, **Удалено вложение**, **Отклонено вложение электронной почты**

- **Технологии обнаружения**

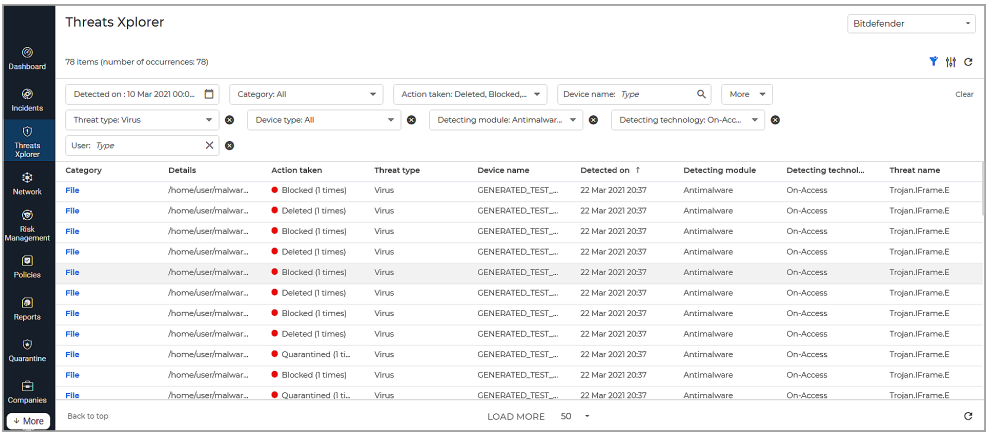
  Активные фильтры: несколько технологий GravityZone, соответствующих выбранным модулям

- Интервал отчетности и компания автоматически соотносятся с вашим выбором из раздела **Краткое описание**

9. XPLORER УГРОЗ

Угрозы Xplorer специально разработан, чтобы обеспечить Вам повышенную видимость обнаруженных угроз в Впшей сети. Эта функция централизует события обнаружения от нескольких технологий GravityZone и классифицирует их по категории, типу угрозы, действиям по исправлению и многим другим.

Вы можете легко идентифицировать и проанализировать любое событие вашей компании за определенный промежуток времени, используя доступные фильтры.



Xplorer угроз

На странице **Программа для устранения угроз** Вы можете просмотреть полный список событий обнаружения в вашей сети. В таблице отображаются записи в обратном хронологическом порядке, таким образом, самые последние события всегда находятся в начале.

Важно

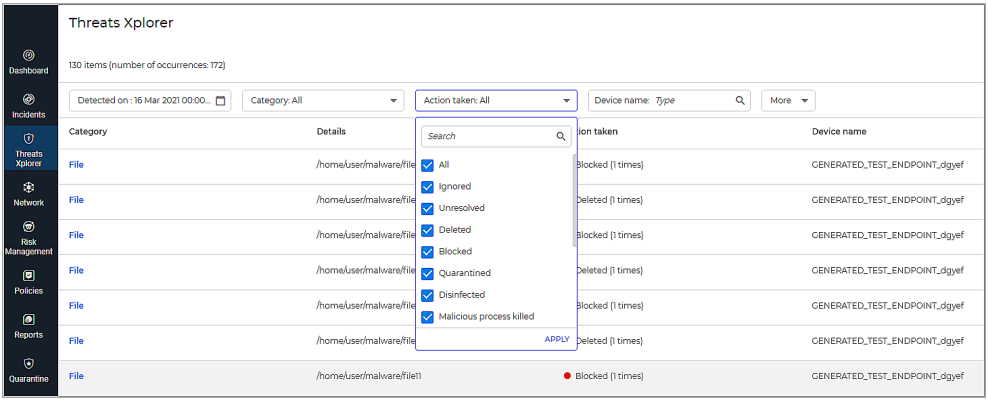
- Все представленные данные напрямую коррелируют с выбранным периодом и компанией.
- В таблице отображаются события обнаружения за последние 90 дней.

Функция централизует события обнаружения из следующих модулей:

- Защита от вредоносного ПО
- Защита сети
- Защита хранилища
- Защита Exchange
- Контроль устройств
- Брандмауэр

9.1. Анализ событий обнаружения

Угрозы Xplorer предоставляет широкий выбор столбцов и фильтров, которые помогут вам перемещаться по списку событий. Вы можете либо выбрать фильтры из раскрывающегося меню столбца, либо ввести ключевые слова, соответствующие Вашим желаемым результатам.



Threats Xplorer - Колонки

Вы можете выбрать интересующую компанию в правом верхнем углу страницы, а также просматривать события с определенным интервалом.

Чтобы задать интервал времени или настроить его, используйте **обнаруженный на** в левой части фильтров и выберите один из следующих параметров:

- **Последние 24 часа**
- **Последние 7 дней**

- **Последние 30 дней**
- **Пользовательский**

Доступные колонки:

Категория
В этом столбце идентифицированные угрозы классифицируются по общим категориям, таким как файлы, электронные письма, веб-сайты, процессы и другие.

Подробная информация
В этом столбце содержится конкретная информация об обнаруженной угрозе, такая как путь к файлу или процессу, веб-адрес веб-сайта, тема электронной почты и многое другое.

Выполненное действие
В этом разделе представлены действия, предпринятые в связи с угрозой, а также количество случаев. Например, с помощью доступных фильтров Вы можете просматривать заблокированные, удаленные, помещенные в карантин, сообщенные элементы и другие.

Имя конечного пользователя
В этой колонке Вы можете найти название устройства, на котором произошло обнаружение. Вы можете выполнить поиск по определенному устройству, введя его имя в строке поиска фильтра.

Обнаружено на
В этой колонке Вы можете узнать все о времени и дате обнаружения.

Командная строка
В этом разделе Вы можете найти подробную информацию о командной строке, используемой в обнаруженной угрозе, если таковая имеется.

Тип угрозы
В этой колонке представлен тип выявленной угрозы. Вы можете найти конкретные события, используя соответствующий фильтр. Для получения дополнительной информации о доступных типах угроз обратитесь к разделу Глоссарий.

IP-адрес
В этом разделе Вы можете найти IP-адрес устройства, где было обнаружение.

Тип конечной точки
В этом столбце содержится информация о типе устройства, будь то сервер или рабочая станция.

Пользователь
В этой колонке Вы можете найти имя пользователя, которое упоминалось при атаке.

Модуль обнаружения
В этом разделе Вы найдете имя модуля GravityZone, который идентифицировал угрозу. Для получения более точных результатов поиска используйте доступные фильтры.

Технологии обнаружения
В этом разделе представлена информация о технологии GravityZone, используемой для выявления угрозы.

Имя угрозы
В этой колонке представлено точное название выявленной угрозы.

Безфайловая атака
В этом столбце приведены подробные сведения о существовании атаки без файлов.

Примечание
Количество элементов, расположенное над областью столбцов в левой части страницы, отображает общее количество событий обнаружения в соответствии с выбранными фильтрами. Кроме того, Вы можете найти количество вхождений, которое указывает, сколько раз было обнаружено событие.

Вы можете использовать параметры, доступные в верхней правой части страницы, чтобы:

- Удалите раздел фильтры, расположенный над столбцами
- Обновите сетку и отобразите последние события.
- Очистите выбранные и применённые фильтры.
- Выберите или отмените выбор основных столбцов, которые Вы хотите просмотреть, в соответствии с Вашими потребностями.
- Сделайте сетку компактной.

Для улучшенного анализа безопасности и общего доступа Вы можете получить доступ к странице **Threats Xplorer** также из Резюме.

10. РАССЛЕДОВАНИЕ ПРОИСШЕСТВИЙ

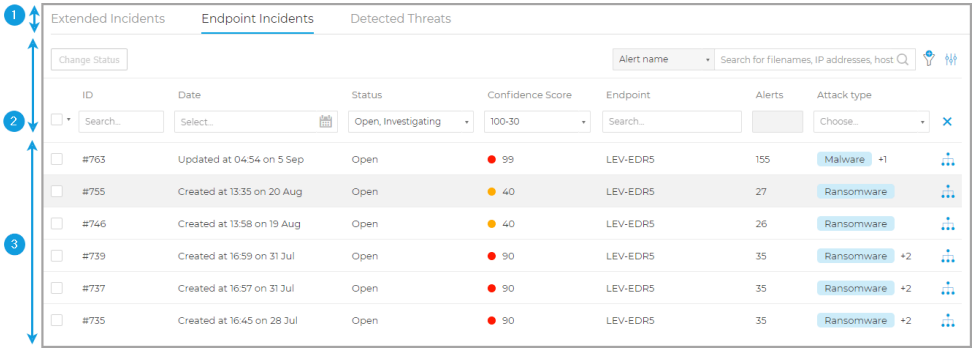
Раздел **Инциденты** позволяет фильтровать, расследовать и предпринимать действия по всем событиям безопасности, которые были обнаружены датчиком инцидентов за определенный промежуток времени.

Раздел **Incidents** содержит следующие страницы:

- **Инциденты** : позволяет просматривать и расследовать события безопасности.
- **Черный список**: управляет заблокированными файлами, участвующими в событиях безопасности.
- **Поиск** : предоставляет параметры для запроса базы данных событий безопасности.
- **Пользовательские правила**: позволяет определять пользовательские правила для обнаружения или исключения определенных событий.

10.1. Страница инцидентов

Используйте страницу **Инциденты** для фильтрации и управления событиями безопасности.



Обзор страницы инцидентов

Примечание
Доступность данных вкладок варьируется в зависимости от лицензии, которую включает в себя текущий план.

Эта страница содержит следующие области:

1. Панель окон с вкладками, включающими различные типы инцидентов:
   - **Инциденты конечных точек**: отображает все подозрительные инциденты, обнаруженные на конечных точках, которые требуют изучения и по которым еще не было предпринято никаких действий.
   - **Обнаруженные угрозы**: отображает все события безопасности, идентифицированные как угрозы модулями предотвращения GravityZone. Эти инциденты обнаруживают на конечных точках и обрабатывают с помощью действий, предусмотренных в политиках безопасности, применяемых к Вашей среде.
2. Параметры фильтрации для настройки Вашей сетки:
   - Нажмите кнопку **Показать/скрыть столбцы**, чтобы добавить или убрать столбцы фильтра.

     Страница обновится автоматически, загрузив карточки событий безопасности с информацией, соответствующей добавленным столбцам.
   - Нажмите кнопку **Показать/скрыть фильтры**, чтобы отобразить или скрыть панель фильтров.
   - Нажмите кнопку **Очистить фильтры**, чтобы сбросить все фильтры.
3. Сетка инцидентов отображает список событий безопасности, соответствующих выбранным фильтрам.

Примечание
Эта функция больше не обеспечивает поддержку Internet Explorer.

Панель обзора

Панель **Обзор** содержит список открытых инцидентов, главных предупреждений, затронутых устройств и другие соответствующие данные, чтобы дать Вам быстрое представление об общей ситуации, связанной с угрозами в Вашей среде.

Панель обзора

Примечание
Доступность и содержание панели **Обзор** могут отличаться в зависимости от лицензии, включенной в Ваш текущий план.

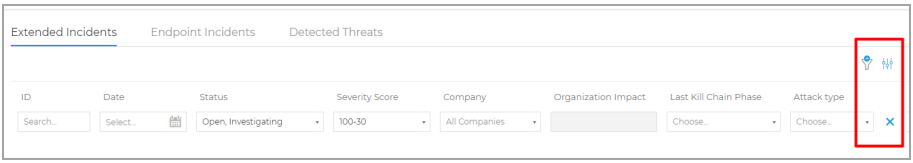
Фильтрация инцидентов из панели Обзор

Вы также можете отфильтровать список инцидентов, выбрав значения на панели

- Если щелкнуть значение в разделе **ОТКРЫТЫЕ ИНЦИДЕНТЫ**, оно отобразит только инциденты с выбранным уровнем серьезности.
- Если щелкнуть значение в разделе **ТОП ОПОВЕЩЕНИЙ**, оно заполнит поле поиска именем оповещения и отобразит только те случаи, когда оповещение было обнаружено.
- Если щелкнуть значение в разделе **ТОП МЕТОДОВ**, оно заполнит поле поиска названием метода и отобразит только те случаи, когда метод был обнаружен.
- Если нажать на значение в разделе **ТОП ЗАТРОНУТЫХ УСТРОЙСТВ**, оно отобразит только инциденты, влияющие на выбранное устройство.

10.1.1. Сетка фильтров

Страница **Инциденты** позволяет выбрать, какие инциденты отображать, настроив сетку фильтров.



Сетка фильтров

- Нажмите кнопку **Показать/скрыть столбцы**, чтобы добавить или убрать столбцы фильтра.

  Страница обновится автоматически, загрузив карточки событий безопасности с информацией, соответствующей добавленным столбцам.

- Нажмите кнопку **Показать/скрыть фильтры**, чтобы отобразить или скрыть панель фильтров.

- Нажмите кнопку **Очистить фильтры**, чтобы сбросить все фильтры.

Подробные сведения о доступных параметрах фильтрации приведены в следующей таблице:

Параметры фильтрации	Подробная информация
Оценка доверия	Показатель достоверности - это число от 100 до 10, указывающее, насколько потенциально опасно событие безопасности. Чем выше число, тем больше уверенности в том, что событие опасно. Он предоставляет контекст, основанный на индикаторах атаки и методах ATT&CK, если это применимо. Для фильтрации по доверительной шкале перетащите ползунок к выбранным значениям. Или вы можете использовать числовые поля под ползунком. Нажмите **OK**, чтобы подтвердить выбор оценки.
Дата	Чтобы фильтровать по дате: 1. Нажмите иконку календаря или поле **Дата**, чтобы открыть страницу конфигурации даты. 2. Выберите временной промежуток, когда произошел инцидент:

Параметры фильтрации	Подробная информация
	• Перейдите на вкладки **с** и **до**, чтобы выбрать даты, определяющие временной интервал. **Примечание** Вы можете указать точное время для начала и завершения, используя поля часов и минут под календарем. • Вы также можете выбрать заранее определенный период относительно текущего времени (последние 7 дней). Для получения дополнительного места для хранения событий Вам необходимо обратиться к своему торговому представителю, чтобы обновить свое решение с помощью 30 -, 90- или 180-дневного **хранения данных**). 3. Нажмите **ОК** , чтобы применить фильтр.
Состояние	Отфильтруйте инциденты по их текущему состоянию, проверив один или несколько параметров статуса, доступных в выпадающем меню **Статус**: • **Открыть**: для неисследованных событий безопасности • **Расследуемые** : для расследуемых событий безопасности • **Ложное срабатывание**: для событий безопасности, помеченных как ложная тревога • **Закрытые**: для событий безопасности с закрытым расследованием
Идентификатор	Сузьте список инцидентов, выполнив поиск определенного идентификационного номера события безопасности.
Конечная точка	Сузьте список инцидентов, выполнив поиск определенного имени конечной точки в управляемой сети.
Тип атаки	Тип атаки - это динамический список наиболее распространенных типов атак, который изменяется в

Параметры фильтрации	Подробная информация
	зависимости от показателей атаки, обнаруженных в перечисленных событиях безопасности.
Выполненное действие	Действие только для блокировки или сообщения, применяемое GravityZone в отношении конкретных инцидентов, определенных в политике.
Оповещения	В столбце **Оповещения** отображается количество оповещений, вызванных за инцидент.
ОС конечной точки	Эта опция фильтрует события безопасности по операционной системе задействованных конечных точек.

Примечание
Параметры фильтрации могут варьироваться в зависимости от типа лицензионного ключа, включенного в Ваш текущий план.

Чтобы найти дополнительные элементы, которые не отображаются в сетке фильтра, выберите один из параметров поиска в выпадающем меню **Поиск**:

- **Имя оповещения** - от 3 до 1000 символов.
- **ATT&CK Technique** - максимум 100 символов.
- **IP-адрес конечной точки** - не более 45 символов.
- **MD5** - максимум 32 символа.
- **SHA256** - максимум 64 символа.
- **Имя узла** - не более 360 символов.
- **Имя пользователя** - не более 1000 символов.

Страница обновится автоматически, загружая только карточки событий безопасности, соответствующие искомому элементу. Для более детального поиска вы можете создавать поисковые запросы на Странице поиска .

10.1.2. Просмотр списка событий безопасности

На странице **Инциденты** отображается список событий безопасности, соответствующих выбранным фильтрам.

По умолчанию на странице 20 событий, сгруппированных по дате. Страница автоматически обновляется через регулярные промежутки времени, когда EDR запускает новые события.

Важно
Все события безопасности старше 90 дней автоматически удаляются из разделов **Расследование** и **Обзор**, а также из репозитория событий безопасности.

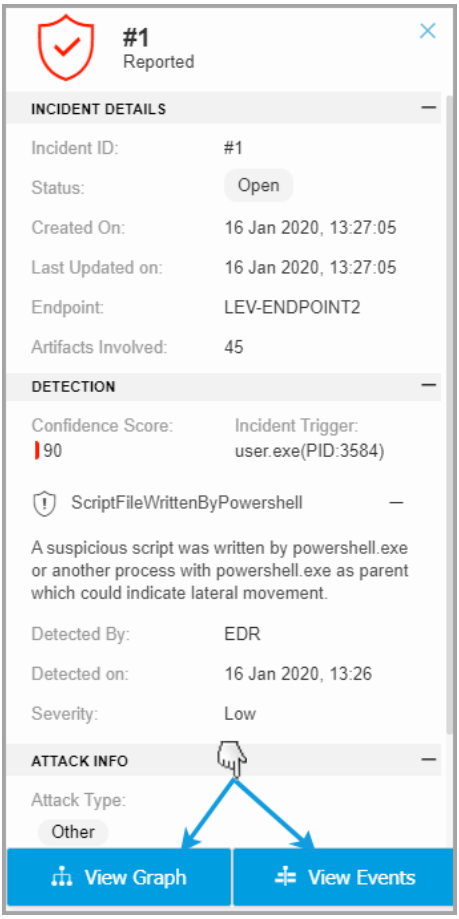
Для навигации по странице используйте стрелки, колесо прокрутки или нажмите на панель прокрутки. Измените количество отображаемых событий внизу страницы. Вы можете просматривать до 100 событий на странице.

Каждая запись события безопасности отображается в расширенном формате карты, предоставляя обзор каждого инцидента с информацией, основанной на выбранных фильтрах.

Примечание
Обратите внимание на цвет слева для того чтобы быстрее оценить достоверность события (низкий, средний или высокий).

Карта событий безопасности

- Если вы нажмете соответствующую кнопку **Посмотреть график** карты событий безопасности, она откроет ее на новой странице, где вы сможете детально проанализировать инцидент и предпринять соответствующие действия.
- Если щелкнуть карточку события безопасности, откроется боковая панель быстрого просмотра с информацией о выбранном инциденте.



Быстрый просмотр информации об инциденте

- Нажмите кнопку **Просмотреть график**, чтобы получить доступ к графической визуализации инцидента.
- Нажмите кнопку **Посмотреть события**, чтобы получить доступ к временной шкале инцидента.

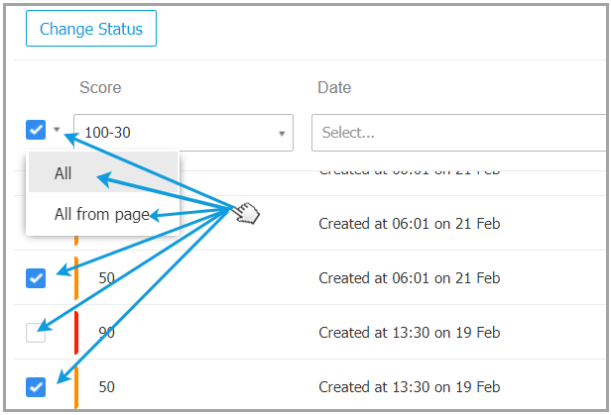
- Если вы установите флажок для любой карты событий безопасности, она активирует кнопку **Изменить статус**, позволяя вам изменить текущий статус инцидента.

Изменение статуса событий безопасности

Статус расследования помогает вам отслеживать инциденты, которые уже были расследованы и помечены как закрытые или ложно сработавшие, инциденты, которые в настоящее время расследуются, а также открытые или новые инциденты, которые еще предстоит проанализировать.

Вы можете изменить состояние одного или нескольких событий безопасности одновременно:

1. Установите флажки на карточках событий безопасности, у которых будет изменен статус.

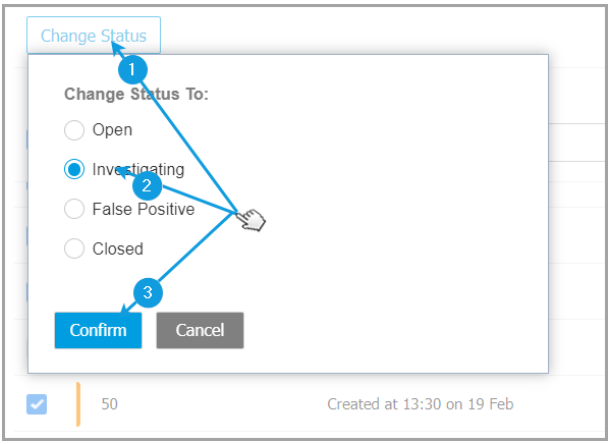


Выбор карт событий безопасности

Вы можете выбрать их по отдельности или с помощью опций массового выбора в выпадающем меню.

Примечание
Вы также можете просматривать несколько страниц событий безопасности, при сохранении своего выбора.

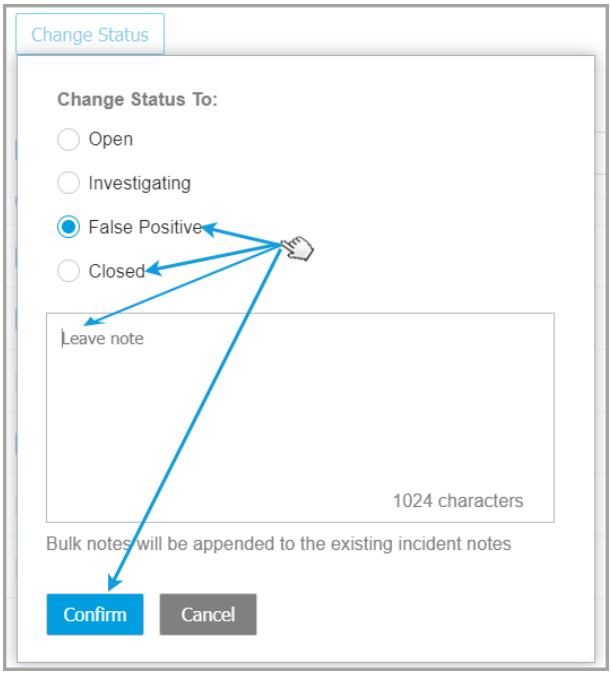
2. Нажмите кнопку **Изменить статус** и выберите нужные параметры:



Изменение статуса события безопасности

- **Open** - когда событие безопасности еще не расследуется.
- **Расследовать** - когда вы начали расследование события.
- **Ложное срабатывание** - когда вы проанализировали событие и определили его как ложноположительное.
- **Закрыть**- когда вы закончили расследование события.

Примечание
При изменении состояния событий на **Ложное срабатывание** или **Закрытое** открывается окно, в котором можно оставить примечание о причинах изменения статуса события, для последующей консультации.



Оставить записку для закрытых событий и событий ложного срабатывания.

Примечание
Примечание будет добавлено к уже существующим внутри отфильтрованных инцидентов.

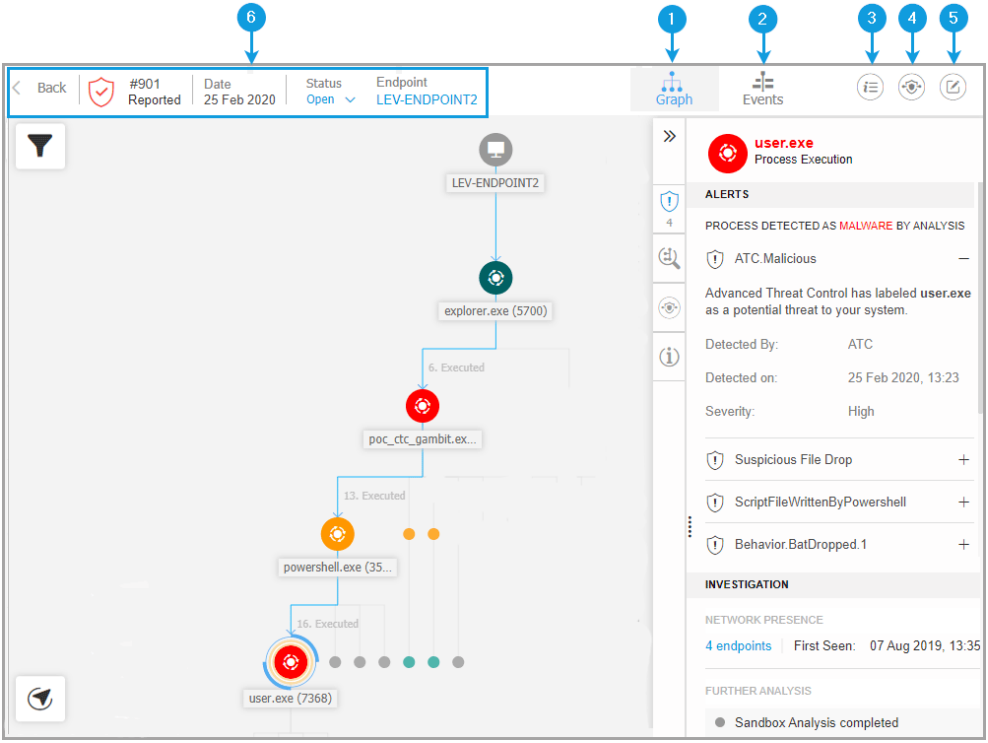
3. Нажмите **Confirm**, чтобы применить выбранную опцию статуса.

10.1.3. Исследование расширенного инцидента

На странице **Инциденты** выберите событие безопасности, которое вы хотите проанализировать, и нажмите **Просмотреть график**, чтобы отобразить его на новой странице.

Каждый инцидент безопасности имеет отдельную страницу, содержащую подробную информацию о последовательности событий (отображаемых на графике в виде связанных узлов событий безопасности), которые

спровоцировали инцидент и предоставляет варианты действий по исправлению.



1. Вкладка «График»

   График отображает инцидент безопасности и составляющие его элементы, выделяя критический путь инцидента и отображая сведения об узле, который спровоцировал инцидент, на панели **Node Details**.

2. Вкладка «События»

   На вкладке «События» отображаются фильтруемые обнаруженные системные события и оповещения, а также соответствующие описания событий.

3. Панель информации об инциденте

   Эта панель содержит сворачиваемую область с такими деталями, как идентификатор инцидента, текущее состояние, временная отметка, когда он был создан и последний раз обновлялся, количество задействованных артефактов, имя триггера и информация об атаке.

4. Панель исправления

   Эта панель содержит сворачиваемую область с действиями, автоматически предпринимаемыми GravityZone, и рекомендуемыми действиями, которые можно выполнить, чтобы смягчить инцидент.

5. Заметки буфера обмена

   При нажатии кнопки **Notes** открывается буфер обмена, в который можно добавлять заметки о текущем инциденте, которые вы можете прочитать при повторном посещении инцидента позднее.

6. Строка состояния инцидента

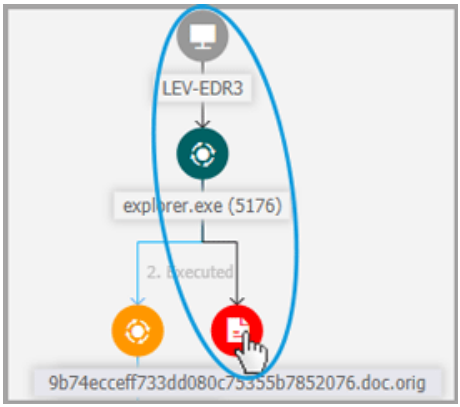
   Строка состояния содержит подробную информацию об идентификаторе инцидента, времени и дате его создания, статусе, триггере инцидента и конечной точке, на которую он влияет. Нажав кнопку **Back**, вы вернетесь на главную страницу **Incidents**.

Узлы событий безопасности

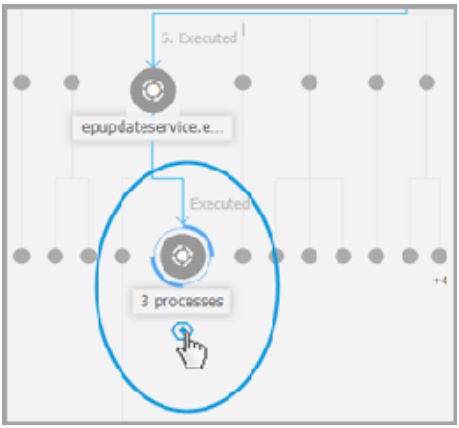
Вот что вам нужно знать об узлах событий безопасности:

- Каждый узел представляет определенный элемент, участвующий в расследуемом инциденте.

- Все узлы, составляющие критический путь, по умолчанию подробно отображаются при открытии инцидента, в то время как другие элементы постепенно исчезают, чтобы избежать загромождения.
  - Если навести курсор на узел, который не является частью критического пути, он будет выделен и покажет путь к исходной точке, не нарушая Critical Path.



- Три или более одинаковых узла событий типа действия, порождаемых родительским узлом, группируются в расширяемый узел кластера.



  - Только узлы без дочерних элементов будут скрыты от графика инцидентов, когда кластерный узел свернут.
  - Узлы, в которых была обнаружена подозрительная активность, не будут добавлены к узлу кластера.
- При нажатии на узел отобразятся следующие данные:
  - Он выделит синим цветом путь к узлу конечной точки вместе со всеми другими задействованными элементами.
  - Боковая панель с расширяемыми секциями, которые предоставляют подробную информацию о выбранном узле, предупреждениях в случае обнаружения сбоев, доступных действиях и рекомендациях. Обратитесь к «Сведения об узле» (p. 346) для получения дополнительной информации.
- Узлы связаны стрелками, указывающими ход действий, которые произошли в конечной точке во время инцидента. Каждая строка помечена именем действия и его хронологическим номером.

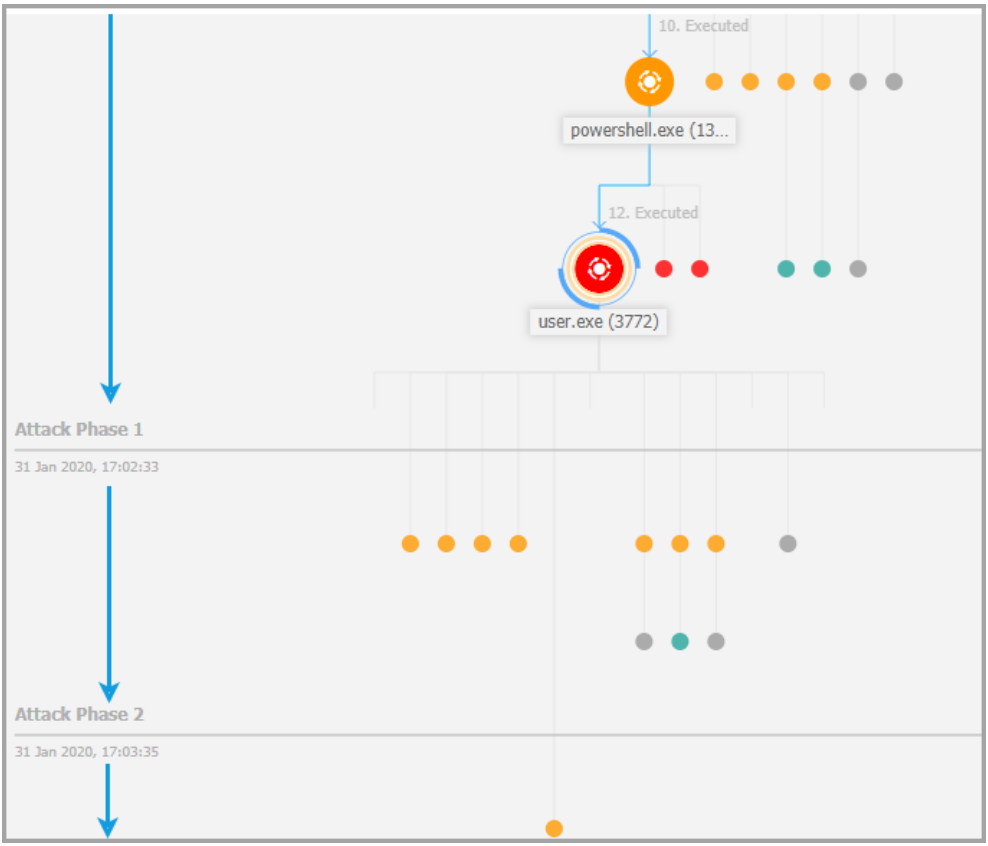
Следующие элементы инцидента могут быть представлены как узлы:

Тип узла	Описание
Конечная точка	Отображает сведения о конечной точке и статусе управления патчами.

Тип узла	Описание
Домен	Показывает информацию о хосте домена и его конечных точках.
Процесс	Отображает сведения о роли процесса в текущем инциденте, информацию о файле, сведения о выполнении процесса, присутствие в сети и дополнительные параметры расследования.
Файл	Показывает сведения о роли файла в текущем инциденте, информацию о файле, присутствие в сети и дополнительные параметры расследования.
Реестр	Отображает информацию Реестра и детали родительского процесса.

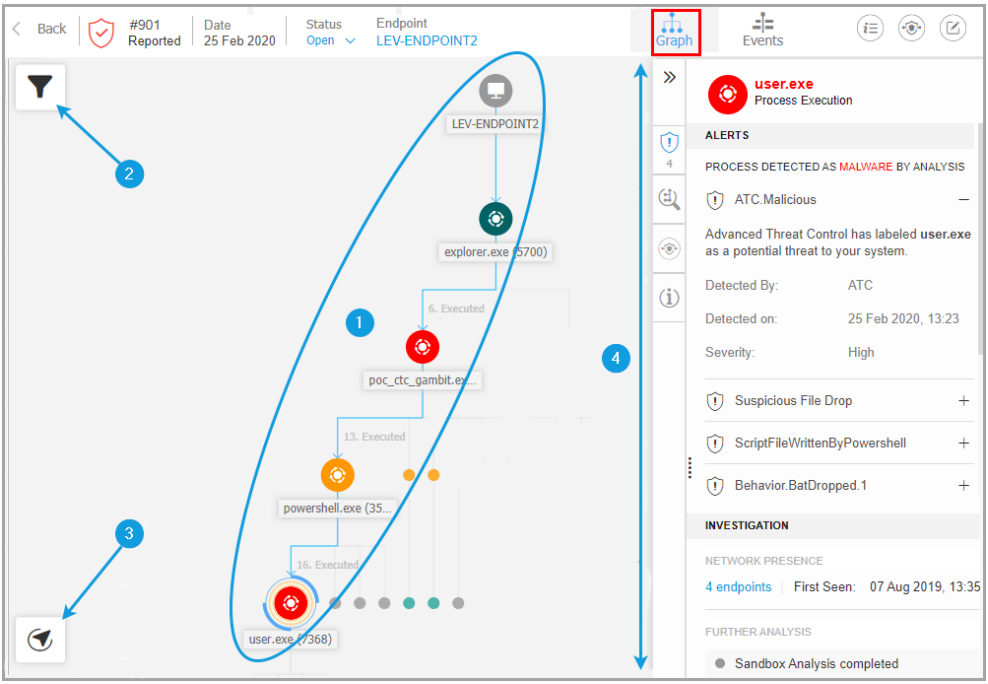
График

График предоставляет интерактивное графическое представление расследуемого инцидента и его контекста, выделяя последовательность элементов, напрямую участвующих в его инициировании, известную как **Критический путь** инцидента, а также всех других задействованных элементов, которые по умолчанию постепенно исчезают. В случае сложных инцидентов, которые развиваются с течением времени, на графике отображается каждый этап атаки.



Поэтапная атака

График включает параметры фильтрации, которые позволяют настраивать график инцидентов для улучшения визуализации, функций навигации по карте инцидентов и панели с подробной информацией о каждом элементе.



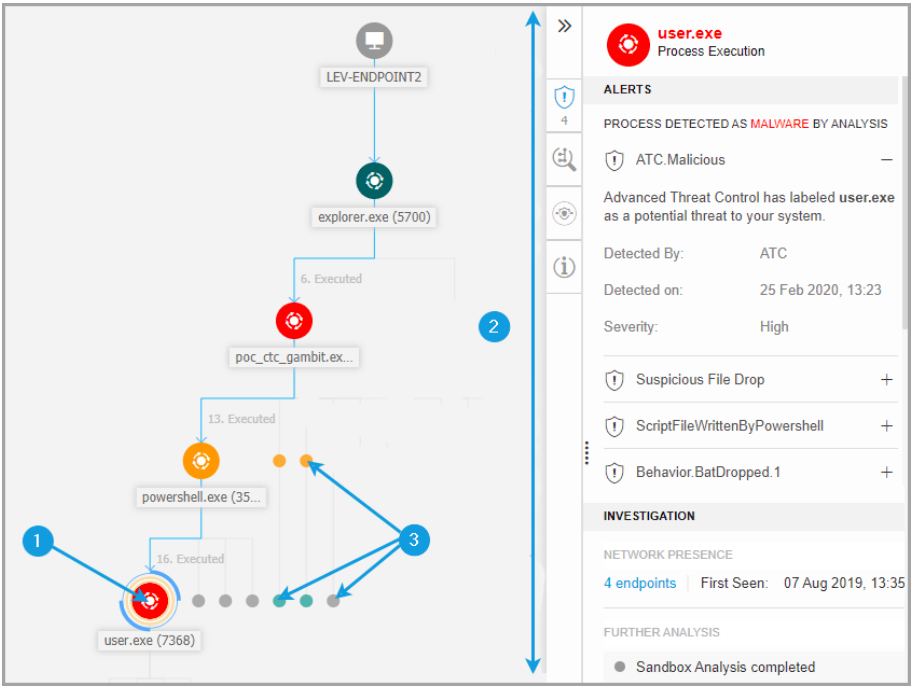
Вкладка «График»

1. Критический путь
2. Меню фильтров
3. Меню навигатора
4. Панель сведений об узле

Критический путь

Критический путь - это последовательность связанных событий безопасности, которые привели к отправке предупреждения, начиная с точки входа в сеть и заканчивая узлом события, который вызвал инцидент. Критический путь инцидента по умолчанию выделяется на графике вместе со всеми содержащимися на нем узлами событий, в то время как остальные элементы свернуты.

Триггерный узел легко выделяется на фоне остальных элементов графика, будучи окруженным дополнительными выделенными элементами (двумя оранжевыми кружками), и по умолчанию рядом с графиком инцидента отображается связанная информационная панель, предоставляя подробную информацию о триггерном узле.



Критический путь

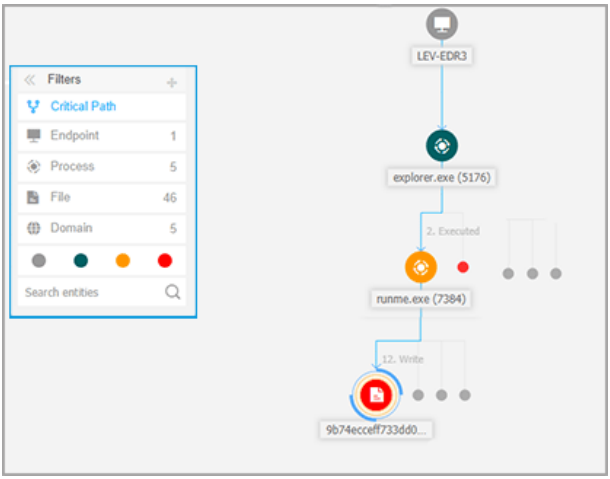
1. Триггерный узел
2. Панель сведений об узле с информацией, сгруппированной по категориям и разворачивающимся разделам
3. Постепенно исчезающие узлы, косвенно вовлеченные в инцидент

Примечание
Щелчок по любому другому элементу, кроме триггерного узла, нарушит критический путь и выделит путь к источнику, от выбранного узла выше до узла конечной точки.

Фильтры

Меню **Фильтры** предоставляет вам расширенные возможности фильтрации, позволяя полностью управлять графиком инцидента, выделяя элементы на основе их типа или релевантности, или скрывая их, чтобы сделать инцидент более компактным и простым для анализа.

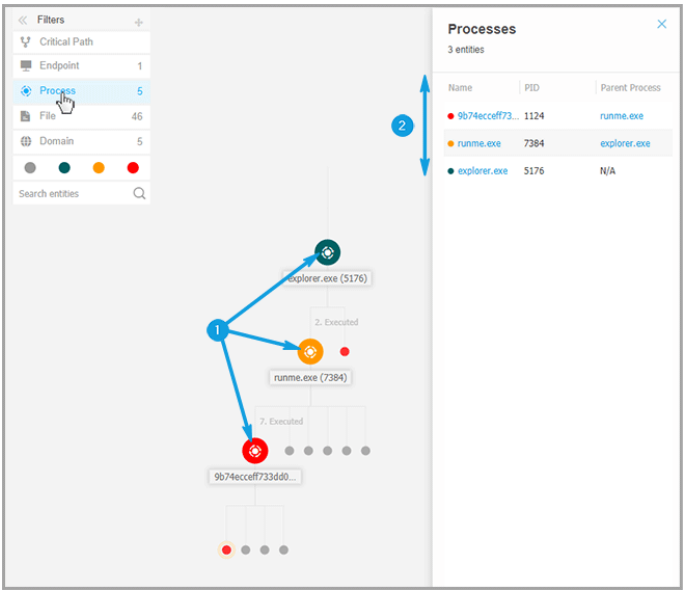
Нажмите и удерживайте значок **Перетащить**, чтобы расположить плавающую панель Фильтры в любом месте внутри графика инцидентов.



Фильтры графика инцидентов

При выборе фильтра типа элемента:

1. График инцидента сжимает и выделяет все элементы выбранного типа, в то время как элементы другого типа исчезают.
2. Он мгновенно открывает панель со списком всех выделенных элементов.



Примечание
Выбор элемента в отображаемом списке выделит его на графике инцидента и откроет панель сведений с информацией по этому элементу.
Только один фильтр может быть применен одновременно.

Параметры фильтрации включают в себя:

- **Критический путь**. Выделяет критический путь инцидента.
- **Конечная точка**. Выделяет конечные точки, затронутые инцидентом.
- **Процесс**: выделяет все узлы процессного типа, связанные с инцидентом.
- **Файл**. Выделяет узлы файлового типа, связанные с инцидентом.
- **Домен**. Выделяет все узлы доменного типа, связанные с инцидентом.
- **Реестр**. Выделяет все узлы реестрового типа, связанные с инцидентом.

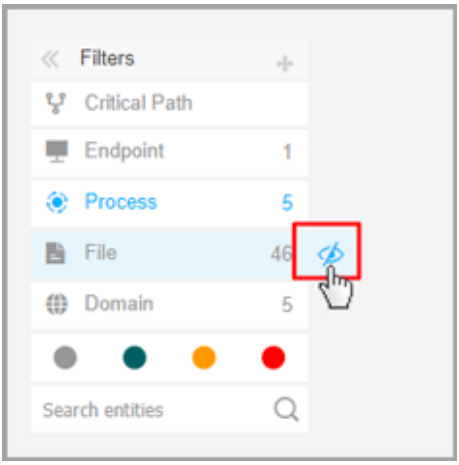
- **Релевантность элементов**. Вы также можете фильтровать элементы по их важности внутри инцидента.
  - **Нейтральный узел**: элементы без прямого воздействия на инцидент безопасности.
  - **Важный узел**: элементы с важной ролью в инциденте безопасности.
  - **Исходный узел**: Точка входа в атаку внутри сети.
  - **Подозрительный узел**: элементы с подозрительным поведением, напрямую связанные с инцидентом безопасности.
  - **Вредоносный узел**: элементы, которые нанесли ущерб вашей сети.

    Примечание
    Наведение курсора на любой из цветных фильтров отображает, какое количество элементов с одинаковой релевантностью вовлечено в инцидент.

- **Поиск объектов**. Вы можете искать имена или расширения файлов компонентов инцидента в поле поиска, и результаты будут отображаться на боковой панели.

Если фильтры не выбраны, график инцидентов сбрасывается до умолчания, при этом элементы конечной точки, источника и триггера подсвечиваются, а остальные элементы постепенно исчезают.

Вы также можете скрыть определенные элементы из графика инцидентов, нажав кнопку **Показать / Скрыть**, отображаемую при наведении указателя мыши на фильтры типа: Файл, Домен и Реестр.



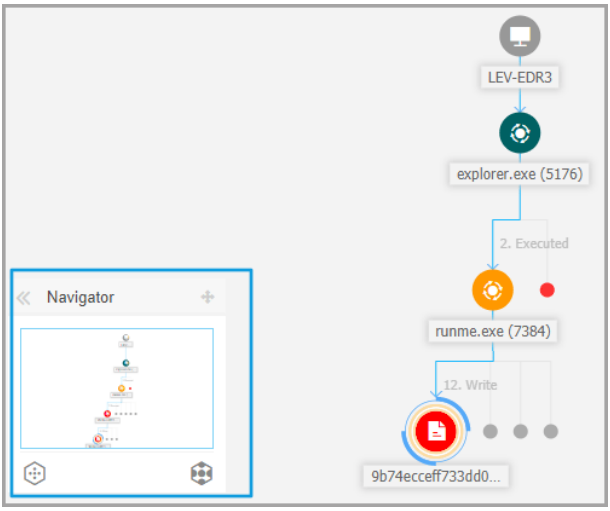
Скрытие типа элемента перерисовывает график инцидентов, удаляя все соответствующие элементы, даже если они сжаты, исключая триггерный узел и узлы с дочерними элементами.

Навигатор

Навигатор позволяет быстро перемещаться по графику инцидентов и исследовать все отображаемые элементы с помощью мини-карты и различных уровней визуализации.

Нажмите и удерживайте значок **Перетащить**, чтобы расположить плавающую панель Навигатор в любом месте внутри графика инцидентов.

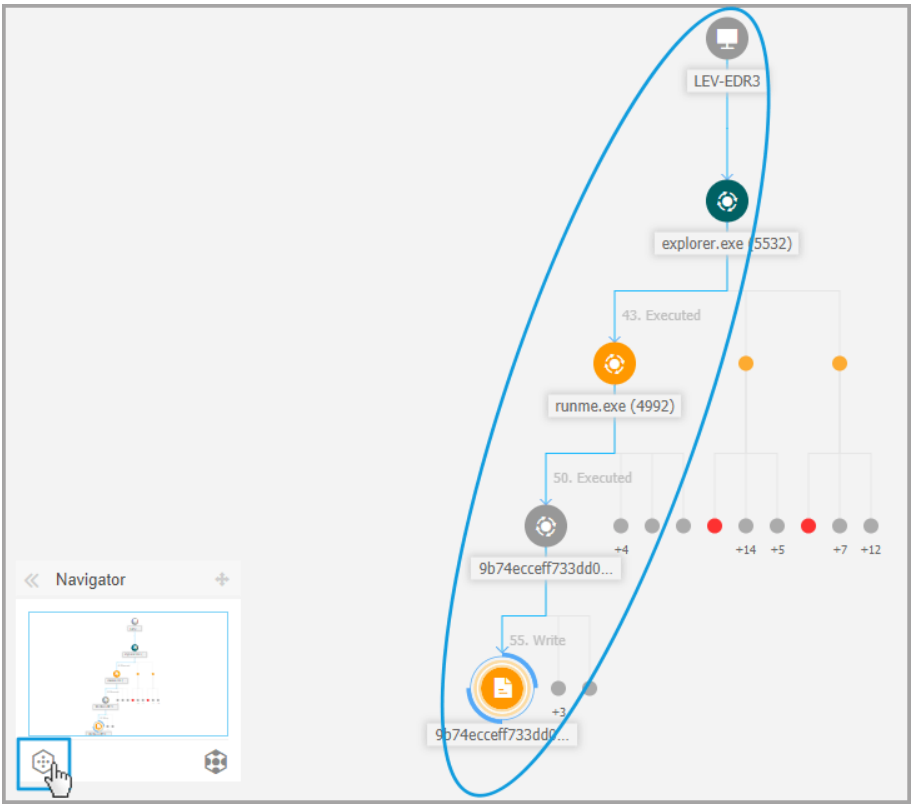
Навигатор свернут по умолчанию. При его расширении в меню будет отображаться миниатюрная версия всей карты инцидентов и кнопки действий для настройки уровня визуализации.



Навигатор

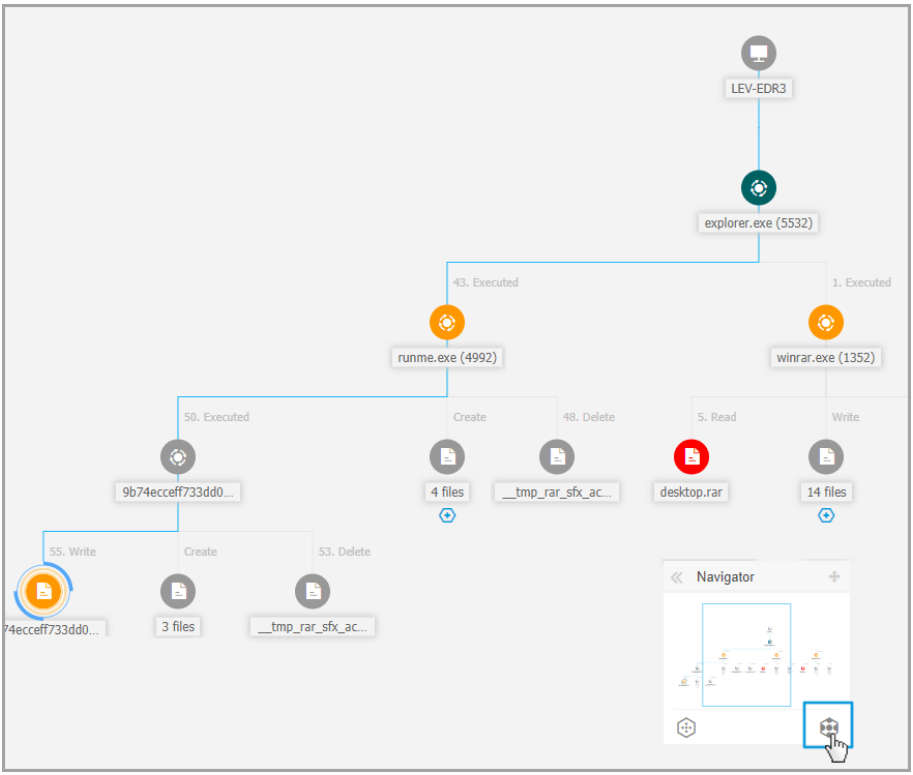
Меню **Навигатор** содержит две кнопки действий для настройки визуализации графика инцидентов: кнопка **Скрыть детали** и кнопка **Подробнее**.

Когда вы нажимаете кнопку **Меньше деталей**, график устанавливается в состояние по умолчанию, выделяя только критический путь инцидента.



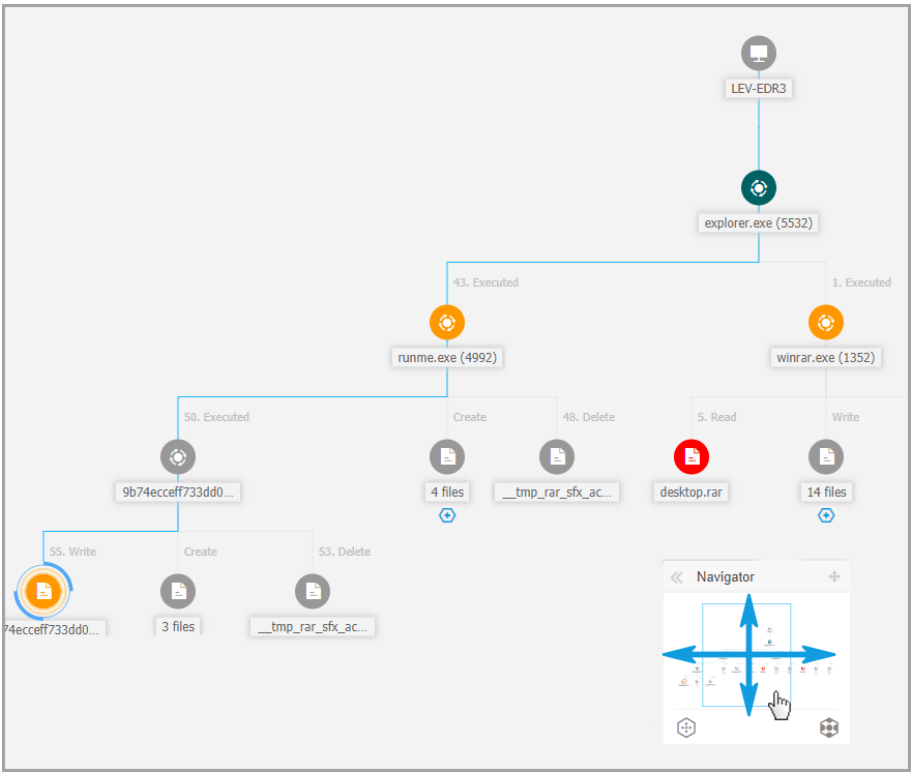
Обзорная визуализация

Когда вы нажмете кнопку **Подробнее**, все элементы графика инцидентов раскрываются, выделяя каждый узел и кластеры узлов.



Увеличенная визуализация

Когда инцидент увеличен и все элементы выделены, график часто может выходить за пределы экрана. В этом случае удерживайте и перетащите селектор карты на мини-карте навигатора, чтобы легко перемещаться в нужную область карты инцидентов, или просто перетащите область графика в нужное направление.

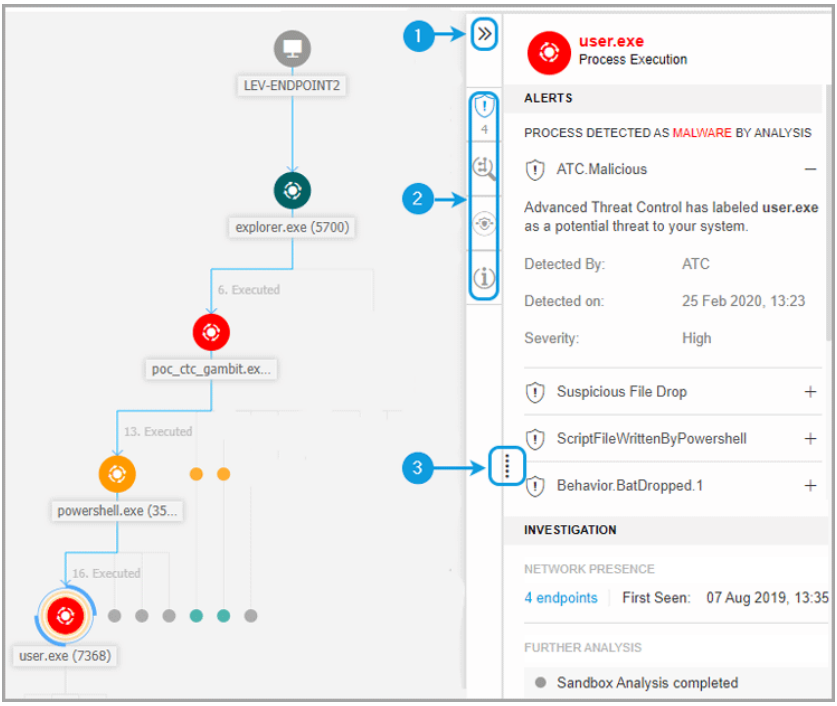


Селектор мини-карты

Сведения об узле

Панель **Сведения об узле** содержит разделы с подробной информацией о выбранном узле, включая действия по предотвращению или исправлению, которые можно предпринять для смягчения инцидента, подробности о типе обнаружения и обнаруженных оповещениях на узле, присутствии в сети, подробностях выполнения процесса, дополнительных рекомендациях по управлению событием безопасности или действиях для дальнейшего исследования элемента.

Чтобы просмотреть эту информацию и выполнить действия на панели, выберите узел на карте событий безопасности.



Панель сведений об узле

1. Вы можете свернуть или развернуть панель **Сведения об узле**, нажав кнопку **Свернуть**.
2. Вы можете легко ориентироваться в информации, отображаемой на панели **Сведения об узле**, щелкая иконки каждой из четырех основных категорий:
   - **ОПОВЕЩЕНИЯ**

     В этом разделе отображаются одно или несколько обнаружений, спровоцированных на выбранном узле, включая сведения о технологии Bitdefender, включившей элемент в инцидент, причину, по которой было спровоцировавшую обнаружение, имя обнаружения и дату, когда он был обнаружен.
   - **Исследование**

В этом разделе отображаются метки даты для начального обнаружения и все конечные точки, где был обнаружен этот элемент.

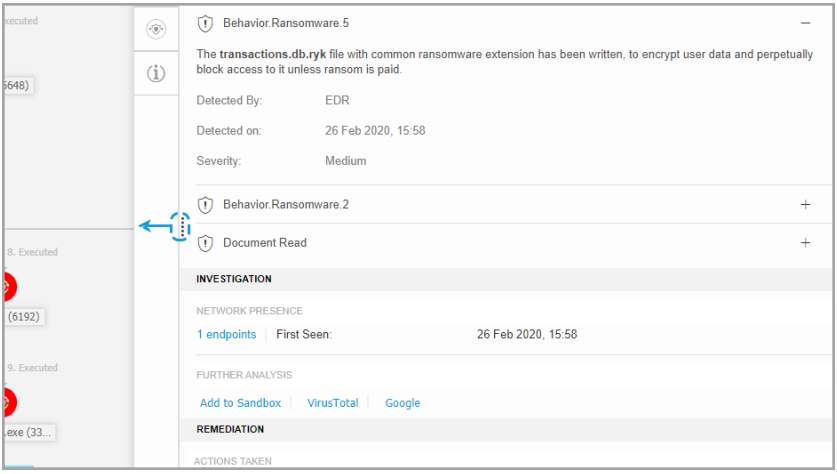
- **Исправление**

  В этом разделе отображаются действия, автоматически выполненные GravityZone, действия, которые вы можете предпринять немедленно для уменьшения угрозы, а также подробные рекомендации для каждого предупреждения, обнаруженного на выбранном узле, чтобы помочь вам в смягчении инцидента и повышении уровня безопасности вашей среды.

- **ИНФОРМАЦИЯ**

  В этом разделе отображается общая информация о каждом файле и конкретная информация в зависимости от типа выбранного узла.

3. Вы можете перетащить панель **Сведения об узле** по направлению к центру экрана, чтобы легко просмотреть его содержимое.



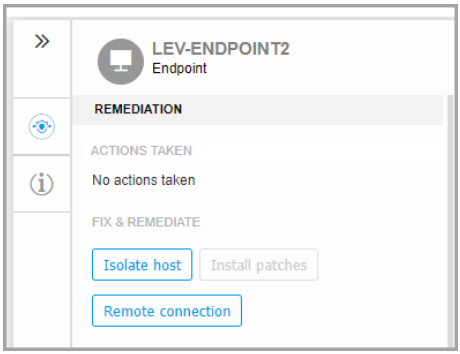
Расширенная панель

Панель сведений для узлов конечных точек

Панель **Сведения об узле** для конечных точек включает две категории:

- **Исправление**

Отображает информацию о действиях, автоматически предпринятых GravityZone для уменьшения угроз и действий, которые вы можете совершить:

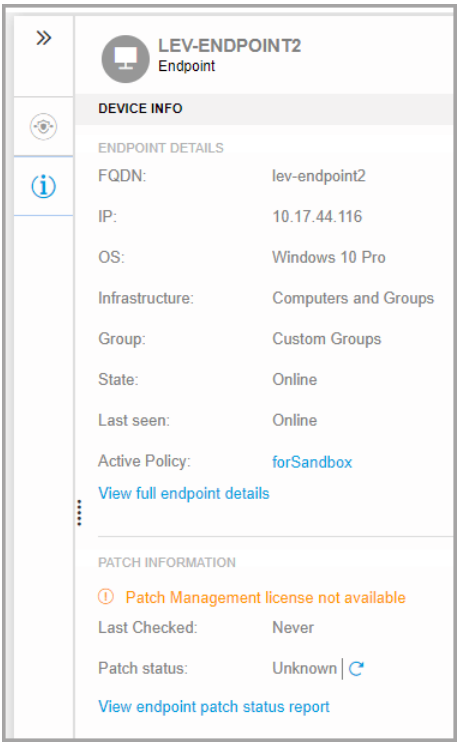


- **Изолировать хост** - используйте это действие, чтобы изолировать конечную точку от сети.
- **Установить патчи** - используйте это действие для установки отсутствующего патча безопасности на целевой конечной точке. Эта опция видна только с модулем Patch Management, надстройкой, доступной с отдельным лицензионным ключом. Обратитесь к Установке патча для получения дополнительной информации.
- **Remote Connection** - используйте это действие, чтобы установить удаленное подключение к конечной точке, участвующей в текущем инциденте, и выполнить ряд пользовательских команд оболочки напрямую в своей операционной системе для немедленного смягчения угрозы или сбора данных для дальнейшего расследования.

  При нажатии на эту кнопку отобразится окно Удаленное подключение.

- **ИНФОРМАЦИЯ ОБ УСТРОЙСТВЕ**

  Отображает общую информацию о затронутой конечной точке, такую как имя конечной точки, IP-адрес, операционная система, соответствующая группа, состояние, активные политики и ссылка, которая открывает новое окно, в котором отображаются полные сведения о конечной точке.



Также предоставляет вам такую информацию, как количество установленных исправлений, неисправных исправлений или отсутствующих исправлений по безопасности и не по безопасности. Кроме того, вы можете создать отчет о состоянии исправления конечной точки. Этот раздел предоставляется по запросу для целевой конечной точки.

На панели можно выполнить следующие действия:

– Просмотреть информацию об исправлениях для целевой конечной точки. Чтобы просмотреть сведения о патче, нажмите **Обновить** в этом разделе.

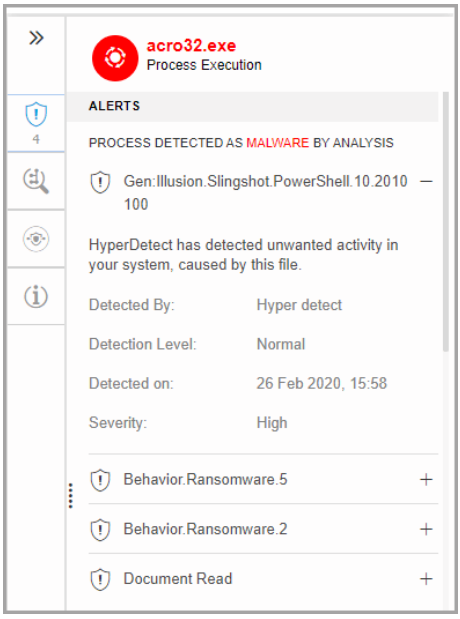
– Просмотреть отчет о состоянии исправления для целевой конечной точки. Чтобы сформировать отчет, нажмите **Просмотреть отчет о состоянии исправлений конечной точки**.

Панель сведений для узлов процесса

Панель **Сведения об узле** для узлов процесса включает четыре категории:

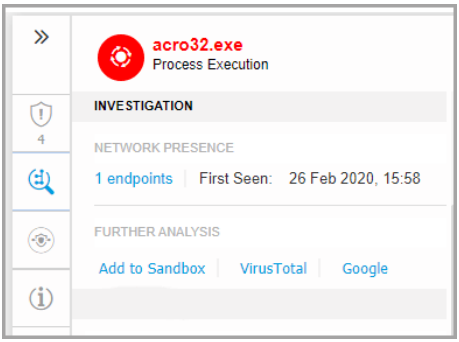
- **ОПОВЕЩЕНИЯ**

  Отображает одно или несколько обнаружений, инициированных на выбранном узле, включая сведения о технологии Bitdefender, которая включила этот элемент в инцидент, причину, по которой было инициировано обнаружение, имя обнаружения и дату, когда оно было обнаружено. Описание каждого предупреждения соответствует последним стандартам MITRE.

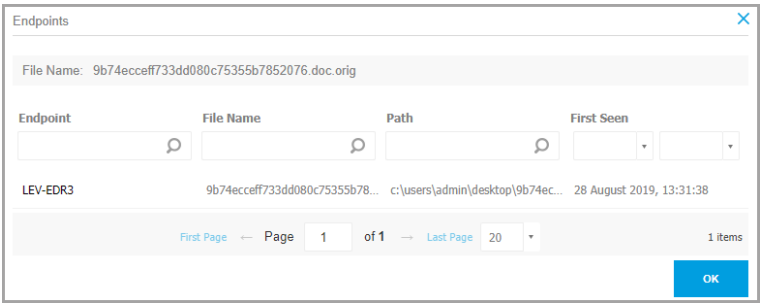


- **Исследование**

  Отображает метки даты для начального обнаружения и все конечные точки, где был обнаружен этот элемент.



Чтобы просмотреть этот список, щелкните число, указанное в поле **конечных точек**, и появится новое окно.

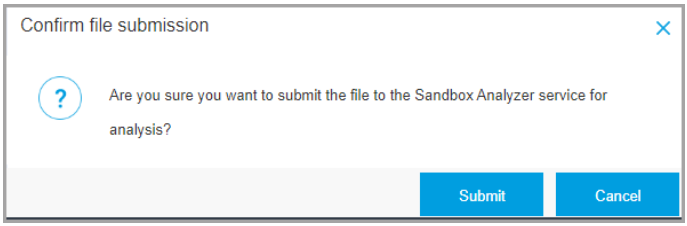


В этом разделе также представлен внешний анализ с помощью внутренних компонентов и сторонних решений.

Доступны следующие действия:

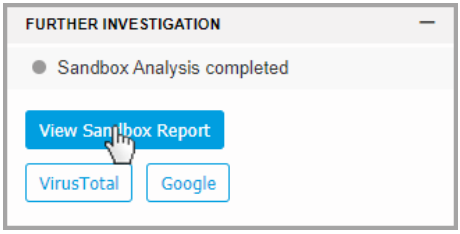
– **Добавить в песочницу** - используйте это действие для создания отчета Sandbox Analyzer.

  Выбор **Добавить в песочницу** предложит вам экран для подтверждения отправки файла.



После подтверждения вы будете автоматически перенаправлены к экрану представления.

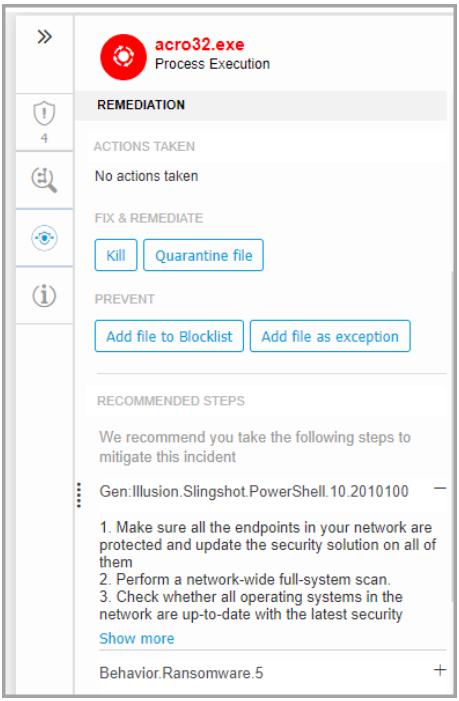
По завершении анализа нажмите кнопку **Просмотреть отчет песочницы**, чтобы открыть полный отчет.



- **VirusTotal** - используйте это действие для внешней отправки файла на анализ.
- **Google** - используйте это действие для поиска хеш-значения файла.

- **Исправление**

  Отображает информацию о действиях, автоматически предпринятых GravityZone для уменьшения угроз и действий, которые вы можете совершить:



- **Завершить процесс** - используйте это действие, чтобы остановить выполнение процесса. Это действие создает задачу уничтожения процесса, видимую в панели выполнения процесса. `Процессы System32` и Bitdefender исключены из этого действия.
- **Файл карантина** - используйте это действие, чтобы сохранить рассматриваемый элемент и предотвратить размещение им полезных данных. Это действие требует, чтобы модуль брандмауэра был установлен на целевой конечной точке.
- **Добавить файл в Черный список** - управлять заблокированными элементами в разделе Черный список.
- **Добавить файл как исключение** - используйте эту опцию, чтобы исключить законную активность в определенной политике. Когда вы выбираете это действие, окно конфигурации предлагает вам выбрать

политику, в которую вы хотите добавить исключение. Управляйте исключениями в **Политика > Антивредоносное > Настройки**.

– **Добавить как исключение EDR** - используйте этот параметр для создания пользовательского правила, которое больше не будет рассматривать процесс как подозрительное или вредоносное обнаружение EDR.

1. Когда Вы нажимаете кнопку **Добавить как исключение EDR**, появляется новое окно с предложением подтвердить действие или отменить его.
2. После подтверждения действия GravityZone уведомляет Вас о том, что новое правило доступно в сетке Правила исключения. Обратите внимание, что имя всех правил, полученных из графика инцидентов, начинается с номера инцидента.

Примечание
Когда Вы начнете изучать правило подробно, чтобы отредактировать его, Вы заметите, что все критерии для него были заполнены автоматически, а добавлен был лишь критерий для чтения с именем предупреждения.

Важно
Функция **Добавить как EDR Исключение** доступна только для:

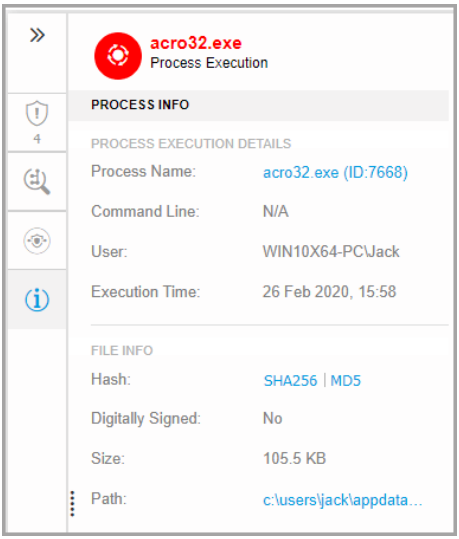
- сигналы, вызванные технологией EDR
- узлы, возникшие при других процессах.
- подозрительные или зловредные узлы

Если исключенный процесс является частью критического пути инцидента, то будущие инциденты, соответствующие этому критерию исключения, больше не будут генерироваться в сетке инцидентов. состоящие из них события по-прежнему будут доступны для просмотра и анализа на странице Поиск.
Если исключенный процесс не является частью критического пути инцидента, то будущие инциденты, соответствующие этому критерию исключения, все равно будут генерироваться в сетке инцидентов, но этот процесс большевике будет рассматриваться как подозрительный или вредоносный.

В данном разделе также содержится подробные рекомендации для каждого оповещения, обнаруженного на выбранном узле, чтобы помочь Вам смягчить инцидент и повысить уровень безопасности Вашей среды.

- **ИНФОРМАЦИЯ О ПРОЦЕССЕ**

  Отображает сведения о выбранном узле процесса, включая имя процесса, выполненную командную строку, пользователя, время выполнения, происхождение и путь файла, значение хеша, или цифровую подпись.



Вы можете скопировать значение хеша в буфер обмена, щелкнув доступные алгоритмы хеширования в поле **Хэш**, а затем **Копировать в буфер обмена** и использовать его для добавления значения хэша файла в **Черный список**. Для получения дополнительной информации см. **Занесение файлов в Черный список** .

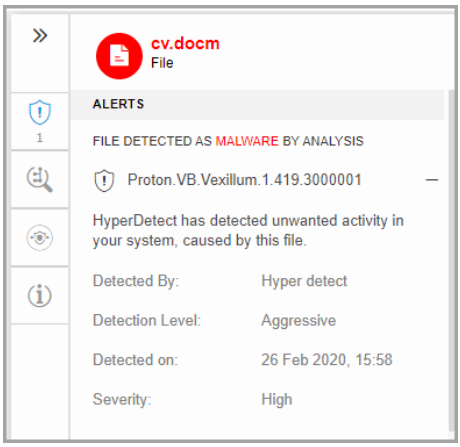
Панель сведений для файловых узлов

Панель **Сведения об узле** для файловых узлов включает четыре категории:

- **ОПОВЕЩЕНИЯ**

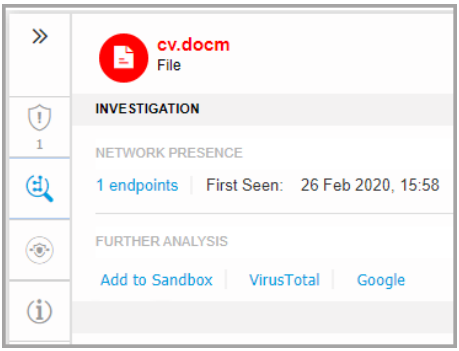
  Отображает одно или несколько обнаружений, инициированных на выбранном узле, включая сведения о технологии Bitdefender, которая

включила этот элемент в инцидент, причину, по которой было инициировано обнаружение, имя обнаружения и дату, когда оно было обнаружено. Описание каждого предупреждения соответствует последним стандартам MITRE.

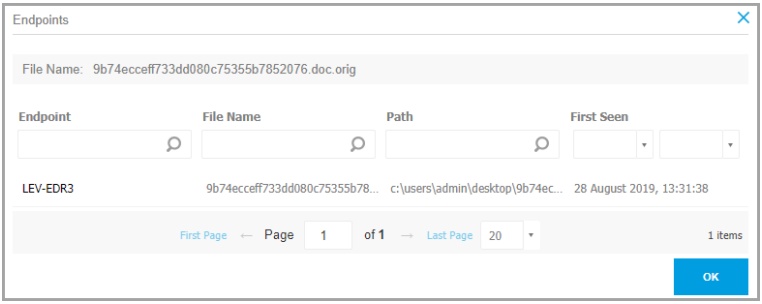


- **Исследование**

  Отображает метки даты для начального обнаружения и все конечные точки, где был обнаружен этот элемент.



Чтобы просмотреть этот список, щелкните число, указанное в поле **конечных точек**, и появится новое окно.

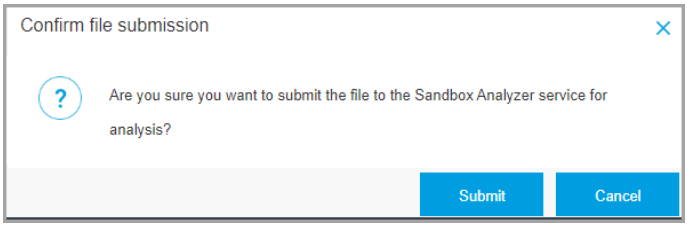


В этом разделе также представлен внешний анализ с помощью внутренних компонентов и сторонних решений.

Доступны следующие действия:

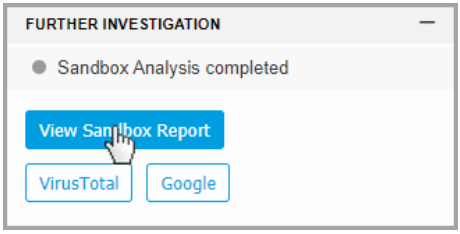
– **Добавить в песочницу** - используйте это действие для создания отчета Sandbox Analyzer.

  Выбор **Добавить в песочницу** предложит вам экран для подтверждения отправки файла.



После подтверждения вы будете автоматически перенаправлены к экрану представления.

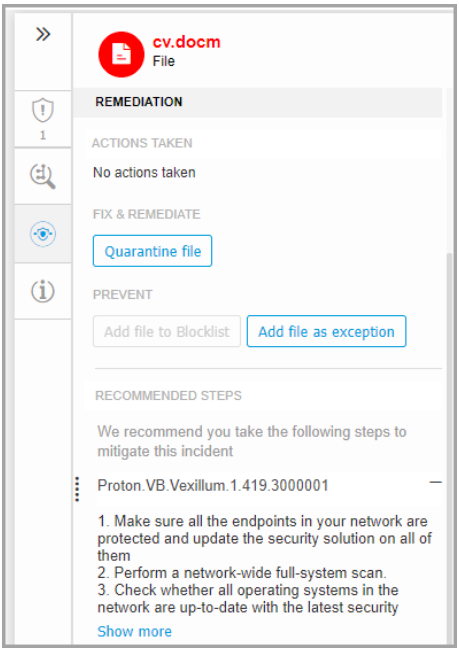
По завершении анализа нажмите кнопку **Просмотреть отчет песочницы**, чтобы открыть полный отчет.



- **VirusTotal** - используйте это действие для внешней отправки файла на анализ.
- **Google** - используйте это действие для поиска хеш-значения файла.

- **Исправление**

  Отображает информацию о действиях, автоматически предпринятых GravityZone для уменьшения угроз и действий, которые вы можете совершить:



- **Файл карантина** - используйте это действие, чтобы сохранить рассматриваемый элемент и предотвратить размещение им полезных данных. Это действие требует, чтобы модуль брандмауэра был установлен на целевой конечной точке.
- **Добавить файл в Черный список** - управлять заблокированными элементами в разделе Черный список.
- **Добавить файл как исключение** - используйте эту опцию, чтобы исключить законную активность в определенной политике. Когда вы выбираете это действие, окно конфигурации предлагает вам выбрать политику, в которую вы хотите добавить исключение. Управляйте исключениями в **Политика > Антивредоносное > Настройки**.
- **Добавить как исключение EDR** - используйте этот параметр для создания пользовательского правила, которое больше не будет рассматривать файл как подозрительное или вредоносное обнаружение EDR.

1. Когда Вы нажимаете кнопку **Добавить как исключение EDR**, появляется новое окно с предложением подтвердить действие или отменить его.
2. После подтверждения действия GravityZone уведомляет Вас о том, что новое правило доступно в сетке Правила исключения. Обратите внимание, что имя всех правил, полученных из графика инцидентов, начинается с номера инцидента.

Примечание
Когда Вы начнете изучать правило подробно, чтобы отредактировать его, Вы заметите, что все критерии для него были заполнены автоматически, а добавлен был лишь критерий для чтения с именем предупреждения.

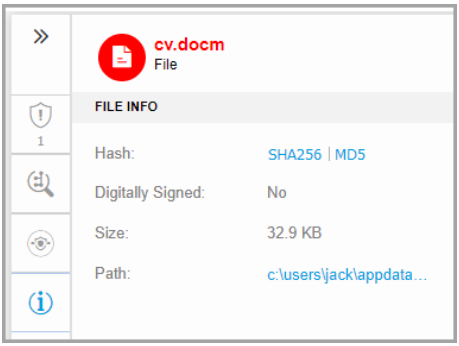
Важно
Функция **Добавить как EDR Исключение** доступна только для:

- сигналы, вызванные технологией EDR
- узлы, возникшие при других процессах.
- подозрительные или зловредные узлы

Если исключенный файл является частью критического пути инцидента, то будущие инциденты, соответствующие этому критерию исключения, больше не будут генерироваться в сетке инцидентов. состоящие из них события по-прежнему будут доступны для просмотра и анализа на странице Поиск.
Если исключенный файл не является частью критического пути инцидента, то будущие инциденты, соответствующие этому критерию исключения, все равно будут генерироваться в сетке инцидентов, но этот процесс большевике будет рассматриваться как подозрительный или вредоносный.

В данном разделе также содержится подробные рекомендации для каждого оповещения, обнаруженного на выбранном узле, чтобы помочь Вам смягчить инцидент и повысить уровень безопасности Вашей среды.

- **Информация о файле**



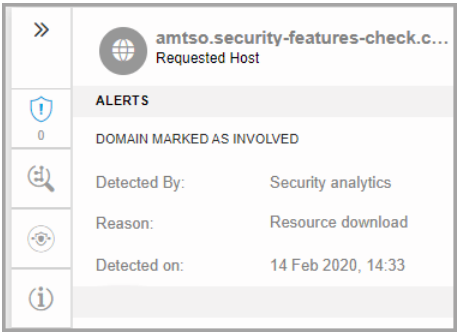
Вы можете скопировать значение хеша в буфер обмена, щелкнув доступные алгоритмы хеширования в поле **Хэш**, а затем **Копировать в буфер обмена** и использовать его для добавления значения хэша файла в **Черный список**. Для получения дополнительной информации см. **Занесение файлов в Черный список** .

Панель сведений для узлов домена

Панель **Сведения об узле** для узлов домена включает четыре категории:

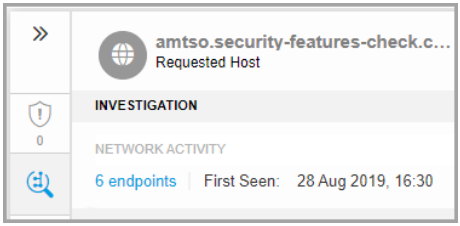
- **ОПОВЕЩЕНИЯ**

  Отображает серьезность домена, отмеченную технологией Bitdefender, которая включала эту сущность в инцидент, причину, которая вызвала обнаружение, и дату, когда она была обнаружена.

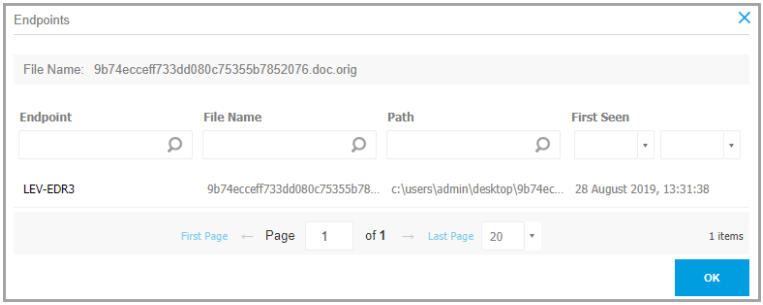


- **Исследование**

  Отображает метки даты для начального обнаружения и все конечные точки, где был обнаружен этот элемент.

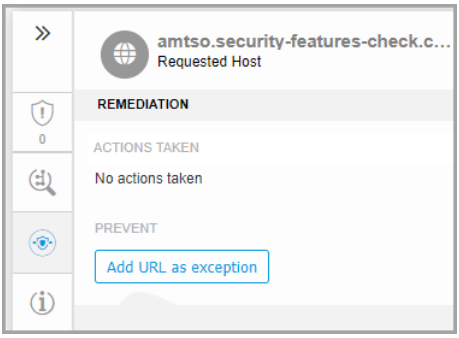


  Чтобы просмотреть этот список, щелкните число, указанное в поле **конечных точек**, и появится новое окно.



- **Исправление**

  Отображает информацию о действиях, автоматически предпринятых GravityZone для уменьшения угроз и действий, которые вы можете совершить:



- **Добавить URL как исключение** - используйте эту опцию, чтобы исключить законную активность в определенной политике. Когда вы выбираете это действие, окно конфигурации предлагает вам выбрать политику, в которую вы хотите добавить исключение. Управляйте исключениями в **Политика > Антивредоносное > Настройки**.
- **Добавить как исключение EDR** - используйте этот параметр для создания пользовательского правила, которое больше не будет рассматривать домен как подозрительное или вредоносное обнаружение EDR.

  1. Когда Вы нажимаете кнопку **Добавить как исключение EDR**, появляется новое окно с предложением подтвердить действие или отменить его.
  2. После подтверждения действия GravityZone уведомляет Вас о том, что новое правило доступно в сетке Правила исключения. Обратите внимание, что имя всех правил, полученных из графика инцидентов, начинается с номера инцидента.

  Примечание
  Когда Вы начнете изучать правило подробно, чтобы отредактировать его, Вы заметите, что все критерии для него были заполнены автоматически, а добавлен был лишь критерий для чтения с именем предупреждения.

  Важно
  Функция **Добавить как EDR Исключение** доступна только для:

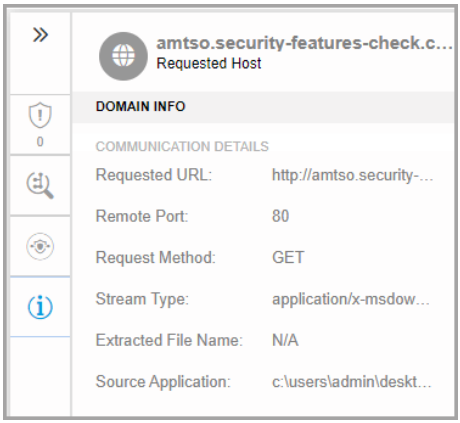
- сигналы, вызванные технологией EDR
- узлы, возникшие при других процессах.
- подозрительные или зловредные узлы

Если исключенный домен является частью критического пути инцидента, то будущие инциденты, соответствующие этому критерию исключения, больше не будут генерироваться в сетке инцидентов. состоящие из них события по-прежнему будут доступны для просмотра и анализа на странице Поиск.

Если исключенный домен не является частью критического пути инцидента, то будущие инциденты, соответствующие этому критерию исключения, все равно будут генерироваться в сетке инцидентов, но этот процесс большевике будет рассматриваться как подозрительный или вредоносный.

- **ИНФОРМАЦИЯ О ДОМЕНЕ**

  Отображает сведения о выбранном узле домена, включая запрошенный URL-адрес, используемый порт, метод запроса, тип потока, имя извлеченного файла, исходное приложение.

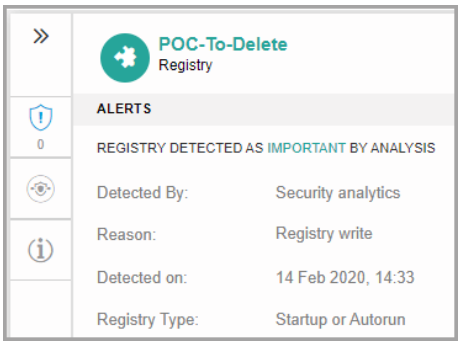


Панель сведений для узлов реестра

Панель **Сведения об узле** для узлов реестра включает три категории:

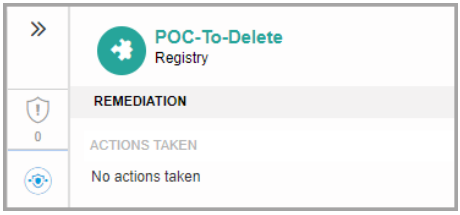
- **ОПОВЕЩЕНИЯ**

Отображает степень серьезности манипулирования реестром, отмеченную технологией Bitdefender, которая включала эту сущность в инцидент, причину, которая вызвала обнаружение, дату, когда оно было обнаружено, и тип реестра.



- **Исправление**

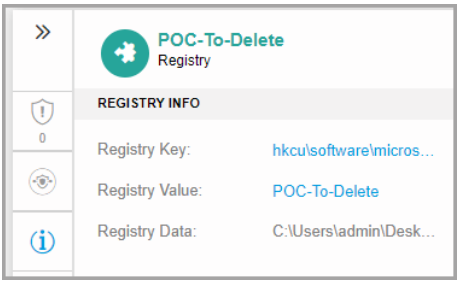
  Отображает информацию о действиях, выполненных автоматически GravityZone.



  Раздел **ИСПРАВЛЕНИЕ** для узлов реестра не предоставляет никаких опций пользовательских действий.

- **ИНФОРМАЦИЯ О РЕЕСТРЕ**

  Отображает подробную информацию о выбранном узле реестра, включая ключ реестра, значение и данные.

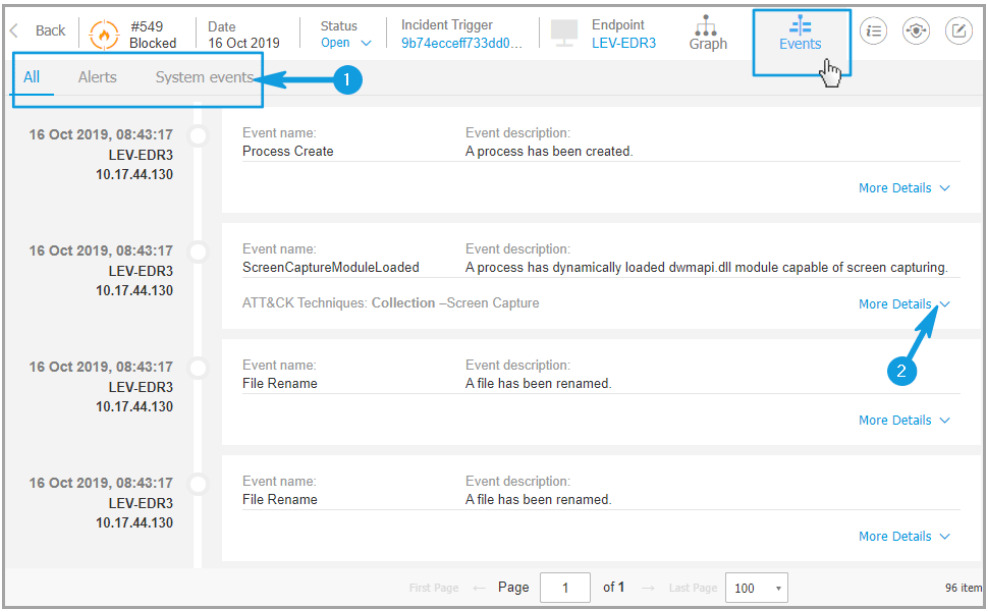


Вы можете щелкнуть ключ реестра и значение, чтобы скопировать его в буфер обмена для дальнейшего анализа.

События (Events)

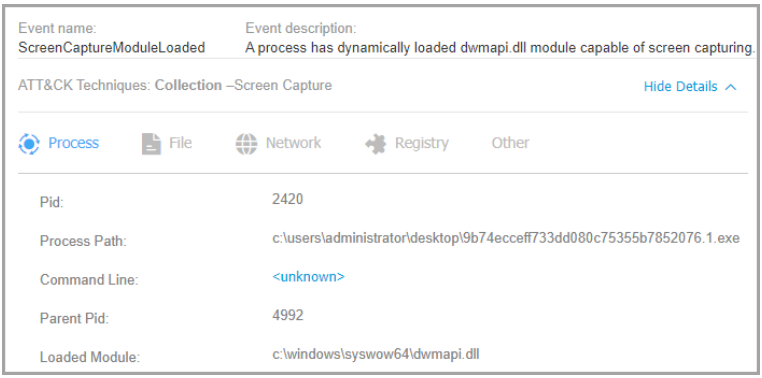
Используйте вкладку **События**, чтобы увидеть, как разворачивалась последовательность событий, спровоцировавшая расследуемый инцидент. В этом окне отображаются коррелированные системные события и предупреждения, обнаруженные с помощью технологий GravityZone, таких как EDR, Network Attack Defense, Anomaly Detection (обнаружение аномалий), Advanced Anti-Exploit (расширенная защита от эксплойтов), Windows Antimalware Scan Interface (AMSI) (интерфейс сканирования вредоносных программ Windows).

Каждое сложное событие имеет подробное описание, объясняющее, что было обнаружено и что может произойти, если артефакт используется в злонамеренных целях в соответствии с новейшими технологиями и тактиками MITRE.



Вкладка «События»

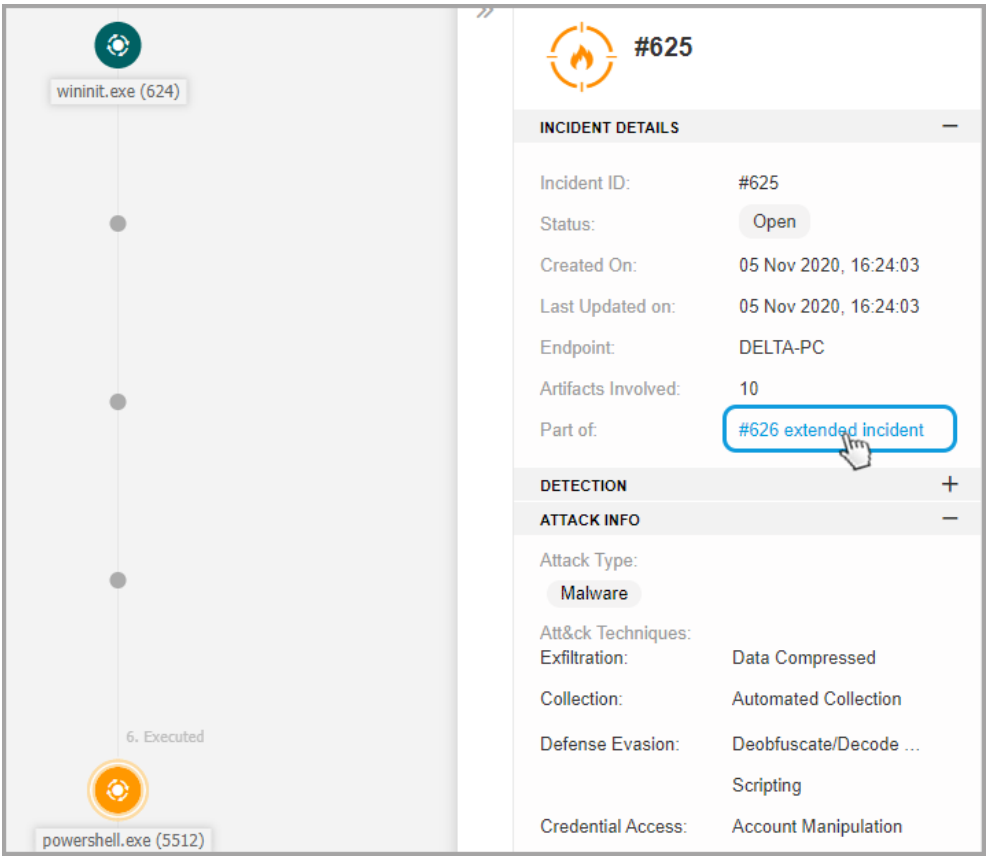
1. Используйте параметры фильтрации для отображения всех событий или только системных событий или сложных событий (предупреждений).
2. Нажмите кнопку **Подробнее**, чтобы развернуть каждое событие и получить доступ к дополнительной информации.



Сведения об инциденте

Эта панель содержит сворачиваемую область с такими деталями, как идентификатор инцидента, текущее состояние, время и дата его создания и последнего обновления, количество задействованных артефактов, имя триггера, описание и информация об атаке.

В этом разделе Вы можете получить доступ к расширенному инциденту, включающему в себя произошедшее на конечных точках, как пример.



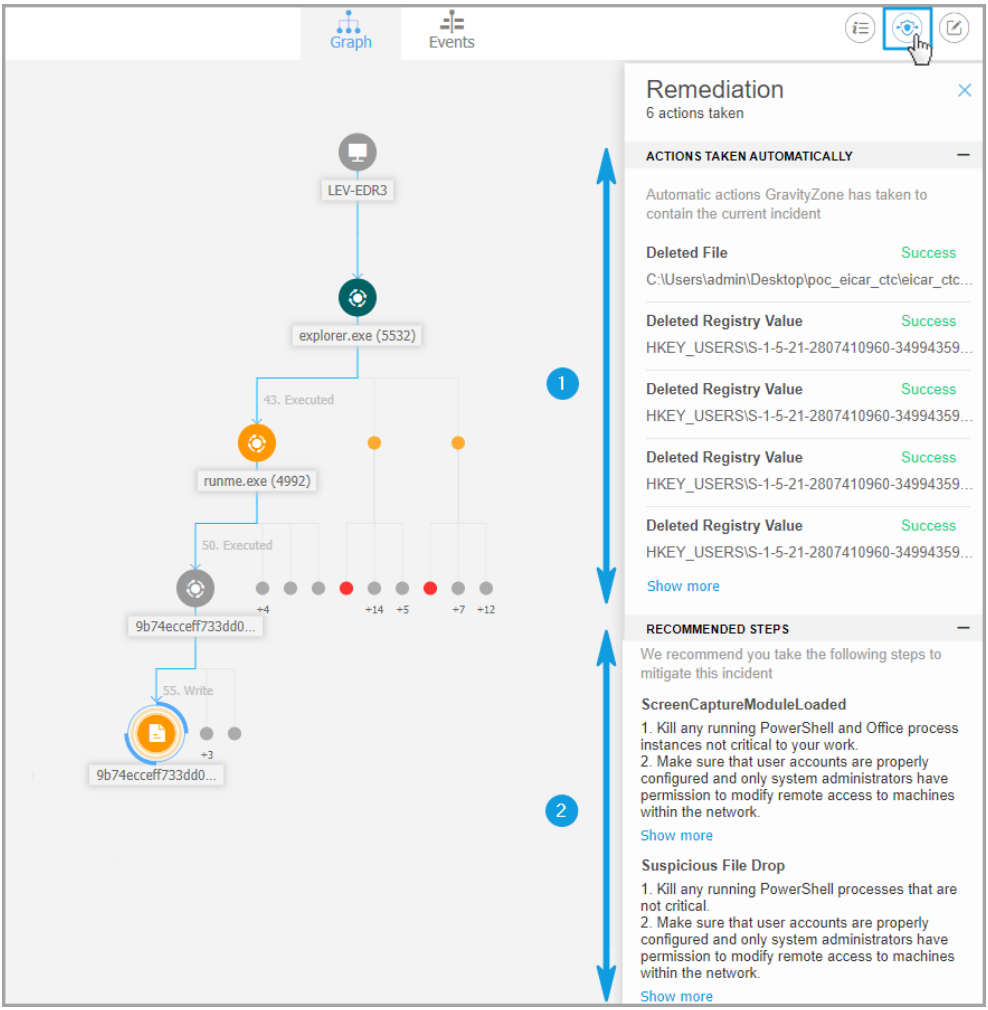
Панель сведений об инцидентах

Панель также содержит предупреждения, обнаруженные на элементе, который спровоцировал инцидент.

Восстановление

Панель **Исправление** предоставляет вам полезную информацию о том, какие корректирующие действия были предприняты GravityZone автоматически в случае атак, заблокированных такими технологиями, как Advanced Threat Control (ATC), HyperDetect, Antimalware, а также рекомендуемые действия,

которые вы можете выполнить, чтобы смягчить инцидент и повысить уровень безопасности вашей системы.



Панель исправления

1. Действия, выполняемые автоматически GravityZone.

2. Рекомендации по дальнейшему смягчению инцидента и повышению безопасности.

> **Примечание**
> Рекомендуемые шаги соответствуют предупреждениям, обнаруженным на узле, который вызвал расследуемый инцидент.

Примечания

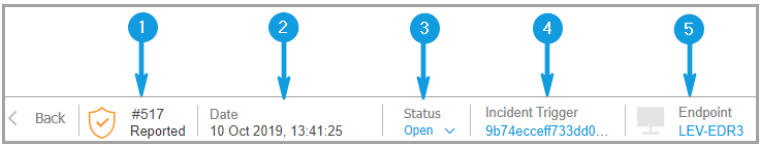
В разделе **Заметки** можно добавить заметку для отслеживания последних изменений и упрощения смены владельца инцидента.

Заметки буфера обмена

1. Чтобы оставить заметку для текущего события, нажмите кнопку **Заметки** , чтобы открыть новое окно.
2. Введите ваше сообщение в этом окне (максимум 2048 символа).

Панель статуса инцидента

Строка статуса инцидента содержит теги событий безопасности, которые могут помочь вам обнаружить ключевую информацию о задействованных конечных точках сети.



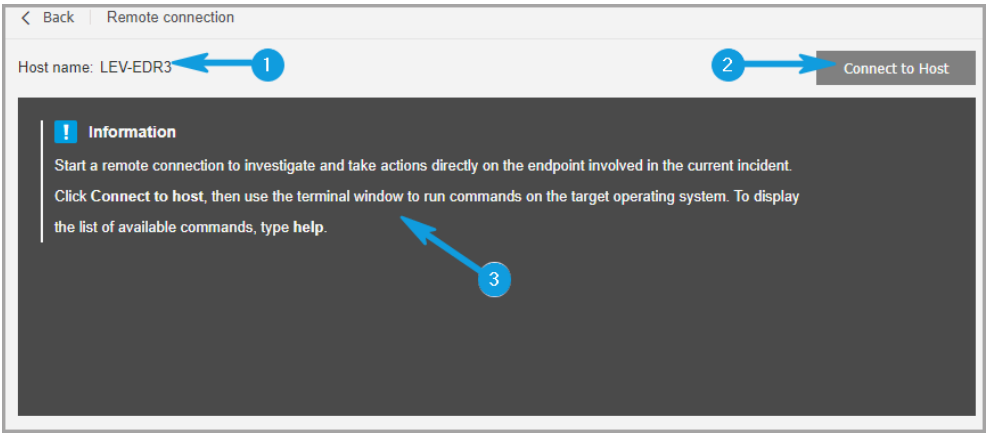
Панель статуса инцидента

1. Идентификатор инцидента - идентификационный номер расследуемого инцидента, только для заблокированного и сообщенного инцидента.
2. Отметка времени обнаружения - дата и время, когда произошел инцидент.
3. Статус инцидента - текущий статус инцидента.
4. Триггер инцидента - имя элемента, который инициировал инцидент.
5. Конечная точка - имя целевой конечной точки.

Нажав кнопку **Назад**, вы вернетесь на главную страницу **Инцидентов** .

Удаленное подключение

Используйте эту вкладку, чтобы установить удаленное соединение с конечной точкой, участвующей в текущем инциденте, и выполнить ряд пользовательских команд оболочки напрямую в своей операционной системе для мгновенной отмены угрозы или сбора данных для дальнейшего расследования.



Вкладка «Удаленное подключение»

На вкладке **Удаленное подключение** содержатся следующие элементы:

1. Имя конечной точки, участвующей в текущем событии безопасности
2. Кнопка управления удаленным подключением (подключить / отключить)
3. Окно терминала

Предварительные условия терминальной сессии

- Версия агента Bitdefender, установленного на конечной точке, поддерживает функцию удаленного подключения.
- Конечная точка должна быть включена и подключена к сети.
- На конечной точке должна быть установлена ОС Windows.
- GravityZone может связываться с конечной точкой.
- Ваша учетная запись GravityZone должна иметь разрешения на управление целевой конечной точкой.

Создание удаленного соединения

Удаленное соединение работает следующим образом:

1. Начните сеанс в реальном времени, нажав кнопку **Подключиться к хосту** .

Состояние соединения будет отображаться рядом с именем конечной точки.

Если соединение не установлено, в окне терминала появится сообщение об ошибке.

Примечание
Вы можете открыть максимум пять терминальных сессий с одной и той же конечной точкой одновременно.

2. После подключения терминал отображает список доступных команд и их описание. Введите нужную команду в окне терминала и нажмите `Enter`.

   Чтобы узнать больше о команде, введите `help`, а затем имя команды (например, `help ps`).

3. Терминал отображает результат команды, когда команда выполнена успешно.

   Если конечной точке не удается завершить выполнение команды, команда будет сброшена.

   История команд записывается в окно терминала. Однако, Вы можете просмотреть ранее введенные команды, нажимая клавиши со стрелками.

4. Чтобы отключиться, нажмите кнопку **Завершить сессию**.

   Сеанс терминала истекает автоматически через пять минут бездействия.

   Навигация за пределами вкладки **Удаленное подключение** при подключении к конечной точке также завершит сеанс терминала.

Команды для сеанса терминала

EDR команды для сеанса терминала - это пользовательские команды, независимые от платформы и использующие общий синтаксис. Здесь и далее приведен список доступных команд, которые Вы можете использовать на конечных точках через сеанс терминала:

- `ps`
  - **Описание**: отображает информацию о состоянии запущенных процессов на выбранной конечной точке, такую как идентификатор процесса (PID), имя, путь или использование памяти.

  - **Синтаксис**: `ps`
  - **Псевдонимы**: `Список задач`
  - **Параметры**: -

- `kill`
  - **Описание**: Завершает работу процесса или приложения на выбранной конечной машине по его PID. Используйте команду `ps/tasklist` для сбора PID,
  - **Синтаксис**: `kill [PID]`
  - **Псевдонимы**: -
  - **Параметры**: `[PID]` - идентификатор процесса на выбранной конечной точке.
- `ls (dir)`
  - **Описание**: Отображает информацию о всех файлах и папках из указанного каталога, такую как имя, тип, размер и дату изменения. Позволяет подстановочным знакам указывать путь. Например:

    `C:\Users\admin\Desktop\s*` все содержимое папки Desktop начиная с "s"

    `C:\Users\publ??` перечисляет все содержимое по указанному пути, с любыми последними двумя буквами.
  - **Синтаксис**: `ls [path]`
  - **Псевдонимы**: `dir`
  - **Параметры**: `[Path]` - путь к файлу или папке на выбранной конечной точке.
- `rm (del, delete)`
  - **Описание**: Удаляет файлы и папки по указанному пути на выбранной конечной точке.
  - **Синтаксис**: `rm [path]`
  - **Псевдонимы**: `del/delete`

- **Параметры**: `[Path]` - путь к файлу или папке на выбранной конечной точке.

- `reg query`
  - **Описание**: отображает всю информацию (имя, тип, значение) указанного пути к ключу реестра.
  - **Синтаксис**: `reg query [keypath] [/k] [keyname] [/v] [valuename]`
  - **Псевдонимы**: -
  - **Параметры**:
    - `keypath`- отображает всю информацию о ключах реестра по указанному пути.
    - `/k [keyname]` - фильтр отображает ключи реестра по указанному имени ключа. Также Вы можете использовать шаблоны (*,?) для фильтрации более широкого диапазона имён.
    - `/v [valuename]` - фильтр отображает значения реестра по указанному имени значения. Также Вы можете использовать подстановочные знаки (*,?) для фильтрации более широкого диапазона имён.

- `reg add`
  - **Описание**: добавляет новый ключ реестра или значение. Перезаписывает значение, если оно уже существует. При перезаписи данных реестра необходимо указать все определенные параметры.
  - **Синтаксис**: `reg add [keyname] [/v] [valuename] [/t] [datatype] [/d] [data]`
  - **Псевдонимы**: -
  - **Параметры**:
    - `[keyname]` - имя ключа реестра.
    - `/v [valuename]` - имя значения реестра. Также требует добавления параметра /d [data]

- `/t [datatype]` - тип данных значения реестра. Вы можете добавить один из следующих типов данных:

  `REG_SZ, REG_MULTI_SZ, REG_DWORD, REG_BINARY, REG_DWORD_LITTLE_ENDIAN, REG_LINK, REG_FULL_RESOURCE_DESCRIPTOR, REG_EXPAND_SZ`

  Если тип не указан явно, то тип `REG_SZ` назначается по умолчанию.

  Если тип установлен как `REG_BINARY`, данные реестра интерпретируются в шестнадцатеричном виде.

- `reg delete`
  - **Описание** : Удаляет ключ реестра или его значения.
  - **Синтаксис**:

    `reg delete [keyname] [/v] [valuename]`

    `reg delete [keyname] [/va]`
  - **Псевдонимы**: -
  - **Параметры**:

    `[keyname]` - удаляет ключ реестра и все его значения.

    `/v [valuename]` - удаляет указанное значение реестра.

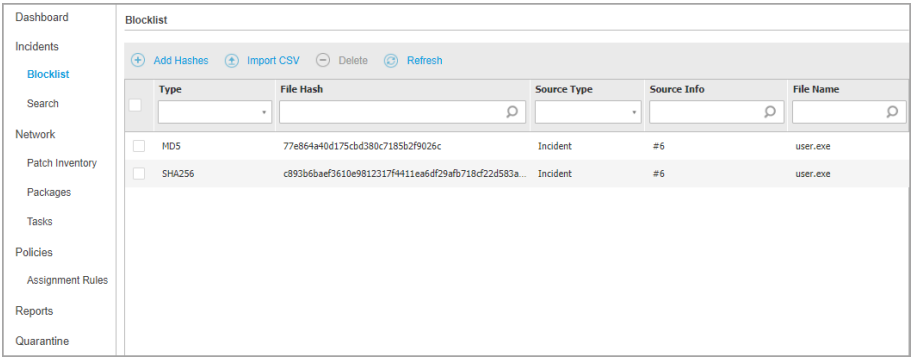
    `/va` - удаляет все значения указанного раздела реестра.
- `cd`
  - **Описание** : Изменяет рабочий каталог согласно указанному пути. Данная команда в качестве параметра требует путь к диску или каталогу на целевой конечной машине
  - **Синтаксис**: `cd [path]`
  - **Псевдонимы**: -
  - **Параметры**: `[Path]` - путь к файлу или папке на выбранной конечной точке.
- `помощь`

- **Описание** : Без указания параметра, в справке перечисляются все доступные команды вместе с кратким описанием. При введении help с параметром, она отобразит полный синтаксис команды, краткое описание и пример использования.
- **Синтаксис**: `help [command]`
- **Псевдонимы**: -
- **Параметры**: имя команды (например: `cd, kill, ls, ps`)

- `clear (cls)`
  - **Описание** : Очищает окно консоли и показывает текущий рабочий каталог.
  - **Синтаксис**: `clear`
  - **Псевдонимы**: `cls`
  - **Параметры**: -

10.2. Занесение в черный список

На странице **Черный список** вы можете просмотреть и управлять компонентами в зависимости от хэш-значения. Просмотрите записи активности в Журнале активности пользователя .



Страница «Черный список»

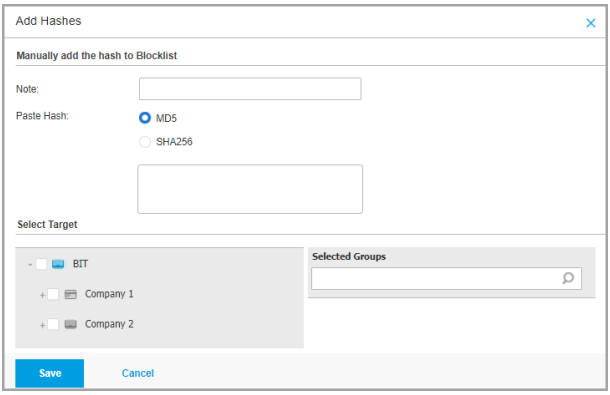
В таблице данных вы можете просмотреть следующие детали для каждого компонента:

- Типы файлов
  - MD5
  - SHA256
- Хэш-значение файлов
- Тип источника:
  - Инцидент
  - Импорт
  - Ручной режим
- Информация об источнике
- Имя файла
- Компания

Добавить хэш-значения к существующему Черному списку:

1. Скопировать хэш-значение из **Информация о файле**.
2. Выберите **MD5** или **SHA256** и вставьте значение в поле ниже.

   Если требуется, добавьте заметку.
3. Нажмите **Сохранить**.



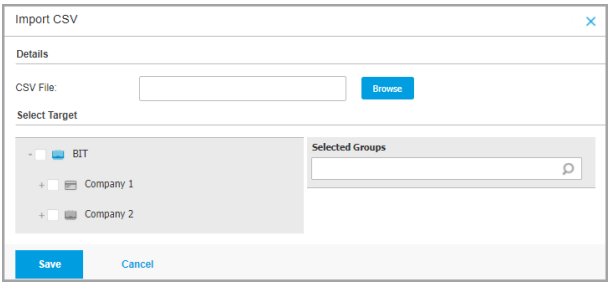
Добавить окно хэш-значения

Важно

Датчик инцидентов заблокирует любой двоичный файл, хеш-значение которого было добавлено в **Черный список**, от запуска процесса.

Импортировать записи хешей в существующий черный список. Чтобы импортировать файл CSV:

1. Нажмите **Импортировать CSV**.
2. Найдите файл CSV и нажмите **Сохранить** .



Окно импорта CSV

Вы также можете импортировать локальные файлы CSV со своего устройства на страницу **Черный список** , но сначала вы должны убедиться, что ваш CSV действителен.

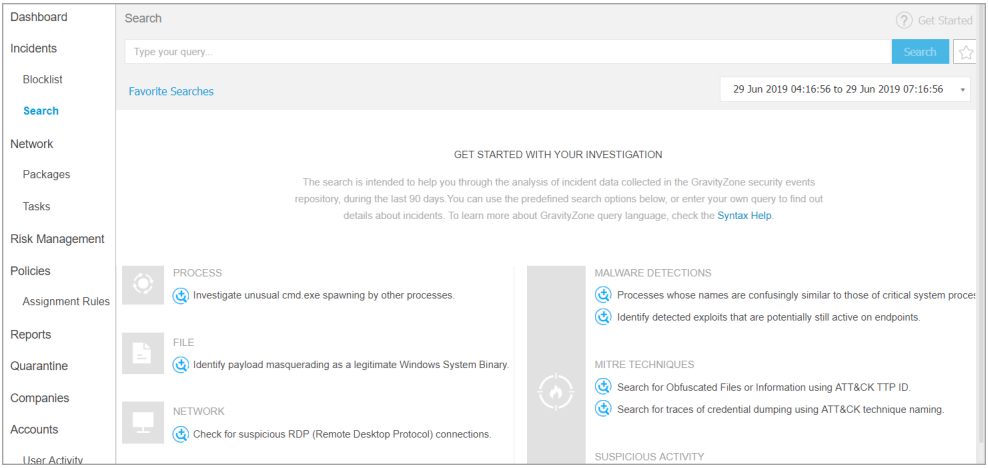
Для создания действительного файла CSV для импорта, вы должны заполнить первые три столбца следующими данными:

1. Первый столбец CSV должен содержать тип хэша: `md5` или `sha256`.
2. Второй столбец должен содержать соответствующие шестнадцатеричные хеш-значения.
3. Третий столбец может содержать необязательную строковую информацию, относящуюся к столбцу **Подробности об источнике** на странице **Черный список**.

Примечание
Информация, соответствующая другим столбцам на странице **Черный список**, будет заполнена автоматически при импорте CSV файла.

10.3. Поиск событий безопасности

Страница **Поиск** позволяет вам просматривать прошлые события на основании сложных критериев.



Обзор страницы поиска

Чтобы просмотреть интересующие вас события, вы должны создавать запросы, используя язык запросов, доступный в GravityZone.

На странице **Поиск** доступны следующие параметры:

- Панель поиска для ввода запросов, отображающая список условий запроса по категориям (при нажатии) и помощник по автозаполнению.
- Сохранение избранных поисков для дальнейшего использования.
- Возможность фильтрации по дате и времени.
- Раздел **Начало работы** со ссылкой на Справку по синтаксису языка запросов.
- Предопределенные запросы, разработанные для полезных случаев поиска событий безопасности.

10.3.1. Язык запросов

Язык запросов предоставляет словарь (поля и операторы) и синтаксис, с помощью которого вы можете создавать запросы. Вы можете найти описание здесь.

Нажмите ссылку **Синтаксис** и выберите вкладку **Язык запросов** , чтобы просмотреть ее содержимое.

Поля

Поле запроса совпадает с полем в базе данных GravityZone. Поля обозначают такие объекты, как пути к файлам, хэши файлов, имена хостов или имена доменов.

Любое поле может иметь одно или несколько значений, представляющих состояние поля в определенный момент времени. Значения относятся к разным типам данных, в зависимости от значения поля.

Операторы

Операторы позволяют создавать отношения между полями для построения критериев поиска. Вы можете пользоваться следующими операторами:

Оператор	Пример	Описание
:	`fieldCategory.option: value1`	Сравнивает значение поля запроса со значениями того же поля в базе данных.

Оператор	Пример	Описание
" "	`fieldCategory.option: "value1 value2"`	Строки, заключенные в кавычки, рассматриваются вместе, как фраза.
( )	`fieldCategory1.option: value1 AND (fieldCategory2.option: value2 OR fieldCategory3.option: value3)`	Условия групповых запросов.
И	`fieldCategory1.option: value1 AND fieldCategory2.option: value2`	Получает результаты, которые соответствуют всем условиям вашего запроса.
или	`fieldCategory1.option: value1 OR fieldCategory2.option: value2`	Получает результаты, которые соответствуют любому из ваших условий запроса.
И НЕ	`fieldCategory1.option: value1 AND NOT fieldCategory2.option: value2`	Этот оператор полезен в сложных запросах и возвращает результаты, не соответствующие указанному термину, за исключением всех других условий.
существует	`_exists_: fieldCategory.option`	Возвращает результаты, содержащие указанное поле.
-	`fieldCategory.option: -value`	Используйте знак минус (-), когда значение должно быть исключено из результатов.
?	`fieldCategory.option: ???_file.path`	Используйте знак вопроса (?), чтобы сопоставить любой отдельный символ в значении вашего поля.

Оператор	Пример	Описание
*	`fieldCategory.option: file.*`	Используйте звездочку (*), чтобы сопоставить любое значение поля.

Синтаксис запроса

Запрос - это логическое условие или последовательность условий, связанных операторами, которые в качестве результатов получают события из базы данных EDR.

Все условия должны относиться к полям. Некоторые условия требуют от вас предоставить значение, а другие нет. Например, вам не нужно значение, когда вы спрашиваете, существует ли поле в деталях события.

Запросы могут быть от простых до сложных. Сложные запросы могут иметь вложенные запросы (запрос в другом запросе).

Допустимый синтаксис поля состоит из категории поля, за которой следует один из параметров в разделе **Яык запросов**, и его соответствующее значение: `fieldCategory.option: value`.

Например, `file.path: "%system32%\com\svchost.exe"` - это довольно простой запрос, который ищет все события, включающие `%system32%\com\svchost.exe` и состоит из:

- Обязательная категория поля и связанный параметр (разделенные точкой): `file.path`
- Оператор: двоеточие (:) - для сравнения значения поля
- Найденное значение: `%system32%\com\svchost.exe`
- Кавычки (" "), так как значение содержит специальные символы, такие как <\> and <.>

10.3.2. Запуск запросов

Чтобы выполнить запрос:

1. Введите строку запроса в поле.

Если нажать на поле **Поиск**, отобразится список поисковых запросов, сгруппированных по категориям. Выберите фразу, с который вы хотите начать создавать запрос.

По мере ввода, Control Center помогает вам с предложениями автозаполнения. С помощью клавиш со стрелками выберите предложенный вариант, а затем нажмите **Enter** , чтобы добавить его в запрос.

Если нужна помощь, нажмите ссылку **Помощь с синтаксисом**.

Примечание
Вы можете использовать вложенные запросы для создания сложных поисков.

2. Чтобы отфильтровать события за определенный промежуток времени, нажмите на поле со временем.

   Важно
   Интервал хранения данных по умолчанию для событий составляет 7 дней. Если Вы хотите увеличить мощность, Вам необходимо обратиться к своему торговому представителю, чтобы обновить свое решение с помощью 30 -, 90- или 180-дневного **хранения данных**).

   Вы обладаете несколькими опциями для определения времени, затрачиваемого на поиск:

   - Только определенная дата

     Выберите дату во вкладке календаря **Из**.
   - Точный временной интервал.

     a. Выберите начальную дату во вкладке календаря **Из**.

     b. Выберите конечную дату во вкладке **В**.
   - Последний временной интервал из доступных опций.
   - Нажмите **ОК**.
3. Нажмите **Поиск** или нажмите **Enter**.

   Вы можете просмотреть соответствующие события вместе с их деталями под вашим запросом.

Важно

При поиске запроса `detections.detection_type` в поле *Поиск* Control Center требует, чтобы вы завершили его с помощью целочисленного значения в диапазоне от 1 до 15 (т.е. `detections.detection_type:1`). Каждое введенное вами значение соответствует определенному типу обнаружения следующим образом:

a. `detections.detection_type:1` - Advanced Threat Control detection
b. `detections.detection_type:2` - обнаружение антивирусных программ статическим ядром
c. `detections.detection_type:3` - обнаружение HyperDetect
d. `detections.detection_type:4` - уведомление Advanced Threat Control о подозрительном событии
e. `detections.detection_type:5` - сообщенное обнаружение типов атак от HyperDetect
f. `detections.detection_type:6` - обнаружение антивирусным сканером CMDLine
g. `detections.detection_type:7` - обнаружение Cross Technologies Correlation
h. `detections.detection_name:8` - обнаружение Network Attack Defense
i. `detections.detection_type:9` - несообщенное обнаружение типов атак от HyperDetect
j. `detections.detection_type:10` - обнаружение ограниченного динамического анализа от Sandbox Analyzer
k. `detections.detection_type:11` - обнаружение сканирования регистра буфера памяти
l. `detections.detection_type:12` - обнаружение URL
m. `detections.detection_type:13` - расширенное обнаружение защиты от эксплойтов
n. `detections.detection_type:14` - обнаружение анализа поведения пользователя
o. `detections.detection_type:15` - обнаружение интерфейса сканирования вредоносных программ

p. `detections.detection_type:16` - обнаружения Cross-Technologies Correlation основаны на машинном обучении.

Control Center отображает до 10,000 событий. Если результаты запроса содержат больше 10,000 событий, на экране появится сообщение. В этом случае необходимо уточнить запрос.

10.3.3. Избранные поиски

Поскольку большинство запросов длинные, некоторые даже сложно построить или запомнить. Вместо того, чтобы сохранять их в файл и копировать в GravityZone, вы можете сохранить их непосредственно в GravityZone, чтобы иметь под рукой всякий раз, когда их необходимо использовать.

Чтобы сохранить ваш запрос:

1. Введите строку в поле **Поиск**.
2. Нажмите на значок ☆ справа от поля **Поиск**.
3. Когда будет предложено назвать его, введите имя, которое вы хотите для вашего запроса.
4. Нажмите **Добавить**.

Нажмите ссылку **Закладки** в поле **Запрос**, чтобы просмотреть ваши сохраненные запросы.

Затем у вас есть три опции:

- Выполнить запрос.
- Редактировать имя запроса.
- Удалить запрос.

Чтобы выполнить сохраненный запрос:

1. Нажмите ссылку **Закладки**.
2. Выберите предпочтительный запрос.

   Сохраненная строка будет добавлена в поле **Поиск**.

> **Примечание**
> Если необходимо, редактируйте строку запроса. Дополнительно вы можете сохранить новый поисковой запрос в закладках.

3. Используйте фильтры компании и календаря, чтобы улучшить поиск.
4. Нажмите **Поиск**.

Когда ваш список запросов нуждается в корректировке, наведите курсор мыши на сохраненный запрос, чтобы отобразить встроенные параметры.

- Нажмите значок **Изменить**, чтобы переименовать запрос.
- Нажмите значок **Удалить**, если вам более не нужен запрос.

10.3.4. Предопределенные запросы

Страница **Поиск** содержит несколько примеров сложных запросов, относящихся к расследованиям событий безопасности.

Предопределенные запросы сгруппированы по категориям расследования безопасности.

Чтобы запустить предопределенный запрос:

- Нажмите значок рядом с описанием предопределенного запроса.
- Фраза запроса автоматически появится на панели **Поиск**. Заполните конкретные детали для условий запроса.
- Нажмите кнопку **Поиск**, чтобы выполнить запрос.

Примечание
Вы можете в любое время вернуться к параметрам **Начало работы** со страницы **Поиск**, нажав ссылку **Начало работы** в правом верхнем углу страницы.

10.4. Правила потребителя

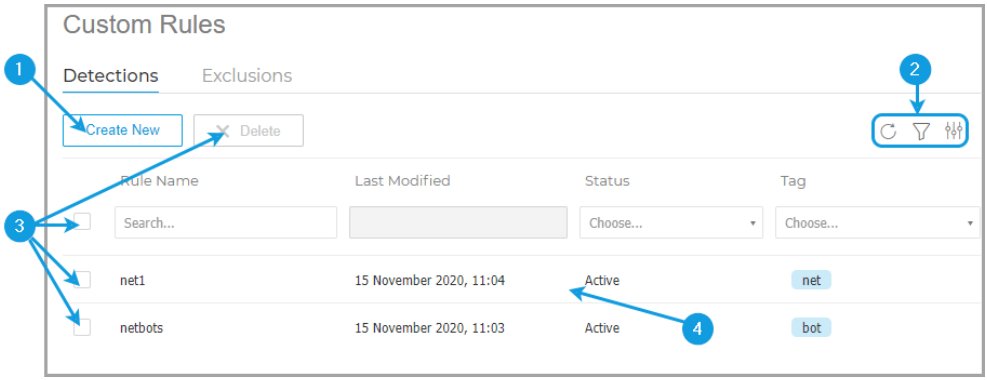
Страница **Пользовательские правила** предоставляет Вам платформу для создания и управления пользовательскими правилами, включающими или исключающими определенные типы поведения из инициирующих инцидентов.

Данная EDR функция включает в себя две основные категории:

- Обнаружения
- Исключения

10.4.1. Обнаружения

На **Обнаружения** вкладке представлена платформа для создания и управления пользовательскими правилами обнаружения. Это предоставляет возможность обозначения определенного поведения в Вашей среде, и отображает соответствующие инциденты на странице Инциденты.



Вкладка обнаружений

1. Нажмите на **Выбрать новое** кнопку для создания нового пользовательского правила обнаружения. Смотрите Создать пользовательские правила исключения раздел для получения более подробной информации.
2. Используйте эти кнопки действий для настройки вашей сетки:
   - Нажмите кнопку **Показать/скрыть столбцы**, чтобы добавить или убрать столбцы фильтра.

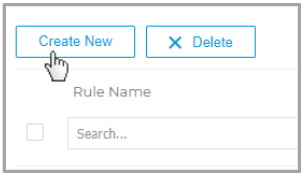
     Страница обновится автоматически, загрузив карточки с информацией, соответствующей добавленным столбцам.

     Вы всегда можете сбросить столбцы фильтра с помощью кнопки **Сбросить** внутри выпадающего меню **Показать/скрыть столбцы**.
   - Нажмите кнопку **Показать/скрыть фильтры**, чтобы отобразить или скрыть панель фильтров.
   - Нажмите кнопку **Обновить**, чтобы обновить список.

3. Установите флажок глобальной проверки или отдельных полей правил, чтобы выбрать их, и нажмите кнопку **Удалить** для удаления их из списка.
4. Нажмите на правило в списке, чтобы развернуть его панель сведений, просмотреть сведения о правиле и при необходимости обновить или удалить его. Смотрите Панель деталей правил исключения для получения более подробной информации.

Создание пользовательского правила исключения:

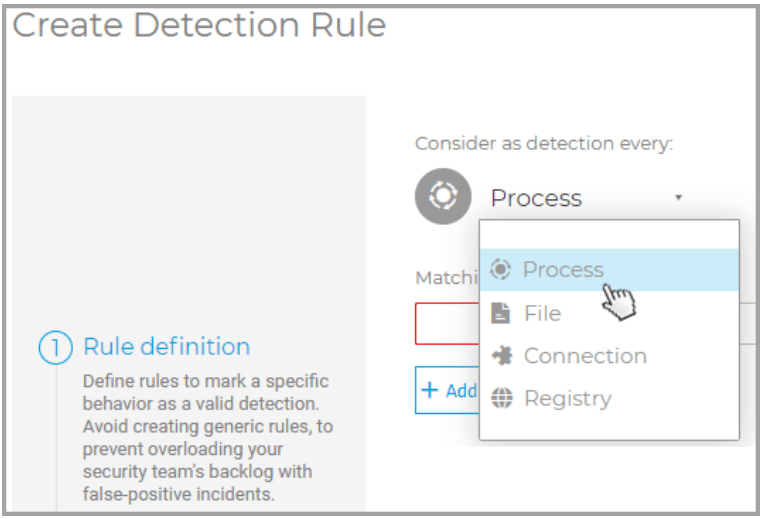
Чтобы создать пользовательское правило обнаружения, нажмите на кнопку **Создать новое**.



Создайте новое правило обнаружения

Он приведет Вас на страницу **Создать правило исключения** в разделе **Определение правила**, где Вы можете начать редактирование правила:

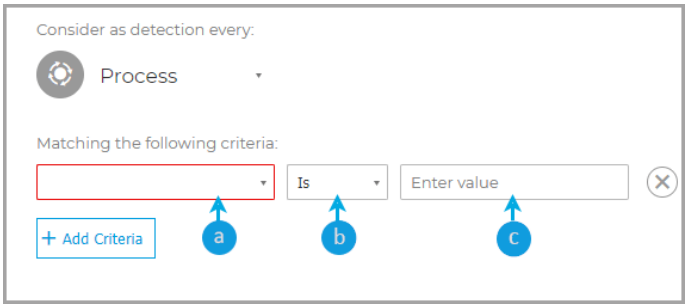
1. Выберете тип элемента, который Вы хотите внести в правило обнаружения.



Вы можете выбрать из:

- Процесс
- Файл
- Подключение
- Реестр

2. Каждый тип элемента имеет определенные критерии соответствия, которые Вы можете выбрать из выпадающего меню:



a. Выберите один из доступных параметров:

b. Выберите тип связи между критерием соответствия и его значением:

- **Is** - исключит все инциденты с элементами, которые соответствуют точному значению, введенному в поле значений.
- **Слдержит** - включит в себя все инциденты с элементами, содержащими значение, введенное в поле значений(например, подстановочные знаки, расширения файлов и пр.).

  Важно
  Использование подстановочных знаков при создании правила обнаружения повышает риск того, что оно станет общедоступным, а это увеличит вероятность переполнения Вашего рабочего бэклога ложными инцидентами.

- **Один из** - включает в себя все инциденты с элементами, соответствующими одному из значений, введенных в поле значений (оператор **или** применяется между введенными значениями).

c. Задайте конкретную величину для каждого критерия.

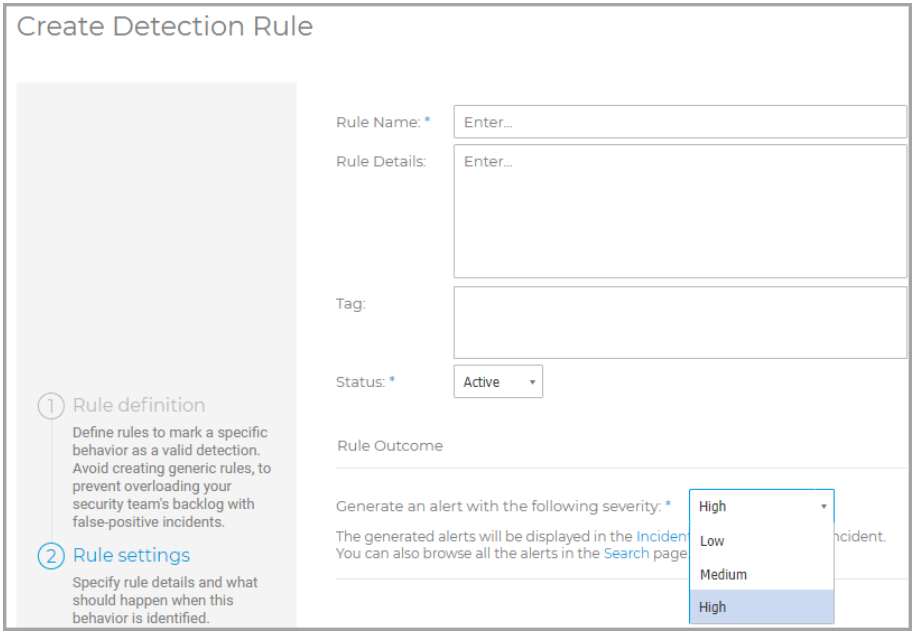
Примечание
При вводе нескольких значений для критерия (при использовании **является одним из условий**) необходимо нажиматьВводпосле каждого значения для завершения действия.

3. Выберете **Добавить параметр** чтобы добавить новый критерий для правила.

Примечание
Правило будет запускать инциденты, имеющие каждый критерий (оператор **и** применяется между несколькими добавленными критериями).

4. После определения всех критерий нажмите **Следующий шаг**.

   Он приведет Вас в раздел **Настройки правила**, где Вы должны заполнить сведения о правиле.



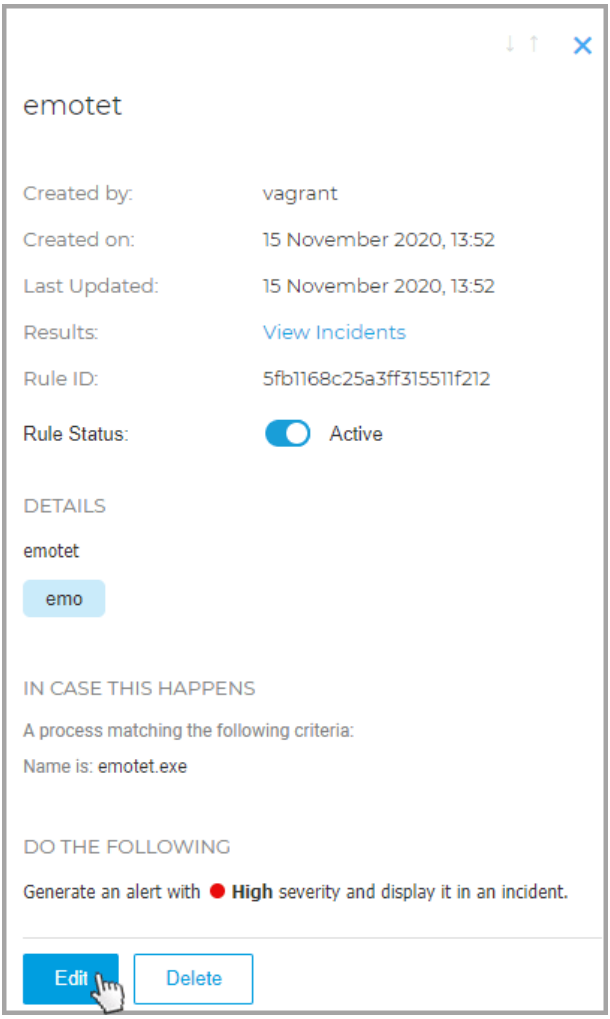
5. Введите название правила В **Название правила** поле. Это поле является обязательным для заполнения.
6. Введите краткое описание правила в **Особенности правила** поле.
7. Добавьте теги, относящиеся к этому правилу, в поле **Теги**, чтобы упростить ряд правил и управление ими.
8. Задайте активный или пассивный статус правила в раскрывающемся меню **Status**.

9. Установите уровень предупреждений, вызванных этим правилом: низкий / средний / высокий в раскрывающемся меню.
10. Нажмите на **Создать правило**, чтобы завершить создание пользовательского правила исключения.

    Новое правило доступно во **Обнаружения** вкладке.

Панель деталей правил исключения

Панель **Сведения о правиле** содержит подробную информацию о выбранном правиле, включая дату создания и автора, дату последнего обновления, уникальный идентификатор и статус, а также ссылку на список событий, соответствующих критериям правила. Он также включает в себя описание правила, связанные теги, включенные критерии соответствия и результат.

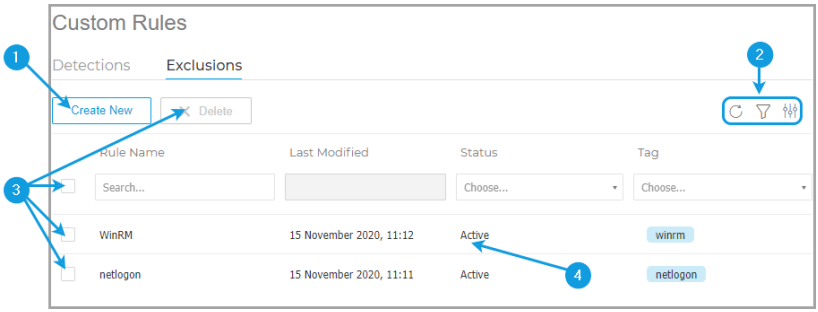


Панель сведений о правиле

- Нажмите на кнопку **Изменить**, чтобы перейти на страницу **Создать правило обнаружения**, где можно обновить определение правила.
- Нажмите **Удалить**, чтобы удалить правило исключения из списка.

10.4.2. Исключения

Страница **Исключения** демонстрирует Вам платформу для создания и управления пользовательскими правилами исключения, чтобы устранять инциденты, которые Вы считаете неуместными для Вашей организации. В противном случае они были бы помечены EDR на странице Инциденты.



Вкладка исключения

1. Нажмите на **Выбрать новое** кнопку для создания нового пользовательского правила исключения. Смотрите Создать пользовательские правила исключения раздел для получения более подробной информации.

   Кроме того, Вы всегда можете создать правило прямо из графика инцидентов, выбрав целевой узел и добавив его в качестве исключения из боковой панели сведений. Смотрите Добавить как исключение EDR функциональность для получения более подробной информации.

2. Используйте эти кнопки действий для настройки вашей сетки:

   - Нажмите кнопку **Показать/скрыть столбцы**, чтобы добавить или убрать столбцы фильтра.

     Страница обновится автоматически, загрузив карточки с информацией, соответствующей добавленным столбцам.

     Вы всегда можете сбросить столбцы фильтра с помощью кнопки **Сбросить** внутри выпадающего меню **Показать/скрыть столбцы**.

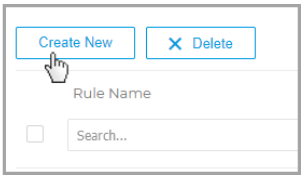
   - Нажмите кнопку **Показать/скрыть фильтры**, чтобы отобразить или скрыть панель фильтров.

- Нажмите кнопку **Обновить**, чтобы обновить список.

3. Установите флажок глобальной проверки или отдельных полей правил, чтобы выбрать их, и нажмите кнопку **Удалить** для удаления их из списка.
4. Нажмите на правило в списке, чтобы развернуть его панель сведений, просмотреть сведения о правиле и при необходимости обновить или удалить его. Смотрите Панель деталей правил исключения для получения более подробной информации.

Создание пользовательского правила исключения:

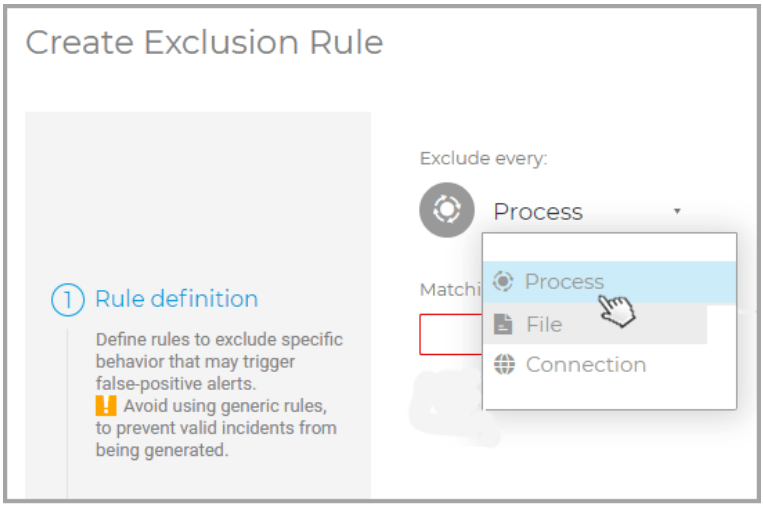
Чтобы создать пользовательское правило исключения, нажмите кнопку **Новое** на странице **Исключения**.



Создать новое правило исключения

Он приведет Вас на страницу **Создать правило исключения** в разделе **Определение правила**, где вы можете начать редактирование правила:

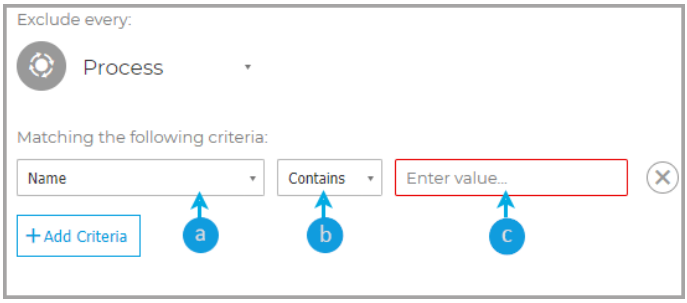
1. Выберете тип элемента, который Вы хотите внести в правило исключения.



Вы можете выбрать из:

- Процесс
- Файл
- Подключение

2. Каждый тип элемента имеет определенные критерии соответствия, которые Вы можете выбрать из выпадающего меню:



a. Выберите один из доступных параметров:

b. Выберите тип связи между критерием соответствия и его значением:

- **Is** - исключит все инциденты с элементами, которые соответствуют точному значению, введенному в поле значений.
- **Слдержит** - исключит все инциденты с элементами, содержащими значение, введенное в поле значений(например, подстановочные знаки, расширения файлов и пр.).

  Важно
  Использование подстановочных знаков при создании правила исключения повышает риск сделать его слишком доступным, что увеличивает вероятность игнорирования реальных угроз и делает Вашу компанию более уязвимой.

- **Is one of** - исключит все инциденты с элементами, соответствующими одному из значений, введенных в поле значений (оператор **или** применяется между введенными значениями).

c. Задайте конкретную величину для каждого критерия.

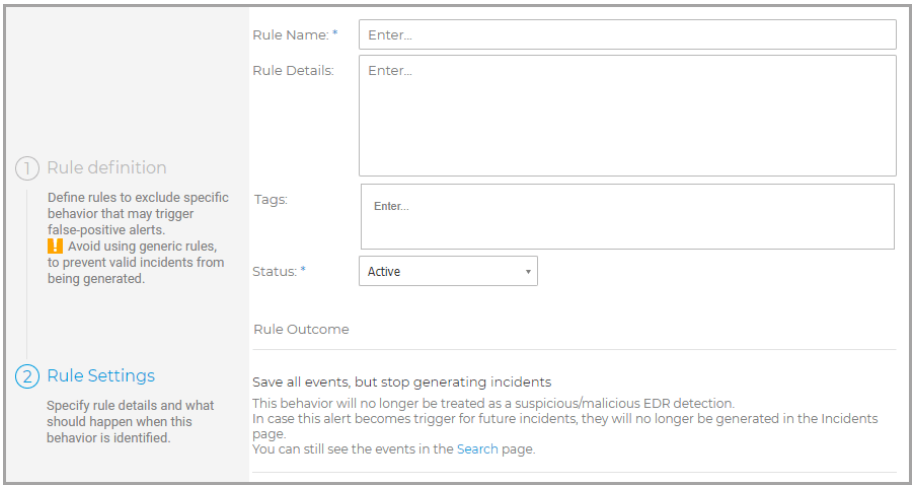
Примечание
При вводе нескольких значений для критерия (при использовании **является одним из условий**) необходимо нажиматьВводпосле каждого значения для завершения действия.

3. Выберете **Добавить параметр** чтобы добавить новый критерий для правила.

Примечание
Правило будет исключать инциденты, имеющие каждый критерий (оператор **и** применяется между несколькими добавленными критериями).

4. После определения всех критерий нажмите **Следующий шаг**.

   Он приведет Вас в раздел **Настройки правила**, где Вы должны заполнить сведения о правиле.

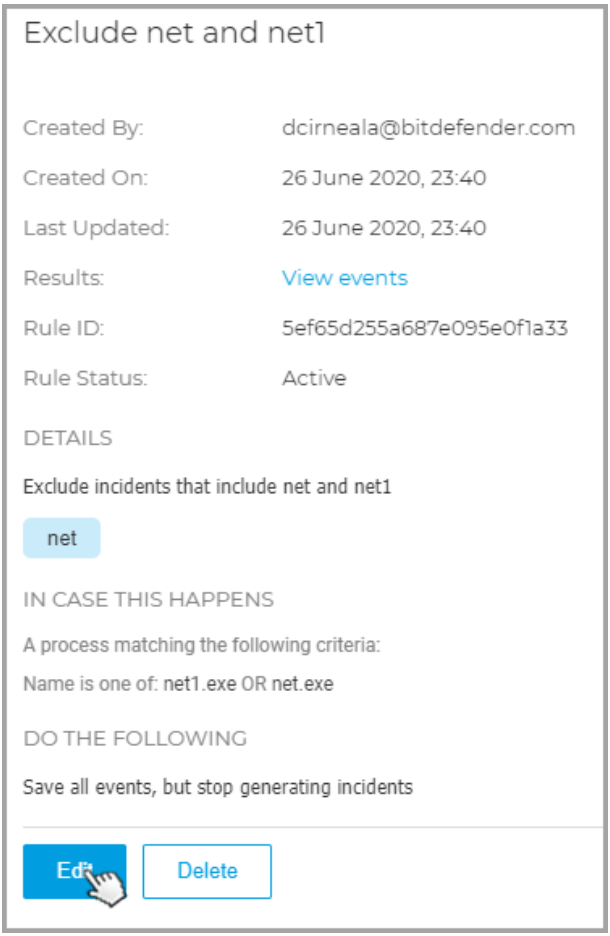


5. Введите название правила В **Название правила** поле. Это поле является обязательным для заполнения.
6. Введите краткое описание правила в **Особенности правила** поле.
7. Добавьте теги, относящиеся к этому правилу, в поле **Теги**, чтобы упростить ряд правил и управление ими.
8. Задайте активный или пассивный статус правила в раскрывающемся меню *Status*.
9. Нажмите на **Создать правило**, чтобы завершить создание пользовательского правила исключения.

   Новое правило доступно во **Обнаружения** вкладке.

Панель деталей правил исключения

Панель **Сведения о правиле** содержит подробную информацию о выбранном правиле, включая дату создания и автора, дату последнего обновления, уникальный идентификатор и статус, а также ссылку на список событий, соответствующих критериям правила. Он также включает в себя описание правила, связанные теги, включенные критерии соответствия и результат.



Панель сведений о правиле

- Нажмите на кнопку **Изменить**, чтобы перейти на страницу **Создать правило исключения**, где можно обновить определение правила.
- Нажмите **Удалить**, чтобы удалить правило исключения из списка.

11. УПРАВЛЕНИЕ РИСКАМИ КОНЕЧНОЙ ТОЧКИ

Управление Рисками Конечной Точки (ERA) помогает оценивать и укреплять конфигурации безопасности конечных точек в соответствии с лучшими отраслевыми практиками, чтобы минимизировать поверхность атаки.

Важно
Модуль Управление рисками конечной точки доступен только для операционных систем Windows для настольных компьютеров и серверов.

ERA собирает и анализирует данные с помощью задач сканирования рисков, выполняемых на выбранных устройствах в вашей сети.

Для этого сначала необходимо убедиться, что модуль ERA активирован из политики, применяемой к выбранным устройствам:

1. Перейдите на страницу **Политики**.
2. Нажмите кнопку **Добавить** и настройте параметры **Общие**.
3. Прокрутите и выберите политику **Управления рисками**.
4. Установите флажок, чтобы включить функции **Управление рисками** и начать настройку политик, определяющих, как запускать задачу **Сканирование рисков**.

Примечание
Для получения дополнительной информации об индикаторах риска GravityZone см. эту статью Базы Знаний.
Дополнительную информацию об известных уязвимостях приложений смотрите на веб-сайте Подробности CVE.

Выполните следующие действия для запуска задач сканирования рисков и оценки результатов:

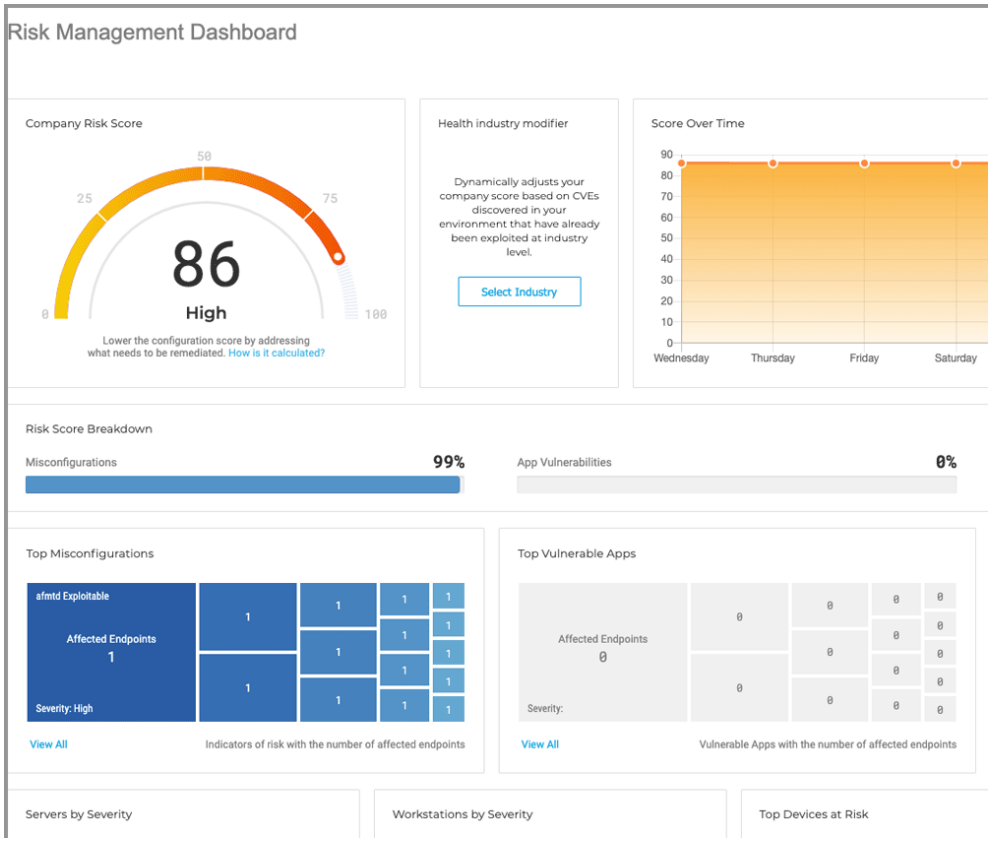
1. Задачи сканирования рисков на конечных точках могут быть запущены двумя способами:
   a. По запросу - выбрав конечные точки на странице **Сеть** и отправив задачу **Сканирование рисков** из меню **Задачи**.
   b. По расписанию, настроив в политике задачу сканирования рисков, которая будет автоматически запускаться на целевых машинах с установленным интервалом времени.

После успешного завершения сканирования рисков, GravityZone рассчитывает оценку риска для каждой конечной точки..

2. Перейдите в панель **Управления рисками** для получения следующей информации:
   - Оценка риска компании и эволюция оценки
   - Оценки риска и статистика разбиты на ошибки в конфигурации, уязвимые приложения, человеческие риски и затронутые устройства
   - Описание каждого показателя риска и рекомендуемые корректирующие действия
3. Откройте страницу Риски безопасности, чтобы проанализировать и устранить обнаруженные ошибки конфигурации и уязвимости приложений, а также потенциальные риски, вызванные поведением пользователя.

11.1. Панель Управления Рисками

Страница **Управления рисками** предоставляет обзор безопасности вашей сети и информацию оценки рисков.



Панель управления рисками

1. Общая оценка риска
2. Модификатор индустрии здравоохранения
3. Оценка с течением времени
4. Главные ошибки конфигурации
5. Основные уязвимости приложения
6. Высшие человеческие риски
7. Соотношение количества серверов и степени опасности

8. Серверы по уровню опасности
9. Основные устройства под угрозой
10. Лучшие пользователи в области соблюдения безопасности

Данные, отображаемые на этой странице, организованы в несколько виджетов:

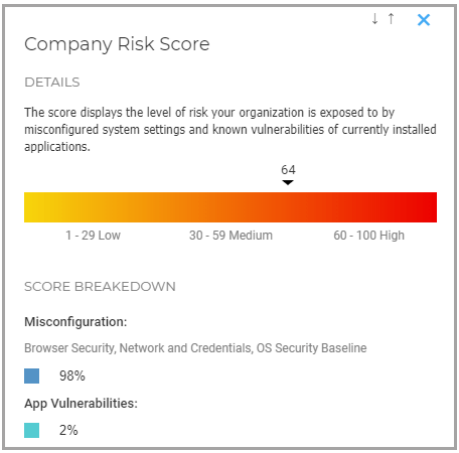
Общая оценка риска

Общая оценка риска отображает его уровень, которому подвергается Ваша организация из-за некорректно настроенных параметров системы и известных уязвимостей, установленных в настоящее время приложений, а также из-за рисков, вызванных поведением или активностью пользователей. Оценка корректируется при помощи Health Industry Modifier, который вычисляет риск, вызванный использованием несовместимых с Вашей системой приложений.

Оценка отображает средний показатель из трех основных категорий риска: **Ошибки конфигурации** и **Уязвимость приложений**, а также **Человеческие риски**

Виджет оценки рисков компании

Нажмите на виджет, и откроется панель сведений, где вы сможете увидеть детали того, как общий риск рассчитывается и разбивается на подкатегории.

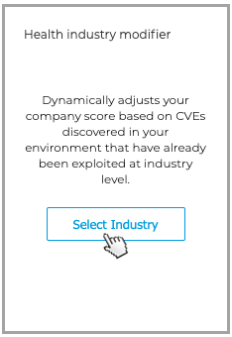


Панель сведений о рисках компании

Примечание
Выполнение Сканирования рисков по требованию на новом целевом устройстве повлияет на общий балл. Результаты будут храниться в течение 90 дней или до следующего сканирования.

Модификатор индустрии здравоохранения

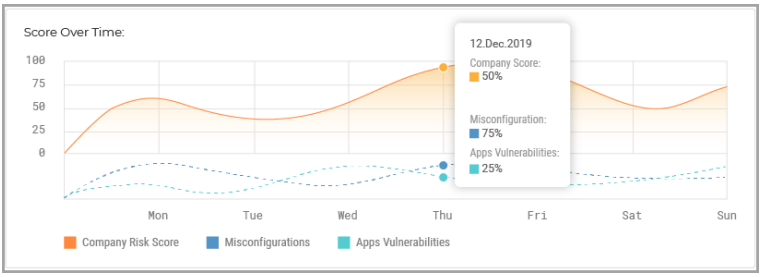
Модификатор отрасли здравоохранения динамически корректирует оценку компании на основе общих уязвимостей и рисков (CVE), обнаруженных в Вашей среде, которые уже использовались на отраслевом уровне.



Модификатор индустрии здравоохранения

Оценка с течением времени

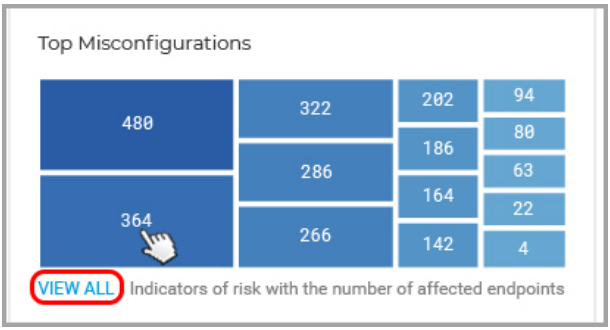
Этот виджет представляет собой гистограмму, которая отображает еженедельное изменение количества затронутых устройств, определенных как уязвимые после сканирования рисков. Данные гистограммы отражают количество устройств, на которые влияют индикаторы риска за последние семь дней, до 12:00 (время сервера) текущего дня.



Виджет Оценки во времени

Главные ошибки конфигурации

Этот виджет отображает 15 лучших результатов для индикаторов, которые вызвали предупреждение о риске после сканирования устройств, упорядоченных по количеству затронутых устройств. Каждая карта представляет собой один индикатор, который вызвал предупреждение о риске как минимум для одного устройства.



Виджет главных ошибок конфигурации

Каждая карта отображает следующие элементы:

- Название индикатора.
- Количество устройств, обнаруженных как уязвимые этим индикатором.
- Уровень серьезности проблем конфигурации.

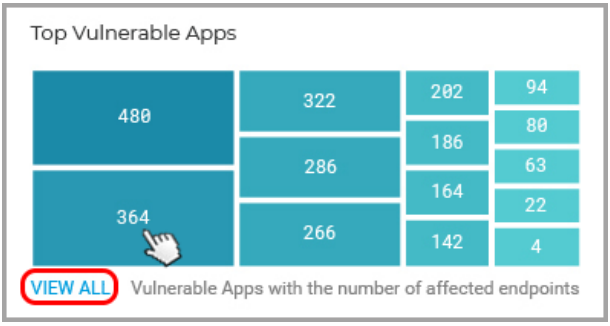
Если Вы нажмете на виджет индивидуального индикатора, он откроет выбранный индикатор риска во вкладке Неверные настройкистраницы **Риски безопасности** , где Вы можете предпринять соответствующие действия для снижения этого риска.

Если вы нажмете кнопку **Просмотреть все**, вы увидите весь список обнаруженных ошибок конфигурации на вкладке Ошибки конфигурации на странице **Риски безопасности**.

Примечание
Для получения более подробной информации о некорректной настройке обратитесь к Этой статье KB.

Основные уязвимости приложения

Этот виджет представляет 15 лучших результатов для известных уязвимостей приложений, которые вызвали предупреждение о риске после сканирования устройств, упорядоченных по количеству затронутых устройств. Каждая карта представляет собой одно уязвимое приложение, который вызвало предупреждение о риске как минимум для одного устройства.



Виджет самых уязвимых приложений

Каждая карта отображает следующие элементы:

- Имя приложения
- Количество устройств ставшими уязвимыми из-за этого приложения.
- Серьезность для уязвимых приложений

Если Вы нажмете на виджет приложения, он откроет выбранную уязвимость во вкладке Уязвимости приложениястраницы **Риски безопасности** , где Вы можете предпринять соответствующие действия для снижения этого риска.

При нажатии кнопки **Просмотреть все**, вы увидите весь список обнаруженных уязвимостей приложений на вкладке Уязвимости приложений на странице **Риски безопасности** .

Примечание
Вы можете найти подробности об известных уязвимостях приложений на веб-сайте Подробности CVE.

Основные риски, связанные с поведением пользователей

Этот виджет отображает топ-15 результатов по потенциальным рискам, вызванным непреднамеренным или опрометчивым поведением активных пользователей в Вашей сети, упорядоченных по количеству уязвимых пользователей. Каждая карта подвергается человеческому риску со стороны хотя бы одного пользователя.

Виджет основных рисков, связанных с поведением пользователей

Каждая карта отображает следующие элементы:

- Название человеческих рисков.

- Число пользователей, чье опрометчивое или непреднамеренное поведение может подвергнуть опасности Вашу организацию.
- Степень серьезности для человеческих рисков.

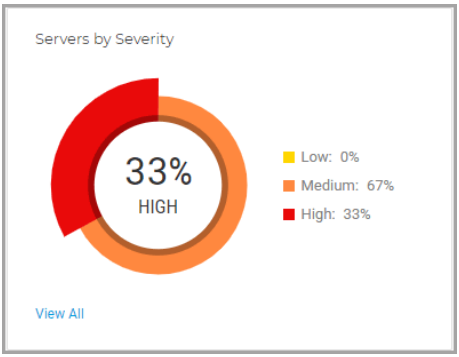
Если Вы нажмете на виджет индивидуального человеческого риска, он откроет выбранный риск во вкладке Человеческие риски страницы **Риски безопасности**, где Вы можете просмотреть и проанализировать его более подробно

Если вы нажмете кнопку **Просмотреть все**, вы увидите полный список обнаруженных человеческих рисков, полученных в связи с активностью пользователя, на вкладке Человеческие риски на странице **Риски безопасности**.

Примечание
Эта новая функция ERA доступна в виде предварительной версии, позволяет Вам только просматривать человеческие риски и игнорировать их, если они не имеют отношения к Вашей среде. В ближайшем будущем будет добавлена расширенна функциональность.

Соотношение количества серверов и степени опасности

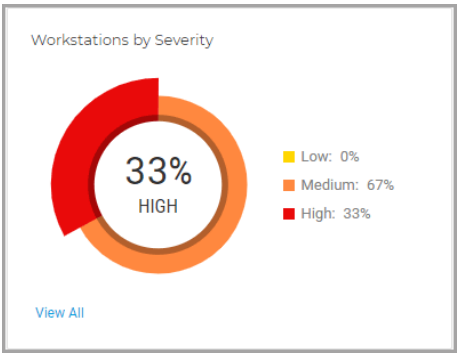
Этот виджет показывает серьезность рисков, угрожающих серверам в вашей среде. Воздействие обнаруженных ошибок конфигурации и уязвимостей приложений отображается в процентах.



Виджетов серверов по серьезности

Серверы по уровню опасности

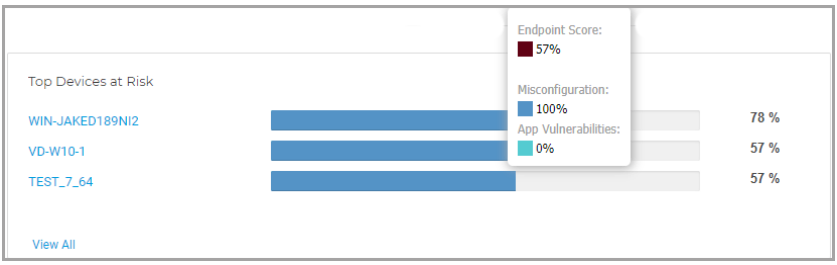
Этот виджет показывает серьезность рисков, угрожающих рабочим станциям в вашей среде. Воздействие обнаруженных ошибок конфигурации и уязвимостей приложений отображается в процентах.



Виджет рабочих станций по серьезности

Основные устройства под угрозой

Этот виджет отображает наиболее уязвимые серверы и рабочие станции в вашей среде в соответствии с общим баллом, рассчитанным после сканирования на ошибки конфигурации и уязвимости.

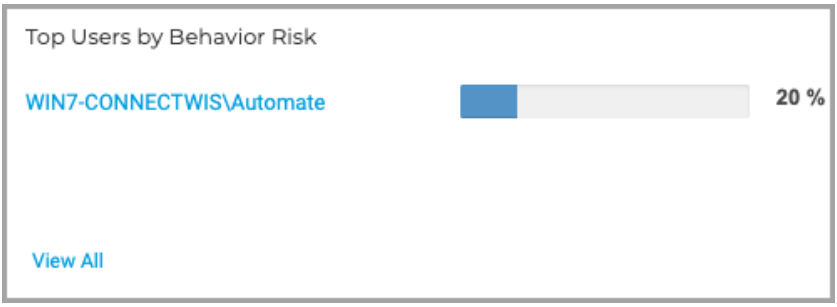


Виджет топ устройств в опасности

Если Вы нажмете на кнопку **Видеть все**, то увидите весь список устройств, подверженных потенциальным угрозам, во вкладке Устройства страницы **Риски безопасности**.

Основные риски, связанные с поведением пользователей

Этот виджет отображает наиболее уязвимых пользователей в вашей среде в соответствии с общим баллом, полученном в результате анализа их поведения и активности.

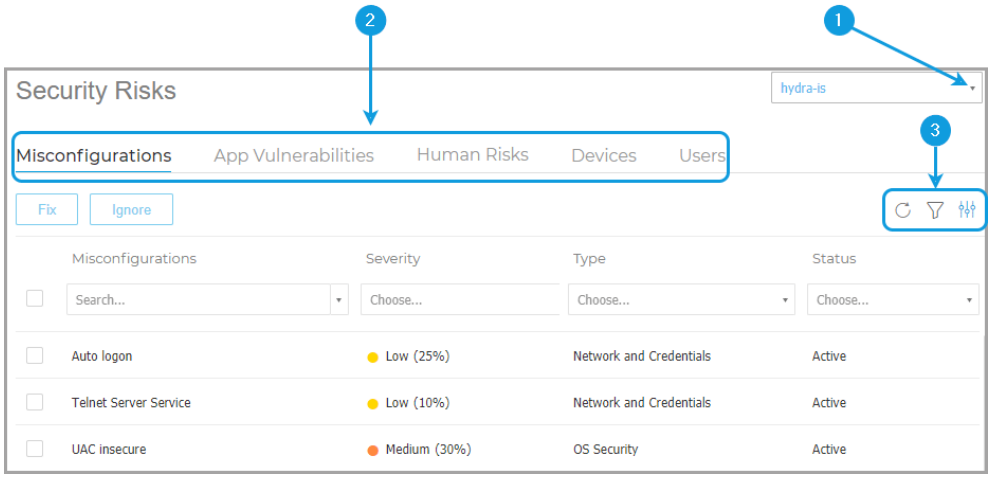


Виджет самых уязвимых приложений

Если Вы нажмете кнопку **Видеть все**, то увидите весь список пользователей, которые своим поведением могли подвергнуть Вашу организацию потенциальным угрозам, на вкладке Пользователи страницы **Риски безопасности**.

11.2. Риски безопасности

На этой странице отображаются все риски и затронутые устройства, а также уязвимые пользователи, обнаруженные в Вашей среде после выполнения задачи **Сканирование рисков**.



Страница Рисков безопасности

Индикаторы риска отображаются в полностью настраиваемой сетке со сложными параметрами фильтрации:

1. Выберите компанию под вашим руководством для анализа и снижения рисков, влияющих на нее.
2. Выберите категорию для расследования:
   - Ошибки в конфигурации
   - Уязвимости приложения
   - Человеческие риски
   - Устройства
   - Пользователи
3. Используйте эти кнопки действий для настройки вашей сетки:
   - Нажмите кнопку **Показать/скрыть столбцы**, чтобы добавить или убрать столбцы фильтра.

     Страница обновится автоматически, загрузив карточки индикаторов риска с информацией, соответствующей добавленным столбцам.

Вы всегда можете сбросить столбцы фильтра с помощью кнопки **Сбросить** внутри выпадающего меню **Показать/скрыть столбцы**.

- Нажмите кнопку **Показать/скрыть фильтры**, чтобы отобразить или скрыть панель фильтров.
- Нажмите кнопку **Обновить**, чтобы обновить список.

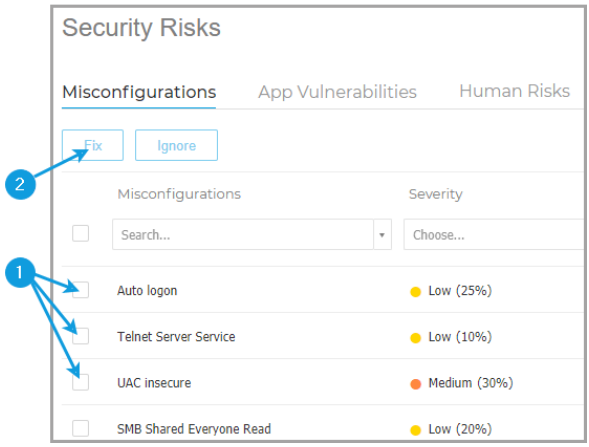
Каждая запись индикатора отображается в расширенном формате карты, предоставляя обзор каждого инцидента с информацией, основанной на выбранных фильтрах.

Ошибки в конфигурации

Вкладка **Неправильная настройка**отображает по умолчанию GravityZonevсе индикаторы риска. Он предоставляет подробную информацию об их серьезности, количестве затронутых устройств, типе ошибки конфигурации, типе смягчения (вручную или автоматически) и статусе (активен или игнорируется).

Исправить многочисленные проблемы конфигурации сразу же:

1. Установите общий флажок или отдельные флажки индикаторов риска, чтобы выбрать их.



Исправьте многочисленные риски во вкладке проблем конфигурации

2. Нажмите на **Исправить риски** кнопку.

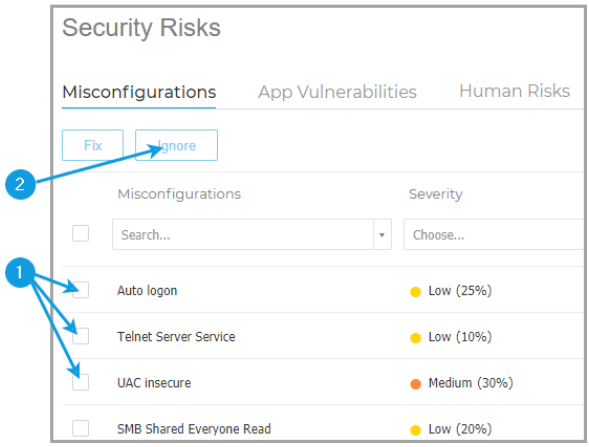
   Появится новое окно, в котором вам нужно подтвердить действие или отменить его.

3. Новая задача создается для применения рекомендуемой настройки на всех затронутых устройствах.

> **Примечание**
> Вы можете проверить ход выполнения задачи на странице **Сеть** > **Задачи**. Если показатель риска можно смягчить только вручную, вам необходимо самостоятельно получить доступ к затронутым устройствам и применить рекомендуемую конфигурацию.

Изменить статус проблем конфигурации:

1. Установите общий флажок или отдельные флажки индикаторов риска, чтобы выбрать их для изменения статуса.



Измените статус многочисленных рисков во вкладке проблем конфигурации

2. Нажмите кнопку **Игнорировать/Восстановить риски**, чтобы изменить статус с **Активен** на **Игнорируется**, или наоборот.

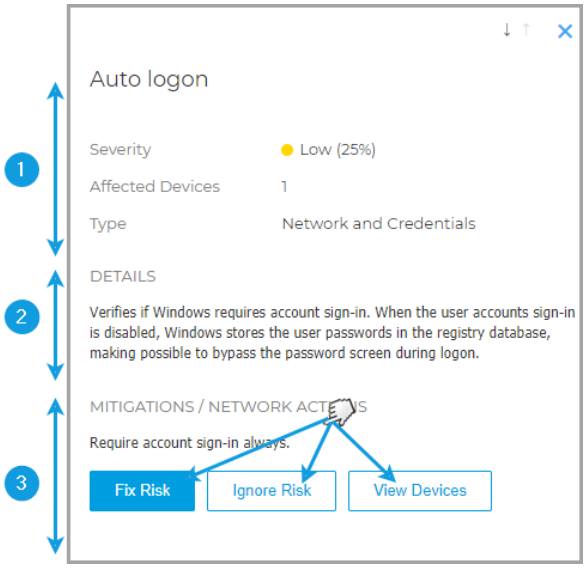
> **Примечание**
> Действие **Игнорировать риски** применяется ко всем выбранным устройствам и влияет на общий балл риска компании при выполнении нового сканирования рисков. Мы настоятельно рекомендуем вам оценить, как игнорируемые индикаторы рисков могут повлиять на безопасность вашей организации.

Вы можете настроить информацию, отображаемую на карточках, и отфильтровать ошибки конфигурации, используя следующие параметры:

Параметры фильтрации	Подробная информация
Ошибка конфигурации	Этот столбец содержит выпадающее меню с возможностью поиска, которое позволяет фильтровать список индикаторов по имени.

Параметры фильтрации	Подробная информация
Степень серьезности	Этот столбец позволяет фильтровать список показателей по степени серьезности каждого показателя риска. Вы можете выбрать между Низким, Средним и Высоким.
Выбранные устройства	В этом столбце показано количество серверов и рабочих станций, которые могут быть подвержены угрозам по определенному показателю риска.
Тип	Этот столбец позволяет фильтровать список показателей риска по типу: • Защита Браузера • Сеть и учетные данные • Безопасность операционной системы
Тип интеграции	Этот столбец позволяет отфильтровать список показателей риска, которые можно уменьшить вручную или автоматически.
Состояние	Этот столбец позволяет фильтровать список показателей риска по их статусу, Активен или Игнорируется.

Щелкните по ошибке конфигурации, которую Вы хотите проанализировать, чтобы развернуть ее боковую панель.



Панель подробностей для ошибок конфигурации

Каждая панель содержит:

1. Информационный раздел с названием индикатора риска, его уровнем серьезности, количеством уязвимых устройств и типом.
2. Раздел **Подробности**, в котором подробно описаны настройки и рекомендации по настройке.
3. Раздел **Смягчение**, содержащий рекомендации по минимизации риска для затронутых устройств, а также доступные действия:
   a. Нажмите кнопку **Исправить риск**, чтобы правильно настроить этот параметр.

      Появится новое окно, в котором вам нужно подтвердить действие или отменить его.

   b. Новая задача создается для применения рекомендуемой настройки на всех затронутых устройствах.

> **Примечание**
> Вы можете проверить ход выполнения задачи на странице **Сеть** > **Задачи**.

Если показатель риска можно смягчить только вручную, вам необходимо самостоятельно получить доступ к затронутым устройствам и применить рекомендуемую конфигурацию.

c. **Игнорировать риски** функция меняет статус выбранного риска и переносит его из **Активных** в **Игнорируемые**.

> **Примечание**
> Вы можете вернуть его в активное состояние в любое время на свой выбор, нажав кнопку **Восстановить риск**.

d. Функция **Просмотр устройств** позволяет перейти на вкладку Устройства, чтобы увидеть все устройства, на которые влияет данный индикатор риска.

Уязвимости приложения

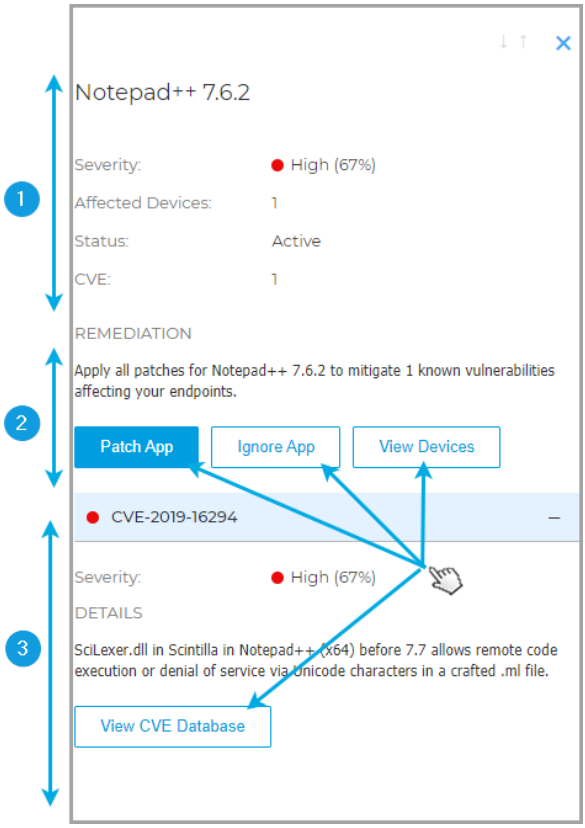
На вкладке **Уязвимости приложений** отображаются все уязвимые приложения, обнаруженные на устройствах в вашей среде во время сканирования. Он предоставляет подробную информацию об уровне их серьезности, количестве известных CVE на приложение и количестве затронутых устройств.

Вы можете настроить информацию, отображаемую на карточках, и отфильтровать уязвимые приложения, используя следующие параметры:

Параметры фильтрации	Подробная информация
Приложения	В этом столбце есть раскрывающееся меню с возможностью поиска, которое позволяет фильтровать список уязвимых приложений по имени.
Степень серьезности	Этот столбец позволяет фильтровать список уязвимых приложений по уровню серьезности каждого приложения. Вы можете выбрать между Низким, Средним и Высоким.
CVE	В этом столбце показано количество общих уязвимостей и рисков (CVE) для приложений, установленных в настоящее время в вашей среде.

Параметры фильтрации	Подробная информация
Выбранные устройства	В этом столбце показано количество серверов и рабочих станций, которые могут быть подвержены угрозам по определенному показателю риска.

Выберите уязвимое приложение, которое вы хотите проанализировать, чтобы развернуть его боковую панель.



Панель подробностей для уязвимых приложений

Каждая панель содержит:

1. Информационный раздел с названием приложения, уровнем серьезности, количеством устройств, на которые оно влияет, и количеством эксплойтов, которые могут повредить вашу среду.
2. Раздел **Исправление** с действиями по смягчению последствий и списком обнаруженных CVE:
   a. Нажмите кнопку **Улучшить приложение**, чтобы применить доступные исправления для уязвимого приложения.

      Важно
      Функция **Улучшить приложение** работает только для сканируемых устройств, на которых установлен модуль Управление патчами.

      Появится новое окно, в котором вам нужно подтвердить действие или отменить его.

   b. Будет создана новая задача по применению исправлений к уязвимым приложениям на всех уязвимых устройствах.

      Примечание
      Вы можете проверить ход выполнения задачи на странице **Сеть** > **Задачи**.

   c. **Игнорировать приложения** функция меняет статус выбранного приложения и переносит его из **Активных** в **Игнорируемые**.

      Примечание
      Вы можете вернуть его в активное состояние в любое время, нажав кнопку **Восстановить приложения**.

   d. Действие **Просмотр устройств** позволяет перейти на вкладку Устройства, чтобы увидеть все устройства, на которые влияет данное уязвимое приложение.
3. Разверните перечисленные CVE и нажмите кнопку **Просмотр базы данных CVE**, чтобы получить доступ к сведениям с конкретной информацией.

Человеческие риски

На вкладке **Человеческие риски** отображаются все риски, вызванные необдуманными или непреднамеренными действиями активных пользователей или отсутствием мер, принятых для надлежащей защиты их

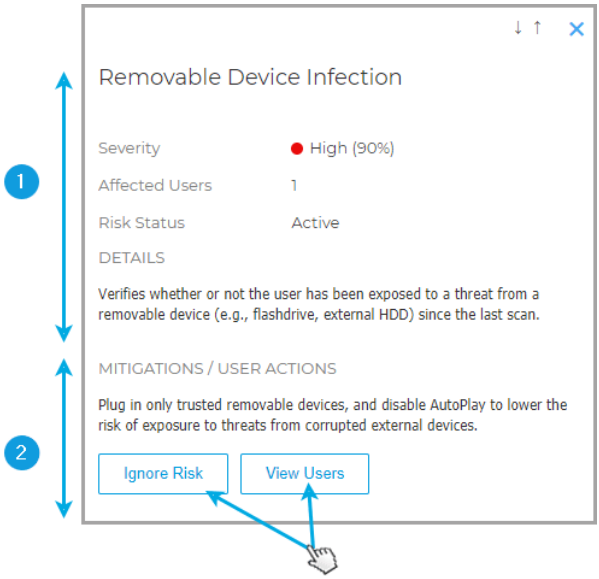
рабочих сессий во время работы в Вашей сети. Он предоставляет подробную информацию об уровне серьезности, количестве уязвимых пользователей, статусе риска и типе

Примечание
Более подробную информацию о том, как мы обрабатываем пользовательские данные, ищите в разделе Сбор данных о человеческом риске

Вы можете настроить информацию, отображаемую на карточках, и отфильтровать человеческие риски, используя следующие параметры:

Параметры фильтрации	Подробная информация
Человеческие риски	Этот столбец содержит выпадающее меню с возможностью поиска, которое позволяет фильтровать список человеческих рисков по названию.
Степень серьезности	Этот столбец позволяет фильтровать список человеческих рисков по их уровню серьезности. Вы можете выбрать между Низким, Средним и Высоким.
Уязвимые пользователи	Данный столбец демонстрирует количество пользователей, вызывающих человечески риски.
Тип интеграции	Этот столбец позволяет отфильтровать список рисков, которые можно уменьшить вручную или автоматически.
Состояние	Этот столбец позволяет фильтровать список рисков по принципу: Активен или Игнорируется.

Выберите человеческие риски, которые Вы хотите проанализировать, чтобы развернуть его боковую панель.



Панель сведений для Human Risks

Каждая панель содержит:

1. Информационный раздел с названием риска, уровнем серьезности, уязвимыми пользователями, статусом риска и подробным описанием риска.
2. **Смягчения/Действия пользователей** раздел со смягчением действий:
   a. **Игнорировать риски** функция меняет статус выбранного риска и переносит его из **Активных** в **Игнорируемые**.

      Примечание
      Вы можете вернуть его в активное состояние в любое время на свой выбор, нажав кнопку **Восстановить риск**.

   b. Действие **просмотр пользователей** приведет Вас ко вкладке Пользователи, чтобы просмотреть всех пользователей, которые спровоцировали этот риск, будучи активными в Вашей сети.

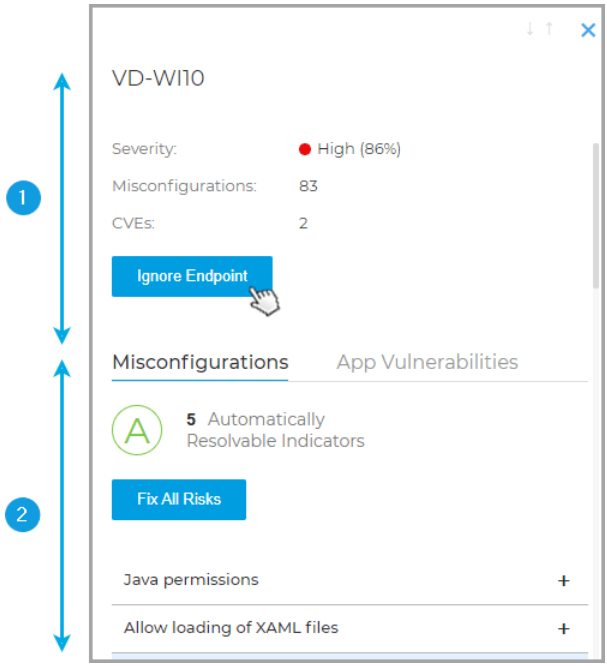
Устройства

На вкладке **Устройства** отображаются все сканируемые серверы и рабочие станции, которыми вы управляете. Он предоставляет подробную информацию об их имени, уровне серьезности, типе устройства и количестве рисков, влияющих на них.

Вы можете настроить информацию, отображаемую на карточках и фильтрующих устройствах, используя следующие параметры:

Параметры фильтрации	Подробная информация
Устройство	Этот столбец содержит выпадающее меню с возможностью поиска, которое позволяет фильтровать список затронутых серверов и рабочих станций по имени.
Степень серьезности	Этот столбец позволяет фильтровать список устройств согласно их уровню влияния друг на друга. Вы можете выбрать между Низким, Средним и Высоким.
Ошибки в конфигурации	В этом столбце показано количество ошибок конфигурации, обнаруженных на устройстве.
CVE	В этом столбце показано количество общих уязвимостей и рисков (CVE), обнаруженных для каждого устройства.
Тип устройств	Этот столбец позволяет фильтровать список устройств по их типу. Вы можете выбрать между сервером и рабочей станцией.

Нажмите на устройство, которое вы хотите исследовать, чтобы развернуть его боковую панель.



Панель подробностей для устройств

Каждая панель содержит:

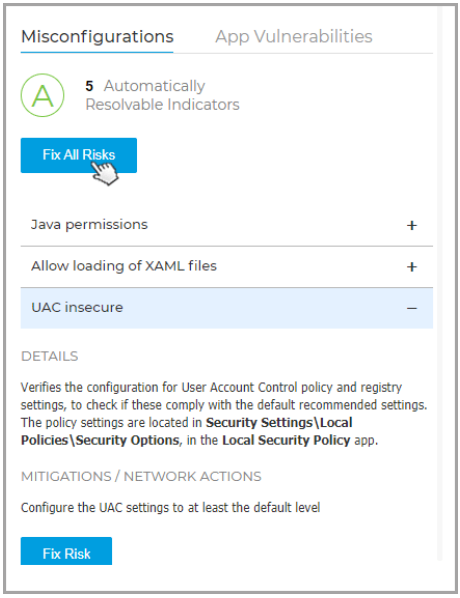
1. Информационный раздел с названием устройства, уровнем серьезности, количеством ошибок конфигурации, распространенными уязвимостями и незащищенностью, которые на него влияют.

   Игнорировать конечную точку функция меняет статус выбранного устройства и переносит его из **Активных** в **Игнорируемые**.

   Примечание
   Вы можете вернуть его в активное состояние в любое время на свой выбор, нажав кнопку **Восстановить риск**.

2. Раздел о рисках, подробно отображающий каждую ошибку конфигурацию и уязвимое приложение, обнаруженное на устройстве, сгруппирован в две вкладки.

- На вкладке **Ошибки конфигурации** содержатся все ошибки конфигурации, обнаруженные на устройстве, сгруппированные в индикаторы риска, которые можно исправить автоматически, и индикаторы риска, которые можно устранить только вручную.



a. Нажмите на **Исправить все риски** кнопку, чтобы изменить все неверные настройки и политики, влияющие на устройство.

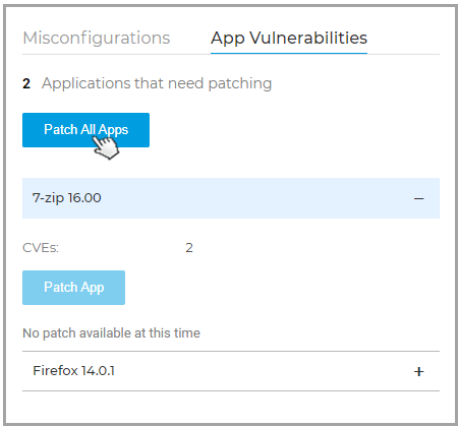
   Появится новое окно, в котором вам нужно подтвердить действие или отменить его.

b. Новая задача создается для применения рекомендуемой настройки на затронутом устройстве.

> **Примечание**
> Вы можете проверить ход выполнения задачи на странице **Сеть** > **Задачи**.
> Для показателя риска, который можно смягчить только вручную, Вам необходимо самостоятельно получить доступ к затронутым устройствам и применить рекомендуемую конфигурацию.

Примечание
Вы также можете исследовать отдельно каждую неправильную конфигурацию, влияющую на текущее устройство, и исправлять их одну за другой при помощи кнопки **Устранить риск**.

- На вкладке **Уязвимости приложений** содержатся все уязвимые приложения, обнаруженные на устройстве, и количество CVE, влияющих на каждое приложение.



a. Нажмите кнопку **Исправить все приложения**, чтобы применить доступные исправления ко всем уязвимым приложениям, которые подвергают выбранное устройство угрозам.

Важно
Функция **Исправить все приложения** работает только для сканируемых устройств, на которых установлен модуль Управление патчами.

Появится новое окно, в котором вам нужно подтвердить действие или отменить его.

b. Будет создана новая задача по применению исправлений к уязвимым приложениям на этом устройстве.

Примечание
Вы можете проверить ход выполнения задачи на странице **Сеть** > **Задачи**.

Примечание
Вы также можете исследовать отдельно каждое уязвимое приложение, влияющее на текущее устройство, и исправлять их одно за другим при помощи кнопки **Исправить приложение**.

Пользователи

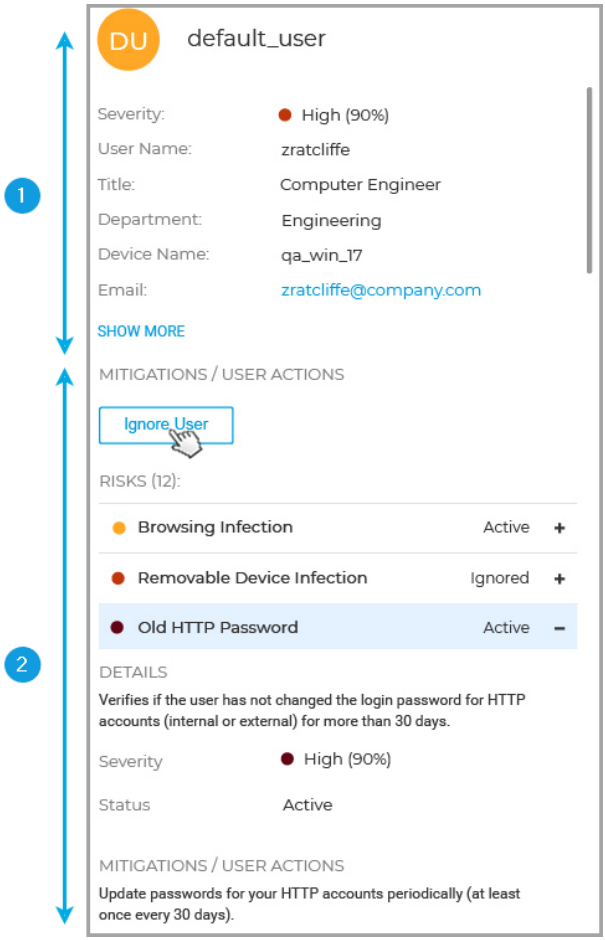
На вкладке **Пользователи** отображаются все пользователи, которые намеренно или неосознанно подвергают Вашу среду угрозам. Он предоставляет такую информацию, как имя пользователя, уровень общей серьезности риска для этого пользователя, должность пользователя и отдел, количество рисков, которым они подвергаются, и их статус при расчете общего риска компании.

Вы можете настроить информацию, отображаемую на карточках и фильтрующих устройствах, используя следующие параметры:

Параметры фильтрации	Подробная информация
Пользователи	Этот столбец содержит поле с возможностью поиска, которое позволяет фильтровать список уязвимых пользователей по имени.
Степень серьезности	Этот столбец позволяет фильтровать список уязвимых пользователей по их уровню серьезности. Вы можете выбрать между Низким, Средним и Высоким.
Номер риска	Данный столбец демонстрирует число человеческих рисков, которые представляет каждый пользователь.
Название	Данный столбец позволяет Вам фильтровать список пользователей по их праву в данной организации.
Отдел	Данный столбец позволяет Вам фильтровать список пользователей по отделу, к которому они относятся в данной организации.

Параметры фильтрации	Подробная информация
Состояние	Этот столбец позволяет фильтровать список пользователей по принципу: Активен или Игнорируется.

Нажмите на пользователя, которого Вы хотите изучить, разворачивая боковую панель.



Панель сведений для пользователей

Каждая панель содержит:

1. Информационный раздел с именем пользователя, названием и отделом, контактной информацией, уровнем серьезности и статусом.
2. **Смягчения/Действия пользователей** раздел со смягчением действий:
   a. **Игнорировать пользователя** функция меняет статус выбранного пользователя и переносит его из **Активных** в **Игнорируемые**.

Примечание
Вы можете вернуть его в активное состояние в любое время на свой выбор, нажав кнопку **Восстановить пользователя**.

12. ИСПОЛЬЗОВАНИЕ ОТЧЕТОВ

GravityZone позволяет создавать и просматривать централизованные отчеты о состоянии безопасности управляемых сетевых объектов. Отчеты можно использовать для различных целей:

- Отслеживать и обеспечивать соблюдение политик безопасности предприятия.
- Проверять и оценивать статус безопасности сети.
- Выявлять проблемы безопасности сети, угрозы и уязвимости.
- Отслеживание инцидентов безопасности.
- Использовать функции управления высокого уровня с четким и удобным представлением данных о безопасности.

Доступно несколько различных типов отчетов, так что вы сможете легко получить необходимую информацию. Информация представлена в удобочитаемых интерактивных графиках и таблицах, что позволяет быстро проверить статус безопасности сети и выявить любые угрозы.

В отчетах можно объединить данные управляемых объектов всей сети или отдельных групп. Таким образом, в одном отчете будут содержатся следующие сведения:

- Статистические данные по всем группам управляемых объектов сети.
- Подробная информация по каждому управляемому объекту сети.
- Список компьютеров, которые отвечают определенным критериям (например, те, на которых отключена защита от вредоносных программ).

Некоторые отчеты также позволяют быстро исправить ошибки, найденные в сети. Например, вы можете легко обновить данные о всех выбранных сетевых объектах прямо из отчета, без необходимости переходить и запускать задачу обновления в разделе **Сеть**.

Все запланированные отчеты доступны в Control Center, но вы можете сохранить их на ваш компьютер или отправить по электронной почте.

Доступные форматы включают Portable Document Format (PDF) и comma-separated values (CSV).

12.1. Типы отчетов

Различные типы отчетов доступны по каждому типу конечных точек:

- Отчеты по компьютерам и виртуальным машинам
- Отчеты Exchange

12.1.1. Отчеты по компьютерам и виртуальным машинам

Следующие типы отчетов доступны для физических и виртуальных машин:

Антифишинговая активность

Информирует вас об активности антифишингового модуля Bitdefender Endpoint Security Tools. Вы можете просмотреть количество заблокированных фишинговых веб-сайтов на выбранных конечных устройствах и пользователей, которые были зафиксированы во время последнего обнаружения. Нажав на ссылку в колонке **Заблокированные сайты**, вы также сможете просмотреть URL веб-сайтов, сколько раз они были заблокированы и когда было последнее событие блокировки.

Заблокированные приложения

Информирует вас об активности следующий модулей: Защита от вредоносного ПО, Брандмауэр, Контроль контента, Advanced Anti-Exploit и ATC/IDS. Вы можете просмотреть количество заблокированных приложений на выбранных конечных точках и пользователей, которые были зарегистрированы во время последнего обнаружения.

Щелкните номер, связанный с целью, чтобы просмотреть дополнительную информацию о заблокированных приложениях, количестве произошедших событий и дате и времени последнего события блока.

На основании этого отчета вы можете быстро настроить модули защиты, чтобы разрешить выбранному приложению работать в конечной точке назначения:

Нажмите кнопку **Добавить исключение**, чтобы определить исключения в следующих модулях: Защита от вредоносных программ, ATC, Управление контентом и брандмауэр. Появится окно подтверждения, уведомляющее о новом правиле, что приводит к изменению существующей политики для этой конкретной конечной точки.

Заблокированные веб-сайты

Информирует вас об активности модуля управления веб-доступом Bitdefender Endpoint Security Tools. Для каждого объекта вы можете просмотреть количество заблокированных веб-сайтов. Нажав на цифру вы можете просмотреть дополнительную информацию, например:

- URL веб-сайта и категория
- Количество попыток доступа на веб-сайт
- Дата и время последней попытки, а также пользователь, который был зафиксирован в момент обнаружения.
- Причина блокировки, которая включает в себя запланированный доступ, обнаружение вредоносных программ, категории фильтрации и черные списки.

Защита данных

Информирует вас об активности модуля защиты данных Bitdefender Endpoint Security Tools. Вы можете увидеть количество заблокированных сообщений электронной почты и веб-сайтов на выбранных конечных точках, а также пользователей, которые были зафиксированы во время последнего обнаружения.

Активность управления устройствами

Информирует вас о событиях, произошедших при доступе конечных точек через контролируемые устройства. Для каждой конечной точки вы можете просмотреть количество разрешенных / заблокированных попыток доступа и событий только для чтения. Если события произошли, то дополнительную информацию вы сможете получить, нажав на соответствующие цифры. Подробности содержат информацию о:

- Регистрации пользователя на машине
- Типе устройства и его ID
- Разработчике устройства и ID модели
- Дате и времени события.

Состояние шифрования конечных точек

Предоставляет вам данные о состоянии шифрования на конечных точках. Круговая диаграмма отображает количество систем отвечающих, и , соответственно, не отвечающих требованиям настройки политики шифрования.

Таблица ниже в виде круговой диаграммы предоставляет такие данные, как:

- Имя конечного пользователя.
- Полное доменное имя (FQDN).

- IP-адрес рабочей станции
- Операционная система.
- Согласование политики устройства:
  - **Совместимость** - когда все тома шифруются или незашифрованы в соответствии с политикой.
  - **Не совместимо** - когда статус томов не соответствует назначенной политике (например, зашифрован только один из двух томов или процесс шифрования выполняется на этом томе в текущий момент).
- Политика устройства (**Шифрование** или **Дешифровка**).
- Чтобы просмотреть информацию о томах каждой конечной точки кликайте цифры в столбце Общие данные по томам: идентификатор, имя, состояние шифрования (**Зашифровано** или **Незашифровано**), Проблемы, тип (**Загрузка** или **Не загружается**), размер, идентификатор ключа восстановления.
- Название компании.

Состояние модулей конечной точки

Содержит обзор охвата модулей защиты по выбранным целям. В деталях отчета для каждого пользователя вы можете посмотреть, какие модули активны, отключены или не установлены, а также используемый механизм сканирования. При нажатии на имя конечного пользователя (компьютера) отображается окно **Информация** с информацией о конечном пользователе (компьютере) и установленных уровнях защиты.

Нажав кнопку **Реконфигурировать клиента**, Вы можете запустить задачу по изменению начальных настроек одной или нескольких выбранных конечных точек. Для получения большей информации перейдите по Настройка клиента.

Состояние защиты конечных точек

Предоставляет вам различную информацию о состоянии выбранных конечных точек в вашей сети.

- Состояние защиты от вредоносного ПО
- Состояние обновления Bitdefender Endpoint Security Tools
- Состояние сетевой активности (online/offline)
- Состояние управления

Вы можете применять фильтры по показаниям безопасности и состоянии, чтобы найти необходимую информацию.

Активность файрвола

Информирует вас об активности модуля файрвола Bitdefender Endpoint Security Tools. Вы можете увидеть количество блокировок трафика и блокировок сканирования портов на выбранных конечных точках, а также пользователей, которые были зафиксированы и обнаружены.

активность по обнаружению гипервизора

Информирует вас об активности модуля HyperDetect Bitdefender Endpoint Security Tools.

Диаграмма в верхней части страницы отчета показывает динамику попыток атаки за указанный период времени и их распределение по типу атаки. Перемещая курсор над элементами таблицы вы будете видеть соответствующий тип атаки в диаграмме. При нажатии на запись будет отображаться или скрываться соответствующая строка на диаграмме. Кликнув по любому параметру, вы отфильтруете данные таблицы в соответствии с выбранным параметром. Например, если вы нажмете любую точку на оранжевой линии, таблица отобразит только эксплойты.

В нижней части отчета будет отображаться информация о выявленных нарушениях в вашей сети и о том, были ли они рассмотрены. Они относятся к:

- Путь к вредоносному файлу или обнаруженному URL-адресу в случае зараженных файлов. Для атак, не содержащих файлы, назначается имя исполняемого файла, используемого в атаке, и ссылка на окно информации, в котором отображена причина обнаружения и вредоносная командная строка.
- Конечная точка, на которой было выполнено обнаружение
- Модуль защиты, который обнаружил угрозу. Поскольку Hyper Detect является дополнительным уровнем модулей Защиты от вредоносных программ и контента, в отчете появится только один из этих двух модулей, в зависимости от типа обнаружения.
- Тип предполагаемой атаки (целевая атака, нежелательная программа, эксплойты, программы-вымогатели, подозрительные файлы и сетевой трафик)
- Состояние угрозы

- Уровень защиты модуля, на котором обнаружена угроза (Рекомендуемый, Нормальный, Интенсивный)
- сколько раз была обнаружена угроза
- Последнее обнаружение
- Идентификация атаки в качестве не содержащей файлы (да или нет) для быстрой фильтрации обнаруженных атак.

Примечание
Файл может использоваться для различных типов атак. Поэтому GravityZone сообщает об этом для каждого типа атаки, в которой было принято участие.

На основе этого отчета вы можете с легкостью распознать ложные срабатывания, добавив исключения в назначенную политику безопасности. Для этого:

1. Выберите необходимое количество записей в таблице.

   Примечание
   В список исключений нельзя добавить обнаружение без файлов, в силу того, что обнаруженный исполняемый файл не является вредоносной программой, но может представлять угрозу при использовании вредоносной закодированной командной строки.

2. Нажмите кнопку **Добавить исключение** в верхней части таблицы.
3. В окне конфигурации выберите политики, к которым следует добавить исключение, и нажмите **Добавить** .

   Соответствующая информация для каждого добавленного исключения по умолчанию отправляется в Bitdefender Labs, чтобы помочь улучшить возможности обнаружения продуктов Bitdefender. Вы можете управлять этим действием с помощью флажка **Отправить отзыв в Bitdefender для детального анализа** .

Если угроза была обнаружена модулем защиты от вредоносных программ, это исключение будет применяться как к режимам проверки доступа, так и по требованию.

Примечание
Данные исключения можно найти в следующих разделах выбранных политик: **Защита от вредоносных программ > настройки** для файлов и **Контроль контента > Трафик** для URL-адресов.

Состояние активности вредоносного ПО
Помогает вам узнать сколько и какие из выбранных конечных точек были затронуты вредоносным ПО в течении определенного периода времени и какие меры были приняты. Вы также можете просмотреть пользователя, который был зарегистрирован во время последнего обнаружения.

Конечные точки группируются по следующим критериям:

- Конечные точки без каких-либо срабатываний (вредоносные угрозы не были обнаружены за указанный период времени)
- Конечные точки, вылеченные от вредоносных программ (все обнаруженные файлы были успешно вылечены или перемещены в карантин)
- Конечные точки с неразрешенным вредоносным ПО (доступ к некоторым обнаруженным файлам запрещен)

Для каждой конечной точки, нажав ссылки, доступные в колонках результатов лечения, вы сможете просмотреть список угроз и путей к поврежденным файлам.

В этом отчете вы можете запустить задачу полной проверки для неразрешенных целей, нажав кнопку **Сканировать зараженные цели** в Панели инструментов над таблицей данных.

Ежемесячное использование лицензии
Нажмите на цифры в каждом столбце, чтобы посмотреть подробную информацию о каждом модуле и доступном дополнении. Вы можете легко настроить отчет, нажав кнопку **Показать/скрыть столбцы**.

Email Security - ежемесячное использование лицензии
Этот отчет содержит информацию об использовании лицензии для службы Email Security. Все интервалы отчета извлекают информацию об использовании лицензии до конца предыдущего дня. Например, вы генерируете отчет в понедельник в 12 часов дня и устанавливаете интервал на **В этом месяце**. В отчете будет представлена информация об использовании лицензии до конца воскресенья.

Отчет об инцидентах

Информирует вас о деятельности модуля Network Attack Defense. График отображает количество попыток атаки, обнаруженных за указанный интервал. Детали отчета включают в себя:

- Имя конечной точки, IP и полное доменное имя (FQDN)
- Имя пользователя
- Имя обнаружения
- Техника атаки
- Количество попыток
- IP-адрес атакующего
- Целевой IP и порт
- Когда была произведена ближайшая блокировка атаки

При нажатии кнопки **Добавить исключения** для выбранного обнаружения автоматически создается запись в **Глобальных исключениях** из раздела **Защита сети**.

Статус сетевого патча

Проверка статуса обновлений ПО, которое установлено в вашей сети. Отчет передает следующие детали:

- Целевой компьютер (имя конечной точки, IP и операционная система).
- Исправления безопасности (установленные исправления, сбойные исправления, отсутствующие исправления безопасности и исправления, не связанные с безопасностью).
- Состояние и время последнего изменения для проверенных конечных точек.

Состояние защиты сети

Содержит подробную информацию об общем состоянии безопасности выбранных конечных точек. Например, вы можете просмотреть информацию о:

- Имя, IP и FQDN
- Статус:
  - **Возникли проблемы** - конечная точка имеет уязвимости защиты (агент безопасности не обновлен, обнаружены угрозы безопасности и пр.)

- **Проблем нет** - конечные точки защищены, и нет повода для беспокойства.
- **Нет данных** - при создании отчета конечные точки недоступны.
- **Неуправляемо** - агент безопасности пока еще не установлен на конечных точках.

- Доступные уровни защиты
- Управляемые и неуправляемые конечные точки (с установленными агентами безопасности и без)
- Статусе и типе лицензии (дополнительные столбцы, связанные с лицензиями, по умолчанию скрыты)
- Статус инфекции (очищена ли конечная точка)
- Состоянии обновления продукта и механизмов защиты
- Состоянии исправлений безопасности ПО (недостающие исправления связанные и не связанные с безопасностью)

Для неуправляемых конечных точек, в других столбцах вы увидите статус **Неуправляемый**

Сканирование по запросу

Предоставляет информацию о сканировании по запросу, проведенному на выбранных объектах. Круговая диаграмма будет отображать статистику успешных и неудачных проверок. Таблица под графиком будет содержать подробную информацию о типах сканирования, инцидентах и последнем успешном сканировании по каждой конечной точке.

Соблюдение политик

Предоставляет информацию о политиках безопасности, применяемых на выбранных объектах. Круговая диаграмма будет отображать состояние политики. В таблице под графиком вы сможете увидеть политики и их типы, назначенные каждой конечной точке, а также дату и пользователей, которые их назначили.

Sandbox Analyzer ошибки подчинения

Отображает все неудачные попытки перемещения объектов, отправленных с конечных точек, в Sandbox Analyzer за определенный период времени. Приписывание считается неудачным после нескольких попыток повтора.

На графике показано изменение неудачных перемещений в течение выбранного периода, в то время как в таблице сведений о отчетах вы можете просмотреть, какие файлы не могли быть отправлены в Sandbox Analyzer, систему, с которой был отправлен объект, дату и время повторения каждой попытки, ошибку которую выдал код, описание каждой неудачной попытки и название компании.

Результаты Sandbox Analyzer (устарело)

Предоставляет подробную информацию о файлах на целевых конечных точках, которые были проанализированы в песочнице в течение определенного периода времени. В линейной диаграмме отображается количество чистых или опасных анализируемых файлов, в то время как в таблице представлены данные о каждом событии.

Вы можете создать отчет о результатах работы Sandbox Analyzer для всех проанализированных файлов или только для тех, которые были идентифицированы, как вредоносные.

Вы можете просмотреть:

- Примите решение о том, указав, является ли файл чистым, опасным или неизвестным (**Обнаружена угроза** / **Не обнаружено угрозы** / **Неподдерживаемый**). Этот столбец отображается только при выборе отчета для отображения всех проанализированных объектов.

  Чтобы просмотреть полный список типов файлов и расширений, поддерживаемых Sandbox Analyzer, см. «Поддерживаемые Типы и Расширения Фалов для Отправки Вручную» (p. 512).
- Тип угрозы, такой как рекламное ПО, руткит, загрузчик, эксплойт, модификатор хоста, вредоносные инструменты, программа для кражи паролей, программа-вымогатель, спам или троян.
- Дата и время обнаружения, вы можете фильтровать эти данные в зависимости от отчетного периода.
- Имя хоста или IP конечной точки, где был обнаружен файл.
- Имя файлов, если они были отправлены индивидуально, или количество проанализированных файлов в случае групповой отправки. Нажмите ссылку на имя файла или ссылку для просмотра деталей и действий.
- Статус действия обезвреживания файлов (**Частичный** , **Не удалось** , **Только отчетная информация** , **Успешно**).
- Название компании.
- Более подробную информацию о свойствах анализируемого файла можно получить, нажав **Подробнее** в столбце **Результат анализа**

. Здесь вы можете просмотреть сведения о безопасности и подробные отчеты о поведении образцов.

Sandbox Analyzer обращает внимание на следующие поведенческие события:

- Запись / удаление / перемещение / дублирование / замена файлов в системе и на съемных дисках.
- представление недавно созданных файлов.
- Изменения в файловой системе.
- Изменения в приложениях, запущенных внутри виртуальной машины.
- Изменения в панели задач Windows и в меню «Пуск».
- Создание / завершение / вброс процессов.
- Запись / удаление ключей реестра.
- Создание объектов мьютекса.
- Создание / запуск / остановка / изменение / запрос / удаление служб.
- Изменение настроек безопасности браузера.
- Изменение настроек экрана проводника Windows.
- Добавление файлов в список исключений брандмауэра.
- Изменение сетевых настроек.
- Включение выполнения при запуске системы.
- Подключение к удаленному хосту.
- Доступ к определенным доменам.
- Перенос данных в определенные области и из них.
- Доступ к URL-адресам, IP-адресам и портам через различные протоколы связи.
- Проверка индикаторов виртуальной среды.
- Проверка индикаторов инструментов мониторинга.
- Создание моментальных снимков.
- SSDT, IDT, IRP-захваты.
- Сброс памяти для подозрительных процессов.
- Вызов функций API Windows.
- Становится неактивным в течение определенного периода времени, чтобы отложить выполнение.
- Создание файлов с действиями, которые должны выполняться через определенные промежутки времени.

В окне **Результаты анализа** нажмите кнопку **Загрузить**, чтобы сохранить на своем компьютере содержимое сводки поведения в следующих форматах: XML, HTML, JSON, PDF.

Этот отчет будет поддерживаться в течение ограниченного периода времени. Рекомендуется вместо этого использовать карточки отправления для сбора необходимой информации по анализируемым образцам. Карточки отправления доступны в разделе **Sandbox Analyzer** в главном меню Control Center.

Аудит безопасности

Предоставляет информацию о событиях безопасности, произошедших на выбранном объекте. Информация относится к следующим событиям:

- Обнаружение вредоносного ПО
- Заблокированное приложение
- Заблокированное сканирование порта
- Заблокированный трафик
- Заблокированный веб-сайт
- Блочное устройство
- Заблокированная электронная почта
- Заблокированный процесс
- События Advanced Anti-Exploit
- Network Attack Defense события
- Обнаружение программы-вымогателя

Статус Security Server

Помогает оценить состояние серверов Security Server. Вы можете определить возникшие проблемы каждого Security Server с помощью различных индикаторов состояния, таких как:

- **Статус**: показывает общий статус Security Server.
- **Статус машины**: сообщает, какие устройства Security Server остановлены.
- **Статус Антивируса**: указывает, включен или отключен модуль защиты от вредоносных программ.
- **Статус обновления**: показывает, что устройства Security Server обновлены или обновления были отключены.
- **Статус загрузки**: указывает на уровень нагрузки при сканировании на Security Server, как описано ниже:
  - **Неполная**, при использовании менее чем 5% от его возможностей сканирования.

- **Нормальная**, когда нагрузка сканирования является сбалансированной.
- **Полная**, когда нагрузка сканирования превышает 90% от его мощности. В этом случае необходимо проверить политики безопасности. Если все Security Server, выделенные в рамках политики, перегружены, необходимо добавить еще один Security Server в список. В противном случае, проверьте сетевое соединение между клиентами и серверами Security Server без нагрузки.
- **Близкая перегрузка**, когда нагрузка на сканирование составляет от 85 до 90% от полной емкости сканирования.
- **Практически недостаточная загрузка**, когда нагрузка при сканировании составляет от 5 до 10% от полной нагрузки при сканировании.

Также вы можете узнать, сколько агентов подключено к Security Server. Далее, кликая на количество подключенных клиентов можно увидеть список конечных точек. Эти конечные пользователи (компьютеры) могут быть уязвимыми, если у Security Server есть проблемы.

Топ-10 обнаруженных вредоносных программ

Показывает Топ-10 вредоносных программ, обнаруженных в течение определенного периода времени на отдельных конечных точках.

Примечание
Таблица с подробной информацией будет отображать все конечные точки, которые были заражены Топ-10 обнаруженных вредоносных программ.

Топ-10 зараженных конечных точек

Показывает Топ-10 самых зараженных конечных устройств от общего числа обнаружений, в течении определенного периода времени.

Примечание
Таблица с подробной информацией будет отображать все обнаруженные вредоносные программы на Топ-10 зараженных конечных точках.

Состояние обновления

Показывает статус обновления агента безопасности или Security Server, установленного на выбранных объектах. Состояние обновления относится к версиям продукта и механизмов защиты.

Используя имеющиеся фильтры, вы можете легко выяснить, какие клиенты были обновлены и какие нет за последние 24 часа.

В этом отчете вы можете быстро обновить агентов до последней версии. Для этого нажмите на значок **Обновить** на панели инструментов действия над таблицей данных.

Состояние обновления версии продуктов

Показывает доступность новых версий агентов безопасности, установленных на выбранных объектах.

На конечных точках с устаревшими агентами безопасности вы можете быстро установить последнюю версию поддерживаемого агента, нажав кнопку **Обновление**.

Примечание
Этот отчет доступен только тогда, когда решение GravityZone обновлено.

Активность вредоносных программ

Информирует Вас об атаках вымогателей, обнаруженных GravityZone на конечных точках, которыми Вы управляете, и предоставляет Вам необходимые инструменты для восстановления файлов, затронутых во время атак.

Отчет доступен в виде страницы в Control Center, отличной от других отчетов, доступных в главном меню GravityZone.

Страница **Активность вымогателей** состоит из сетки, в которой перечисляются действия, свойственные для каждой атаки:

- Имя, IP-адрес и полное доменное имя конечной точки относительно которой была совершена атака
- Компания, которой принадлежит конечная точка.
- Имя пользователя, вошедшего в систему во время атаки
- Тип атаки, локальный или дистанционный
- Процесс, в рамках которого программа-вымогатель выполняла локальные атаки, или IP-адрес, с которого была инициирована атака
- Дата и время обнаружения.
- Количество файлов, было зашифровано до тех пор, пока атаку не заблокировали

- Действия по восстановлению для всех файлов на целевой конечной точке.

Эти детали скрыты по умолчанию. Нажмите кнопку **Показать/Скрыть столбцы** в правом верхнем углу страницы, чтобы настроить сведения, которые Вы хотите просмотреть в сетке. Если у Вас много записей в сетке, Вы можете скрыть фильтры с помощью кнопки **Показать/Скрыть фильтры** в правом верхнем углу страницы.

Дополнительную информацию можно получить, нажав на номер файла. Вы можете просмотреть список с полным путем к исходным и восстановленным файлам, а также статус восстановления для всех файлов, участвующих в выбранной атаке вымогателей.

Важно
Резервные копии доступны не более чем на 30 дней. Пожалуйста, обратите внимание на дату и время, пока существует возможность восстановления файлов.

Для восстановления файлов от программ-вымогателей:

1. Выберите необходимые Вам атаки в сетке.
2. Нажмите кнопку **Восстановить файлы**. Появится окно подтверждения.

   Создается задача по восстановлению. Вы можете проверить его статус на странице **Задачи**, как и для любой другой задачи в GravityZone.

Если обнаружение является результатом законных процессов, выполните следующие действия:

1. Выберите записи в сетке.
2. Нажмите на **Добавить исключения** кнопку.
3. В новом окне выберите политики, к которым должно применяться исключение.
4. Нажмите **Добавить**.

   GravityZone Будут применены все возможные исключения: на папку, на процесс и на IP-адрес.

   Вы можете проверить или изменить их в разделе **Antimalware > Settings > Custom Exclusions** политики.

Примечание
Деятельность вымогателей отслеживается в течение 2 лет.

12.1.2. Отчеты сервера Exchange

Доступны следующие типы отчетов для серверов Exchange:

Exchange - Заблокированное содержимое и вложения
Содержит информацию о письмах или вложениях, которые модуль управления контентом удалил с выбранных серверов в течение определенного интервала времени. Информация содержит:

- Адреса электронной почты отправителей и получателей.

  Если электронное письмо содержит много получателей, вместо адресов электронной почты в отчете отображается количество получателей, являющееся ссылкой на окно, содержащее список адресов электронной почты.
- Тема Email.
- Тип обнаружения, указывающий, что фильтр управления контентом обнаружил угрозу.
- Действия предпринятые при обнаружении.
- Сервер, на котором была обнаружена угроза.

Exchange - Заблокированые несканируемые вложения
Содержит информацию о письмах, содержащих несканируемые вложения (сильно сжатые, защищенные паролем, и т.д.), заблокированные на почтовых серверах Exchange в течение определенного периода времени. Информация содержит:

- Адреса электронной почты отправителей и получателей.

  Если электронное письмо содержит много получателей, вместо адресов электронной почты в отчете отображается количество получателей, являющееся ссылкой на окно, содержащее список адресов электронной почты.
- Тема Email.
- Действия, выполненные при удалении несканируемых вложений:
  - **Удаленное письмо**, указывает, что все сообщение было удалено.

- **Удаленные вложения**, общее название для всех действий, которые удаляют вложения из сообщений электронной почты, таких как удаление вложения, перемещение в карантин или перемещение с уведомлением.

Нажав на ссылку в колонке **Действие**, вы сможете просмотреть подробную информацию о каждом заблокированном вложении и соответствующем предпринятом действии.

- Дату и время обнаружения.
- Сервер, на котором было обнаружено электронное письмо.

Exchange - сканирование активности электронной почты

Показывает статистику о действиях, предпринятых модулем защиты Exchange, в течении определенного интервала времени.

Действия сгруппированы по типу обнаружения (вредоносные программы, спам, запрещенные вложения и запрещенный контент) и по серверам.

Статистика показывает следующие состояния электронной почты:

- **Карантин.** Эти письма были перемещены в папку карантина.
- **Удалено/Отклонено** Эти письма были удалены или отклонены сервером.
- **Перенаправлено.** Эти письма были перенаправлены на адрес электронной почты, указанный в политике.
- **Очищено и доставлено** В этих письмах угрозы были удалены и пропущены через фильтры.

  Электронная почта считается очищенной, когда все обнаруженные вложения были вылечены, перемещены в карантин, удалены или замещены текстом.
- **Изменено и доставлено.** В заголовки этих писем была добавлена информация о сканировании и такие письма прошли через фильтры.
- **Доставлено без других действий.** Эти письма были проигнорированы защитой Exchange и пропущены через фильтры.

Exchange - Активность вредоносного ПО

Содержит информацию о письмах с вредоносным ПО, обнаруженных на выбранных почтовых серверах Exchange в течении определенного периода времени. Информация содержит:

- Адреса электронной почты отправителей и получателей.

  Если электронное письмо содержит много получателей, вместо адресов электронной почты в отчете отображается количество получателей, являющееся ссылкой на окно, содержащее список адресов электронной почты.

- Тема Email.
- Состояние электронного письма после сканирования на вредоносное ПО.

  Нажав на ссылку состояния, вы сможете просматреть подробную информацию об обнаруженных вредоносных программах и действях над ними.

- Дату и время обнаружения.
- Сервер, на котором была обнаружена угроза.

Exchange - Ежемесячное использование лицензии

Содержит подробную информацию относительно использования лицензий Security for Exchange вашей компанией в течение определенного периода времени.

В таблице под графиком будет представлена подробная информация относительно названия компании, лицензионного ключа, месяца и количества защищаемых почтовых ящиков, принадлежащих вашей компаний.

Количество использованных лицензий - ссылка на новое окно, где вы можете найти подробную информацию об использовании, такую как лицензированные домены вашей компании и принадлежащие ей почтовые ящики.

Exchange - Топ-10 обнаруженных вредоносных программ

Сообщает вам о Топ-10 самых распространенных угроз, обнаруженных в почтовых вложениях. Вы сможете создать два представления, содержащие различные статистические данные. Один вид показывает количество обнаружений, затрагиваемых получателей и одного отправителя.

Например, GravityZone обнаружил одно письмо с зараженным вложением, отправленное пяти получателям.

- При просмотре получателей:

- В отчете показано пять обнаружений.
- В отчете подробно показаны только получатели, а не отправители.

- При просмотре отправителей:
  - В отчете показано одно обнаружение.
  - В отчете подробно показан только отправитель, а не получатели.

Кроме отправителя/получателей и имен вредоносных программ, отчет предоставляет вам следующие данные:

- Тип вредоносных программ (вирус, шпионские программы, PUA и т.д.)
- Сервер, на котором была обнаружена угроза.
- Меры, которые предпринял модуль защиты от вредоносных программ.
- Дату и время последнего обнаружения.

Exchange - Топ-10 получателей вредоносных программ

Показывает Топ-10 почтовых получателей, которые стали мишенью вредоносных рассылок в течение определенного интервала времени.

В отчете подробно предоставляется весь список вредоносных программ, которые затрагивают этих получателей, вместе с предпринятыми действиями.

Exchange - Топ-10 получателей спама

Показывает Топ-10 получателей электронной почты по числу спам- или фишинговых писем, обнаруженных в течение определенного интервала времени. Отчет содержит информацию о предпринятых действиях над соответствующими письмами.

12.2. Создание отчетов

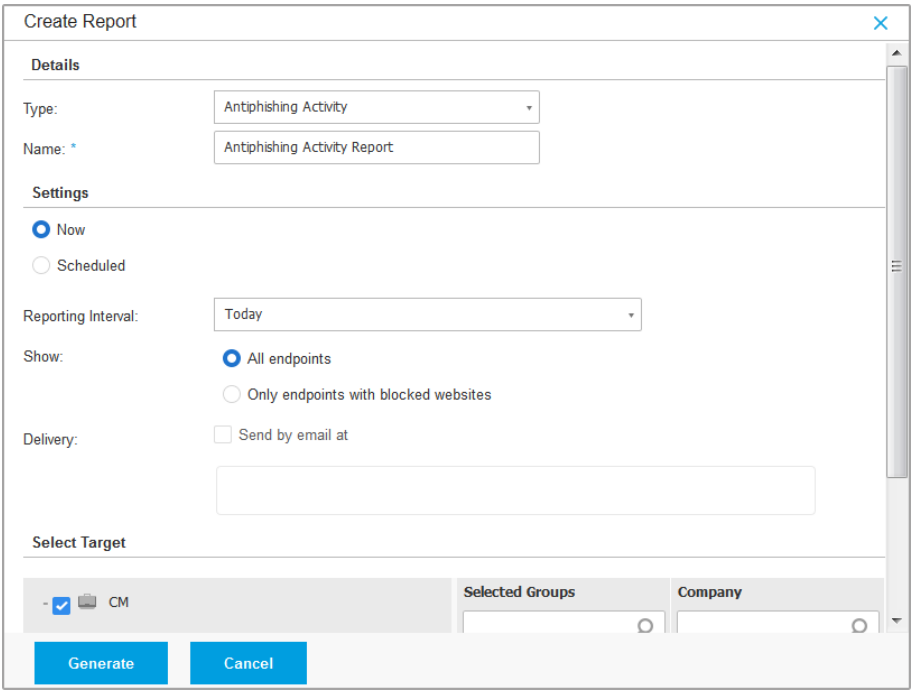
Вы можете создать две категории отчетов:

- **Мгновенные отчеты.** Мгновенные отчеты автоматически отображаются сразу после их создания.
- **Отчеты по расписанию.** Запланированные отчеты могут быть настроены на периодический запуск в заданные дату и время. Список всех запланированных отчетов отображается на странице **Отчеты**.

Важно
Мгновенные отчеты автоматически удаляются при закрытии страницы отчета. Запланированные отчеты сохраняются и отображаются на странице **Отчеты**.

Чтобы создать отчет:

1. Перейдите на страницу **Отчеты**.
2. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Появится окно конфигурации.



Настройки отчета

3. Выберите нужный тип отчета из меню. Для получения более подробной информации, обратитесь к«Типы отчетов» (p. 434)
4. Введите подходящее имя для отчета. При выборе имени учитывайте тип отчета, его назначение и возможности параметров отчета.

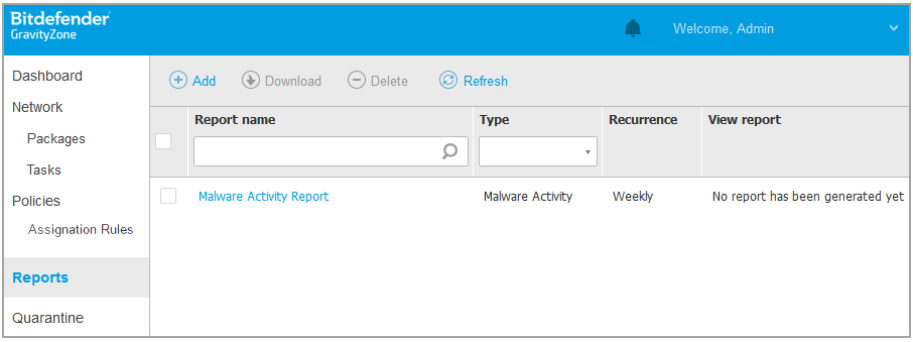
5. Настройка периодичности отчетов:
   - Нажмите **Сейчас**, чтобы создать мгновенный отчет.
   - Выберите **По расписанию**, чтобы настроить автоматическую генерацию отчета через желаемый интервал времени:
     - Почасовой, с указанием интервала между часами.
     - Ежедневный. В этом случае вы также можете установить время начала (часы и минуты).
     - Еженедельный, в указанные дни недели и в заданное время начала (часы и минуты).
     - Ежемесячный, в указанный день каждого месяца и в заданное время (часы и минуты).
6. Для большинства типов отчетов вам необходимо указать интервал времени, к которому относятся обрабатываемые данные. В отчете будут отображаться данные только за выбранный период времени.
7. Некоторые типы отчетов предоставляют возможность фильтрации, чтобы помочь вам легче найти интересующую вас информацию. Используйте параметры фильтрации в разделе **Показать** для получения только необходимой информации.

   Например, для отчета **Статус обновления** вы можете выбрать для просмотра только список сетевых объектов, которые не обновлены, или те, которые должны быть перезагружены для завершения обновлений.
8. **Доставка**. Чтобы получить отчет по расписанию по электронной почте, установите соответствующий флажок. Введите адрес электронной почты, который вы хотите, в поле ниже. По умолчанию, письмо содержит архив с двумя файлами отчета (PDF и CSV). Используйте флажки в разделе **Прикрепить файлы** для настройки - какие файлы и как отправлять их по электронной почте.
9. **Выберите цель**. Прокрутите вниз, чтобы выбрать объекты отчета. Выберите одну или несколько групп конечных точек, которые вы хотите включить в отчет.
10. В зависимости от выбранной переодичности, нажмите **Создать**, чтобы создать мгновенный отчет или **Сохранить**, чтобы создать отчет по расписанию.

- Мгновенный отчет будет отображен сразу после нажатия кнопки **Создать**. Время, необходимое для создания отчетов, варьируется в зависимости от количества управляемых объектов сети. Дождитесь завершения создания выбранного отчета.
- Запланированный отчет будет отображаться в списке на странице **Отчеты**. После того, как экземпляр отчета был создан, вы можете просмотреть отчет, нажав на соответствующую ссылку в колонке **Посмотреть отчет** на странице **Отчеты**.

12.3. Просмотр и управление отчетами по расписанию

Чтобы просматривать и управлять запланированными отчетами, перейдите на страницу **Отчеты**.



Страница отчетов

Все отчеты по расписанию отображаются в таблице вместе с полезной информацией о них:

- Имя и тип отчета
- Периодичность отчета
- Последний созданный экземпляр.

Примечание
Отчеты по расписанию доступны только для пользователя, который их создал.

Чтобы отсортировать отчеты по определенному столбцу, просто нажмите на заголовок нужного столбца. Щелкните заголовок столбца еще раз, чтобы изменить порядок сортировки.

Чтобы быстро найти то, что вы ищете, используйте окна поиска или параметры фильтрации под заголовками столбцов.

Чтобы очистить поле поиска, поместите в него курсор и нажмите на иконку × **Удалить**.

Чтобы быть уверенным, что отображается актуальная информация, нажмите кнопку **Обновить** в верхней части таблицы.

12.3.1. Просмотр отчетов

Чтобы просмотреть отчет:

1. Перейдите на страницу **Отчеты**.
2. Сортируйте отчеты по названию, типу или периодичности, чтобы быстрее найти нужный отчет.
3. Нажмите на соответствующую ссылку в колонке **Посмотреть отчет** для отображения отчета. Отобразится самый последний экземпляр отчета.

   Для просмотра всех экземпляров отчета, обратитесь к«Сохранение отчетов» (p. 459)

Все отчеты содержат краткое содержание (верхняя часть страницы отчета) и подробный раздел (нижняя часть страницы отчета).

- Раздел краткого содержания предоставляет вам статистические данные (круговые диаграммы и графики) для всех выбранных объектов сети, а также общую информацию об отчете, такую как отчетный период (если это применимо), цель отчета и т.д.
- Подробный раздел предоставляет вам информацию о каждом выбранном объекте сети.

Примечание

- Для настройки информации, отображаемой на графике, нажмите на записи легенды, чтобы показать или скрыть выбранные данные.
- Нажмите на графическую область (область круговой диаграммы, прямоугольной), которая вам нужна, чтобы посмотреть в таблице относящуюся к ней информацию.

12.3.2. Редактирование отчетов по расписанию

Примечание
При редактировании отчетов по расписанию, любые обновления будут применены, начиная со следующего запуска отчета. Изменения не затронут отчеты, сгенерированные ранее.

Чтобы изменить настройки отчетов по расписанию:

1. Перейдите на страницу **Отчеты**.
2. Нажмите на имя отчета.
3. Измените необходимые настройки отчета. Вы можете изменить следующее:
   - **Имя отчета.** Выберите подходящее имя для отчета, чтобы вам было проще понимать о чем он. При выборе имени учитывайте тип отчета, его назначение и возможности параметров отчета. Отчетам, которые генерируются по расписанию, имя дается позже.
   - **Периодичность отчетов (по расписанию).** Вы можете запланировать отчеты, чтобы они создавались каждый час (точный часовой интервал), ежедневно (в определенное время), еженедельно (в конкретный день недели и время) или ежемесячно (в конкретный день месяца и время). В зависимости от выбранного расписания, отчет будет включать только данные с последнего дня, недели или месяца соответственно.
   - **Настройки**
     - Вы можете запланировать отчет, чтобы он создавался автоматически каждый час (в определенный часовой интервал), ежедневно (в определенное время), еженедельно (в конкретный день недели и время) или ежемесячно (в конкретный день месяца и время). В зависимости от выбранного расписания, отчет будет включать только данные с последнего дня, недели или месяца соответственно.
     - Отчет будет включать только данные выбранного временного интервала. Вы можете изменить начальный интервал при следующем обращении.
     - Большинство отчетов предоставляют опции фильтрации, чтобы помочь вам легче найти нужную информацию. Когда вы

просматриваете отчет в консоли, будет доступна вся информация, независимо от выбранных опций. Если вы загрузите или отправите отчет, в PDF файл будет включено только краткое содержание и выбранная информация. Подробные данные отчета будут доступны только в CSV формате.

  - Вы можете выбрать получение отчета по электронной почте.

- **Выбрать цель.** Выбранная опция определяет тип объекта текущего отчета (как группы, так и индивидуального сетевого объекта). Нажмите на соответствующую ссылку, чтобы просмотреть объекты текущего отчета. Чтобы изменить их, выберите нужные группы или сетевые объекты, которые будут включены в отчет.

4. Нажмите **Сохранить**, чтобы применить изменения.

12.3.3. Удаление отчета по расписанию

Если отчет по расписанию больше не нужен, его лучше удалить. Удаление отчета по расписанию удалит все его экземпляры, автоматически сгенерированные до этого момента.

Чтобы удалить отчет по расписанию:

1. Перейдите на страницу **Отчеты**.
2. Выберите отчет, который вы хотите удалить.
3. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

12.4. Выполнение действий, основанные на данных отчета

В то время, как большинство отчетов показывают проблемы в вашей сети, некоторые из них также предлагают вам несколько вариантов действий для решения найденных проблем, с помощью всего одного нажатия кнопки мыши.

Чтобы исправить проблемы, отображаемые в отчете, нажмите соответствующую кнопку на панели инструментов над таблицей данных.

Примечание
Вам нужны соответствующие права на **управление сетью**, чтобы выполнить данные действия.

Следующие опции доступны для каждого отчета:

Состояние активности вредоносного ПО

- **Проверить зараженные цели**. Выполняет сконфигурированную задачу полной проверки объектов, которые все еще отображаются как зараженные.

Состояние обновления

- **Обновить**. Обновляет выбранных клиентов до последних доступных для них версий.

Состояние обновления версии продуктов

- **Обновить**. Заменяет старых клиентов конечных устройств на последние доступные версии продуктов.

12.5. Сохранение отчетов

По умолчанию, отчеты по расписанию автоматически сохраняются в Control Center.

Если вам необходимо более продолжительное время хранения отчетов, вы можете сохранить их на ваш компьютер. Сводный отчет будет доступен в формате PDF, в то время как сами подробные данные отчета будут доступны в формате CSV.

Существуют два способа сохранения отчетов:

- Экспортировать
- Загрузить

12.5.1. Экспорт отчетов

Чтобы экспортировать отчет на ваш компьютер:

1. Выберите формат и нажмите **Экспорт CSV** или **Экспорт PDF**.
2. В зависимости от настроек вашего браузера, файл может быть автоматически загружен в папку загрузки по умолчанию или окно загрузки запросит желаемое место, где вы должны указать папку назначения.

12.5.2. Загрузка отчетов

Архив отчетов содержит как сводный отчет (PDF), так и сами данные отчета (CSV).

Чтобы загрузить архив отчета:

1. Перейдите на страницу **Отчеты**.
2. Выберите отчет, который вы хотите сохранить.
3. Нажмите кнопку **Скачать** и выберите либо **Последний экземпляр**, чтобы загрузить последний сгенерированный отчет, либо **Полный архив**, чтобы загрузить архив, содержащий все отчеты.

   В зависимости от настроек вашего браузера, файл может быть автоматически загружен в папку загрузки по умолчанию или окно загрузки запросит желаемое место, где вы должны указать папку назначения.

12.6. Отправка отчетов

Вы можете отправлять отчеты по электронной почте, используя следующие параметры:

1. Чтобы отправить отчет, который вы просматриваете, по электронной почте, нажмите кнопку **Электронная почта**. Отчет будет отправлен на адрес электронной почты, связанный с вашей учетной записью.
2. Чтобы настроить расписание доставки отчетов по электронной почте:
   a. Перейдите на страницу **Отчеты**.
   b. Нажмите на название нужного отчета.
   c. Под **Настройки > Доставка**, выберите **Отправить по email** .
   d. Введите нужный адрес электронной почты в поле ниже. Можно добавить любое необходимое количество адресов электронной почты.
   e. Нажмите **Сохранить**.

> **Примечание**
> Только краткий отчет и график будут включены в файл PDF, отправляемый по электронной почте. Подробные данные отчета будут доступны в файле CSV.

Отчеты отправляются по электронной почте в виде архивов с расширением .zip.

12.7. Печать отчетов

Control Center в настоящее время не поддерживает функцию печати. Чтобы напечатать отчет, необходимо сначала сохранить его на свой компьютер.

13. КАРАНТИН

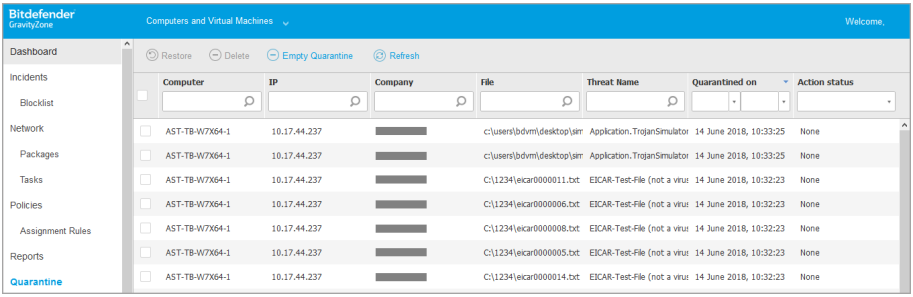
Карантин - это зашифрованная папка, которая содержит потенциально вредоносные файлы, такие как: подозрительно-вредоносные программы, подозрительно-зараженные программы или другие нежелательные файлы. Вирус, изолированный в карантинной зоне, не может причинить никакого вреда, так как его нельзя запустить или открыть для чтения.

GravityZone перемещает файлы в карантин в соответствии с политикой, установленной на конечных точках. По умолчанию, файлы, которые не могут быть вылечены, отправляются в карантин.

Объекты карантина сохраняются локально на каждой конечной точке.

13.1. Просмотр карантина

Страница **Карантин** предоставляет подробную информацию о файлах в карантине со всех конечных точек, которыми вы управляете.



Страница карантина

Информация о файлах, помещенных в карантин, отображается в виде таблицы. В зависимости от количества управляемых конечных точек, а также степени инфекции, таблица карантина может включать в себя большое количество записей. Таблица может содержать несколько страниц (по умолчанию, на странице отображается только 20 записей).

Для перемещения по страницам используйте кнопки навигации в нижней части таблицы. Чтобы изменить количество записей отображаемых на странице, введите другое значение в поле рядом с кнопками навигации.

Для лучшей наглядности данных, в которых вы заинтересованы, вы можете использовать поля поиска из заголовков столбцов, чтобы фильтровать отображаемые данные. Например, вы можете искать конкретную угрозу, обнаруженную в сети, или конкретный сетевой объект. Вы также можете нажимать на заголовки столбцов, чтобы отсортировать данные по определенному столбцу.

Чтобы быть уверенным, что отображается актуальная информация, нажмите кнопку **Обновить** в верхней части таблицы. Данная функция может быть полезной, если вы длительное время находитесь на странице.

13.2. Карантин компьютеров и виртуальных машин

По умолчанию файлы в карантине автоматически отправляются в Лаборатории Bitdefender для анализа исследователями Bitdefender. Если наличие вредоносного ПО подтверждено, выпускается сигнатура, которая позволит его удалить. Кроме того, файлы в карантине сканируются после каждого обновления баз данных сигнатур вредоносных программ. Очищенные файлы автоматически возвращаются на свое место. Данные возможности содержаться в каждой политике безопасности из раздела **Политики** и вы можете выбрать, следует ли сохранять файлы в карантине или лечить их. Для получения более подробной информации, обратитесь к «Карантин» (p. 197).

13.2.1. Просмотр подробной информации карантина

Таблица карантин предоставляет вам следующую информацию:

- Имя конечной точки, на которой угроза была обнаружена.
- IP-адрес конечной точки, на которой угроза была обнаружена.
- Путь к зараженному или подозрительному файлу на конечной точке, на которой он был обнаружен.
- Имя, которое дано вредоносной угрозе исследователями безопасности Bitdefender.
- Дата и время, когда файл был помещен в карантин.
- Состояние выбранного действия над перемещаемым в карантин файлом.

13.2.2. Управление файлами в карантине

В каждой среде параметры карантина отличаются:

- **Security for Endpoints** хранит файлы в карантине на каждом управляемом компьютере. Используя Control Center, у вас есть возможность, как удалять, так и восстанавливать отдельные файлы, помещенные в карантин.
- **Security for Virtualized Environments (Multi-Platform)** хранит файлы в карантине в каждой управляемой виртуальной машине. Используя Control Center, у вас есть возможность, как удалять, так и восстанавливать отдельные файлы, помещенные в карантин.

Восстановление файлов из карантина

В отдельных случаях вам, возможно, потребуется восстановить файлы из карантина в их исходное местоположение или в другое место. Одна из таких ситуаций, когда вам необходимо восстановить важные файлы, хранящиеся в зараженном архиве, который был перемещен в карантин.

Примечание
Восстановление файлов из карантина возможно только в средах, защищенных Security for Endpoints и Security for Virtualized Environments (Multi-Platform).

Для восстановления одного или более файлов, помещенных в карантин:

1. Перейдите на страницу **Карантин**.
2. Установите флажки, на соответствующих файлах в карантине, которые вы хотите восстановить.
3. Нажмите кнопку **Восстановить** в верхней части таблицы.
4. Выберите место, в которое вы хотите восстановить выбранные файлы (или оригинал, или другое место на компьютере).

   Если вы решите восстановить в другое место, необходимо ввести абсолютный путь в соответствующем поле.
5. Выберите **Автоматически добавлять исключения в политику**, чтобы исключить файлы, которые будут восстановлены при будущих проверках. Исключение распространяется на все политики, затрагивающие выбранные файлы, кроме политики по умолчанию, которая не может быть изменена.
6. Нажмите **Сохранить**, чтобы запустить задачу восстановления файлов. В колонке **Действие** вы можете наблюдать статус выполнения.
7. Запрашиваемое действие сразу же отправляется на объекты конечных точек или как только конечные точки появятся в сети.

Вы можете просмотреть детали о выполнении действий на странице **Задачи**. После того, как файл будет восстановлен, соответствующая запись исчезнет из таблицы карантина.

Автоматическое удаление файлов из карантина

По умолчанию файлы в карантине, созданные более 30 дней назад, удаляются автоматически. Этот параметр может быть изменен путем редактирования политики, назначаемой управляемым конечным точкам.

Чтобы изменить интервал автоматического удаления файлов, помещенных в карантин:

1. Перейдите на страницу **Политики**.
2. Найдите политику, назначенную конечным точкам, на которых вы хотите изменить настройку, и нажмите на ее имя.
3. Перейдите на страницу **Антивредоносное ПО > Настройки**.
4. В разделе **Карантин** выберите количество дней, после которого файлы будут удалены.
5. Нажмите **Сохранить**, чтобы применить изменения.

Руководство по удалению файлов из карантина

Если вы хотите вручную удалить файлы из карантина, вы должны сначала убедиться, что файлы, которые вы выбрали для удаления, больше не нужны.

В реальности весь файл может быть вредоносной программой. Если ваше исследование привело к такой ситуации, вы можете изучить карантин на предмет конкретной угрозы и удалить ее из карантина.

Чтобы удалить один или несколько файлов из карантина:

1. Перейдите на страницу **Карантин**.
2. Установите флажки на соответствующих файлах в карантине, которые вы хотите удалить.
3. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы. Вы должны будете подтвердить ваши действия, нажав **Да**.

   В колонке **Действие** вы можете наблюдать статус выполнения.

Требуемое действие направляется на выбранные сетевые объекты сразу же или как только они появятся в сети. После того, как файл будет удален, соответствующая запись исчезнет из таблицы карантина.

Очистка карантина

Чтобы удалить все зараженные объекты:

1. Перейдите на страницу **Карантин**.
2. Нажмите кнопку **Очистить Карантин**.

Все записи из таблицы карантина очищаются. Требуемое действие направляется на выбранные сетевые объекты сразу же или как только они появятся в сети.

13.3. Карантин серверов Exchange

Карантин Exchange содержит электронные письма и вложения. Модуль защиты от вредоносных программ отправляет в карантин вложения электронной почты, в то время как антиспам, фильтрация контента и вложений, отправляет в карантин все электронное письмо.

Примечание
Пожалуйста, обратите внимание, что карантин для серверов Exchange требует дополнительное дисковое пространство на разделе, где установлен агент безопасности. Размер карантина зависит от количества хранящихся элементов и их размера.

13.3.1. Просмотр подробной информации карантина

Страница **Карантин** предлагает вам подробную информацию об объектах в карантине из всех Exchange серверов в вашей организации. Информация доступна в таблице карантина и в окне описания каждого объекта.

Таблица карантин предоставляет вам следующую информацию:

- **Тема.** Тема сообщения на карантине.
- **Отправитель.** Адрес электронной почты отправителя, который отображается в поле заголовка электронной почты **From**.
- **Получатели.** Список получателей, которые отображаются в полях заголовков сообщений электронной почты **To** и **Cc**.

- **Реальные получатели.** Список отдельных адресов электронной почты пользователей, которым предназначалась доставка письма, прежде чем попасть в карантин.
- **Статус.** Состояние объекта после того, как он был просканирован. Статус показывает, помечено ли письмо как спам или содержит нежелательный контент, или вложение зараженно вредоносной программой, подозревается в инфицировании, нежелательное или несканируемое.
- **Имя вредоносного ПО.** Имя, данное вредоносной угрозе, исследователями безопасности Bitdefender.
- **Имя сервера.** Имя сервера, на котором угроза была обнаружена.
- **В карантине.** Дата и время, когда объект был помещен в карантин.
- **Статус действия.** Статус действий над объектами в карантине. Вы можете быстро просмотреть состояние действия - в обработке или действие не удалось выполнить.

Примечание

- Колонки **Реальные получатели**, **Имя вредоносного ПО** и **Имя сервера** скрыты по умолчанию от просмотра.
- Когда несколько вложений от одного адреса электронной почты отправлены в карантин, таблица карантина показывает отдельно каждое вложение.

Чтобы настроить детали параметров карантина, отображающихся в таблице:

1. Нажмите кнопку **Столбцы** в правой верхней части таблицы.
2. Выберите столбцы, которые вы хотите отобразить.

   Чтобы вернуться к просмотру столбцов по умолчанию нажмите кнопку **Сбросить**.

Вы можете получить более подробную информацию, нажав на ссылку **Тема**, соответствующую каждому объекту. Окно **Сведения об объекте** предоставляет вам следующую информацию:

- **Объект в карантине.** Тип объекта в карантине, который может быть как электронной почтой, так и вложением.
- **В карантине.** Дата и время, когда объект был помещен в карантин.

- **Статус.** Состояние объекта после того, как он был просканирован. Статус показывает, помечено ли письмо как спам или содержит нежелательный контент, или вложение зараженно вредоносной программой, подозревается в инфицировании, нежелательное или несканируемое.
- **Имя вложения.** Имя файла вложения обнаруженного защитой от вредоносных программ или модулем фильтрации вложений.
- **Имя вредоносного ПО.** Имя, данное вредоносной угрозе, исследователями безопасности Bitdefender. Эта информация доступна, только если объект был заражен.
- **Точка обнаружения.** Объект обнаружен или на транспортном уровне, или в почтовом ящике, или в общей папке хранилища Exchange.
- **Соответствующее правило.** Правило политики, определившее угрозу.
- **Сервер.** Имя сервера, где была обнаружена угроза.
- **IP отправителя.** IP-адрес отправителя.
- **Отправитель (От).** Адрес электронной почты отправителя, который отображается в поле заголовка электронной почты **От**.
- **Получатели.** Список получателей, которые отображаются в полях заголовков сообщений электронной почты **To** и **Cc**.
- **Реальные получатели.** Список отдельных адресов электронной почты пользователей, которым предназначалась доставка письма, прежде чем попасть в карантин.
- **Тема.** Тема сообщения на карантине.

Примечание
Знак многоточия в конце текста указывает, что часть текста опущена. В этом случае, наведите курсор мыши на текст, чтобы просмотреть его весь в виде всплывающей подсказки.

13.3.2. Объекты на карантине

Сообщения электронной почты и файлы, помещенные в карантин модулем защиты Exchange, хранятся локально на сервере в виде зашифрованных файлов. С помощью Центра управления вы имеете возможность восстановить помещенные в карантин сообщения электронной почты, а также удалять или сохранять любые файлы или электронные письма, помещенные в карантин.

Восстановление электронных писем из карантина

Если вы решили, что электронная почта в карантине не представляет угрозы, вы можете извлечь ее из карантина. Используя веб-службы Exchange, защитник Exchange-сервера отправляет электронное письмо, помещаемое в карантин, в виде вложения по электронной почте для уведомлений Bitdefender.

Примечание
Вы можете восстановить только электронные письма. Для восстановления вложения из карантина, вы должны сохранить его в локальную папку на сервере Exchange.

Для восстановления одного или нескольких писем:

1. Перейдите на страницу **Карантин**.
2. Выберите **Exchange** из меню выбора в верхней части страницы.
3. Установите флажки на соответствующих электронных письмах, которые вы хотите восстановить.
4. Нажмите кнопку **Восстановить** в верхней части таблицы. Появится окно **Восстановить учетные данные**.
5. Выберите учетные данные пользователя Exchange, уполномоченного отправлять восстановленные электронные письма. Если учетные данные, которые вы собираетесь использовать, новые, в первую очередь, вы должны их добавить в диспетчер учетных данных.

   Чтобы добавить необходимые учетные данные:

   a. Введите необходимую информацию в соответствующие поля заголовка таблицы:
      - Имя пользователя и пароль пользователя Exchange.

        Примечание
        Имя пользователя должно включать имя домена, например, `user@domain` или `domain\user`.

      - Адрес электронной почты пользователя Exchange, необходимый только тогда, когда адрес электронной почты отличается от имени пользователя.

- Ссылка Exchange Web Services (EWS), необходимая если автообнаружение Exchange не работает. Это, как правило, происходит в случае с пограничными транспортными серверами в демилитаризованной зоне.

b. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Новый набор учетных данных будет добавлен в таблицу.

6. Нажмите кнопку **Восстановить**. Появится окно подтверждения.

   Запрашиваемое действие сразу направляется на выбранные серверы. После того, как электронная почта восстанавливается, она также удаляется и из карантина, при этом соответствующая запись исчезает из таблицы карантина.

   Вы можете проверить состояние процесса восстановления в любом из этих разделов:

   - **Статус действия** в столбце таблицы карантина.
   - Страница **Сеть > Задачи**.

Сохранение файлов в карантине

Если вы хотите изучить или восстановить данные из карантина, вы можете сохранить файлы в локальную папку на сервере Exchange. Bitdefender Endpoint Security Tools расшифрует файлы и сохранит их в указанном месте.

Чтобы сохранить один или несколько файлов в карантине:

1. Перейдите на страницу **Карантин**.
2. Выберите **Exchange** из меню выбора в верхней части страницы.
3. Отфильтруйте данные в таблице для просмотра всех файлов, которые вы хотите сохранить, введя поисковые термины в полях заголовков столбцов.
4. Установите флажки, на соответствующих файлах в карантине, которые вы хотите восстановить.
5. Нажмите кнопку **Сохранить** в верхней части таблицы.
6. Введите путь к папке на сервере Exchange. Если папка на сервере не существует, то она будет создана.

Важно
Вы должны исключить эту папку из сканирования файловой системы, в противном случае файлы будут перемещены в карантин компьютеров и виртуальных машин. Для получения более подробной информации, обратитесь к «Исключения» (p. 198).

7. Нажмите **Сохранить**. Появится окно подтверждения.

   В колонке **Статус действия** вы можете наблюдать статус выполнения. Вы так же можете просматривать статус выполнения на странице **Сеть > Задачи**.

Автоматическое удаление файлов из карантина

По умолчанию, файлы в карантине старше 15 дней удаляются автоматически. Вы можете изменить эту настройку, отредактировав политику, назначенную управляемому серверу Exchange.

Чтобы изменить интервал автоматического удаления файлов, помещенных в карантин:

1. Перейдите на страницу **Политики**.
2. Нажмите на название политики, назначенной серверу Exchange, которая вам необходима.
3. Перейдите на страницу **Защита Exchange > Общие**.
4. В разделе **Настройки** выберите количество дней, после которого файлы будут удалены.
5. Нажмите **Сохранить**, чтобы применить изменения.

Руководство по удалению файлов из карантина

Чтобы удалить один или несколько объектов из карантина:

1. Перейдите на страницу **Карантин**.
2. Выберите **Exchange** из меню выбора.
3. Установите флажки на соответствующие файлы, которые вы хотите удалить.
4. Нажмите кнопку **Удалить** в верхней части таблицы. Вы должны будете подтвердить ваши действия, нажав **Да**.

   В колонке **Статус действия** вы можете наблюдать статус выполнения.

Запрашиваемое действие сразу направляется на выбранные серверы. После того, как файл будет удален, соответствующая запись исчезнет из таблицы карантина.

Очистка карантина

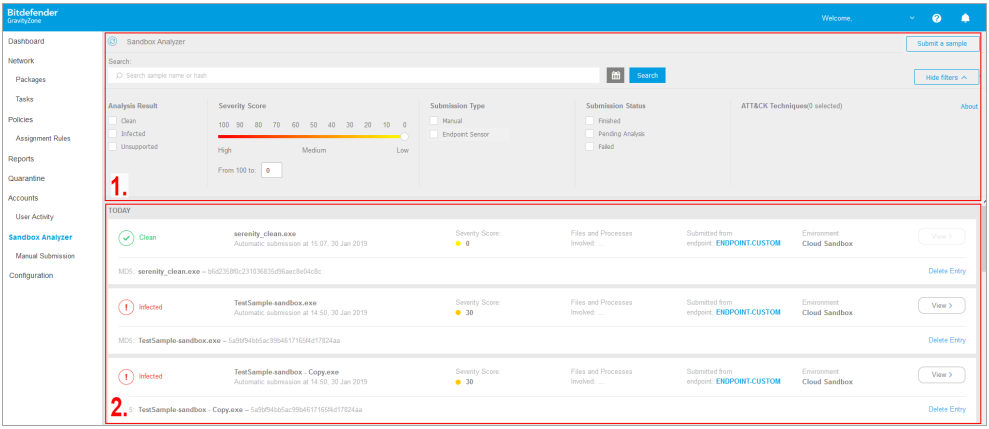
Чтобы удалить все зараженные объекты:

1. Перейдите на страницу **Карантин**.
2. Выберите **Exchange** в меню выбора.
3. Нажмите кнопку **Очистить Карантин**.

Все записи из таблицы карантина очищаются. Запрошенное действие немедленно отправляется объектам целевой сети.

14. ИСПОЛЬЗОВАНИЕ SANDBOX ANALYZER

Страница **Sandbox Analyzer** предоставляет собой единый интерфейс для просмотра, фильтрации и поиска автоматической и ручной отправки в среде песочницы. Страница **Sandbox Analyzer** состоит из двух областей:



Страница Sandbox Analyzer

1. **Область фильтрации** позволяет искать и фильтровать материалы по различным критериям: имя, хэш, дата, результат анализа, статус и методы MITER ATT&CK.
2. **Область карточек отправки** отображает все заявки в компактном формате с подробной информацией о каждой из них.

На странице Sandbox Analyzer вы можете сделать следующее:

- Фильтровать карточки отправки
- Просмотреть список отправленных объектов и подробную информацию об анализе
- Удалять карточки отправки
- Сделать ручную подачу

14.1. Фильтрация карточек отправки

Вот что вы можете сделать в области фильтров:

- Фильтровать заявки по различным критериям. Страница автоматически загрузит только карты событий безопасности, соответствующие выбранным критериям.
- Сбросьте фильтры, нажав кнопку **Очистить фильтры** .
- Скрыть вкладку фильтры, нажав кнопку **Скрыть фильтры** . Вы можете снова отобразить скрытые параметры, нажав **Показать фильтры** .

Вы можете фильтровать отправления Sandbox Analyzer по следующим критериям:

- **Пример имени и хэша (MD5)**. Введите в поле поиска часть или все имя или хэш искомого примера, а затем нажмите кнопку **Поиск** с правой стороны.
- **Дата**. Чтобы фильтровать по дате:
  1. Нажмите значок календаря , чтобы настроить временные рамки поиска.
  2. Определите интервал. Нажмите кнопки **ОТ** и **ДО** в верхней части календаря, чтобы выбрать даты, определяющие временной интервал. Вы также можете выбрать заранее определенный период из списка параметров справа относительно текущего времени (например, последние 30 дней).

     Вы также можете указать часы и минуты для каждой даты временного интервала, используя опции под календарем.
  3. Нажмите **ОК** , чтобы применить фильтр.
- **Результат анализа**. Выберите один или несколько из следующих параметров:
  - **Очистить** - образец безопасен.
  - **Зараженный** - образец опасен.
  - **Неподдерживаемый** - образец имеет формат, который Sandbox Analyzer не может проверить. Чтобы просмотреть полный список типов файлов и расширений, поддерживаемых Sandbox Analyzer, см. «Поддерживаемые Типы и Расширения Фалов для Отправки Вручную» (p. 512).

- **Оценка серьезности**. Значение указывает, насколько опасен образец по шкале от 100 до 0 (ноль). Чем выше оценка, тем опаснее образец. Степень серьезности применяется ко всем отправленным образцам, включая образцы со статусом **Чистый** или **Неподдерживаемый** .
- **Тип отправки**. Выберите один или несколько из следующих параметров:
  - **Вручную**. Sandbox Analyzer получил образец с помощью опции **Отправка вручную**.
  - **Датчик конечной точки**. Bitdefender Endpoint Security Tools отправил образец в Sandbox Analyzer на основе параметров политики.
- **Сведения передачи**. Установите один или несколько из следующих флажков:
  - **Выполнено** - Sandbox Analyzer предоставил результат анализа.
  - **В ожидании анализа** - Sandbox Analyzer проверяет образец.
  - **Ошибка** - Sandbox Analyzer не смог проверить образец.
- **ATT&CK techniques**. Эта опция фильтрации объединяет базу знаний MITRE's ATT&CK если это применимо. Значения методов ATT&CK меняются динамически в зависимости от событий безопасности.

  Нажмите ссылку **О программе** , чтобы открыть ATT&CK Matrix в новой вкладке.

14.2. Просмотр подробностей анализа

На странице **Sandbox Analyzer** отображаются карточки отправки по дням, в обратном хронологическом порядке. Карточки для подачи содержат следующие данные:

- Результат анализа
- Имя образца
- Тип отправки
- Оценка серьезности
- Задействованные файлы и процессы
- Детонационная среда
- Значение хэша (MD5)
- ATT&CK techniques
- Статус отправки, когда результат недоступен

Каждая карта подачи содержит ссылку на подробный отчет об анализе HTML, если таковой имеется. Чтобы открыть отчет, нажмите кнопку **Вид** с правой стороны карточки.

Отчет в формате HTML предоставляет обширную информацию, организованную на нескольких уровнях, с описательным текстом, графикой и снимками экрана, которые иллюстрируют поведение образца в среде детонации. Вот что вы можете узнать из HTML-отчета Sandbox Analyzer:

- Общие данные об анализируемой выборке, такие как: название и классификация вредоносного ПО, данные о представлении (имя файла, тип и размер, хэш, время отправки и продолжительность анализа).
- Результаты поведенческого анализа, которые включают все события безопасности, зафиксированные во время детонации, организованы в секции. К событиям безопасности относятся:
  - Запись / удаление / перемещение / дублирование / замена файлов в системе и на съемных дисках.
  - представление недавно созданных файлов.
  - Изменения в файловой системе.
  - Изменения в приложениях, запущенных внутри виртуальной машины.
  - Изменения в панели задач Windows и в меню «Пуск».
  - Создание / завершение / вброс процессов.
  - Запись / удаление ключей реестра.
  - Создание объектов мьютекса.
  - Создание / запуск / остановка / изменение / запрос / удаление служб.
  - Изменение настроек безопасности браузера.
  - Изменение настроек экрана проводника Windows.
  - Добавление файлов в список исключений брандмауэра.
  - Изменение сетевых настроек.
  - Включение выполнения при запуске системы.
  - Подключение к удаленному хосту.
  - Доступ к определенным доменам.
  - Перенос данных в определенные области и из них.
  - Доступ к URL-адресам, IP-адресам и портам через различные протоколы связи.
  - Проверка индикаторов виртуальной среды.
  - Проверка индикаторов инструментов мониторинга.
  - Создание моментальных снимков.
  - SSDT, IDT, IRP-захваты.

- Сброс памяти для подозрительных процессов.
- Вызов функций API Windows.
- Становится неактивным в течение определенного периода времени, чтобы отложить выполнение.
- Создание файлов с действиями, которые должны выполняться через определенные промежутки времени.

Важно
Доклады HTML доступны только на английском языке, несмотря на то, какой язык используется в GravityZone Control Center.

14.3. Удаление карточек подачи

Чтобы удалить карточку отправки, которая Вам больше не нужна:

1. Перейдите к карточке отправки, которую Вы хотите удалить.
2. Нажмите **Удалить запись** в левой части карточки.
3. Нажмите **Да**, чтобы подтвердить выбор.

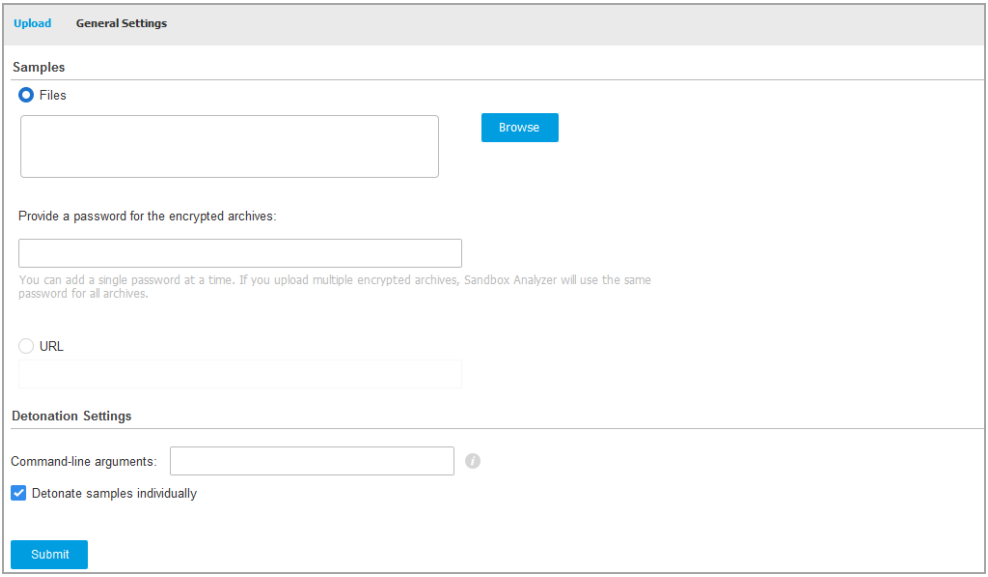
Примечание
Вы удалите только карту отправки, выполнив следующие действия. Информация об отправке по-прежнему доступна в отчете **Sandbox Analyzer Результаты (устарело)** . Однако этот отчет будет по-прежнему поддерживаться только в течение ограниченного периода времени.

14.4. Manual Submission

В **Sandbox Analyzer > Ручная отправка** Вы можете отправить образцы подозрительных объектов в Sandbox Analyzer, чтобы определить, являются ли они угрозами или безвредными файлами. Вы также можете перейти на страницу **Отправка вручную**, нажав кнопку **Отправить образец** в верхнем правом углу области фильтрации на странице Sandbox Analyzer.

Примечание
Sandbox Analyzer Ручное управление совместимо о всеми веб-браузерами, требуемыми Control Center, кроме Internet Explorer 9. Чтобы отправить объекты в Sandbox Analyzer, войдите в Control Center с помощью любого другого поддерживаемого веб-браузера, указанного в «Подключение к Control Center» (p. 18).

Для получения информации о том, как Sandbox Analyzer нарушает правила HIPAA, обратитесь к разделу "GravityZone и HIPAA" в Руководстве по установке.



Sandbox Analyzer > ручная отправка

Чтобы отправить образцы в Sandbox Analyzer:

1. На странице **Загрузка** в разделе **Образцы** выберите тип объекта:
   a. **Файлы**. Нажмите кнопку **Просмотреть** выберите объекты, которые вы хотите представить для поведенческого анализа. Для архивов, защищенных паролем, Вы можете определить один пароль для каждой загрузки сеанса в специальном поле. В процессе анализа Sandbox Analyzer применяет указанный пароль ко всем отправленным архивам.
   b. **URL**. Заполните соответствующие поля с любым URL, который вы хотите проанализировать. Вы можете отправить только один URL за сеанс.

      Примечание
      Ограничение по длине для детонированных URL-адресов составляет 1000 символов.

2. В разделе **Параметры детонации** настройка параметров анализа для текущей сессии:
   - **Параметры командной строки**. Добавьте столько аргументов командной строки, сколько вы хотите, разделенных пробелами, чтобы изменить работу определенных программ, таких как исполняемые файлы. Параметры командной строки применяются ко всем отправленным образцам во время анализа.
   - **Детонировать образцы индивидуально**. Установите флажок, чтобы файлы из пакета были проанализированы один за другим.
3. В разделе **Профиль детонации** настройте уровень сложности поведенческого анализа, влияя на пропускную способность Sandbox Analyzer. Например, если установлено значение **Высокое**, Sandbox Analyzer будет выполнять более точный анализ на меньшем количестве образцов за тот же интервал, чем на **Среднее** или **Низкое**.
4. В разделе **Общие параметры** вы можете внести конфигурации, которые распространяются на все материалы руководства, независимо от сессии:
   a. **Лимит времени для образца детонации (минуты)**. Выделите фиксированное количество времени для завершения анализа образца. Значение по умолчанию составляет 4 минуты, но иногда анализ может занять больше времени. По истечении настроенного интервала времени Sandbox Analyzer прерывает анализ и генерирует отчет на основе данных, собранных до этого момента. Если проверка прервана до полного завершения, анализ может содержать неточные результаты.
   b. **Количество разрешенных повторных запусков**. В случае непредвиденных ошибок Sandbox Analyzer пытается взорвать образец, как настроено, до завершения анализа. Значение по умолчанию - 2. Это означает, что Sandbox Analyzer попытается еще два раза проверить образец в случае ошибки.
   c. **Предфильтрация** . Выберите этот параметр, чтобы исключить из детонации уже проанализированные образцы.
   d. **Доступ к интернету во время детонации**. Во время анализа некоторые образцы требуют подключения к Интернету для завершения анализа. Для лучшего результата, мы рекомендуем Вам оставить данную опцию включенной.
   e. Нажмите **Сохранить** чтобы сохранить изменения.

5. Вернитесь к разделу **Загрузка**.
6. Нажмите **Подтвердить**. Шкала загрузки показывает статус отправки.

   После представления, **Sandbox Analyzer** в разделе появится новая карта. Когда анализ будет завершен, карточка обеспечивает вердикт и соответствующие детали.

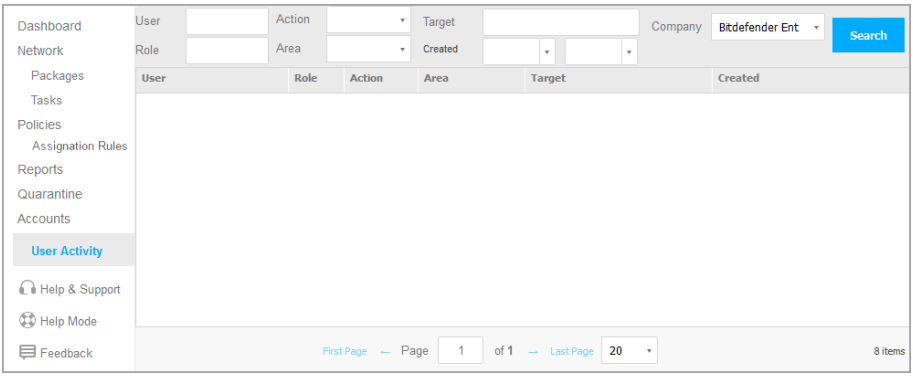
Примечание
Чтобы вручную отправить образцы к Sandbox Analyzer вы должны иметь права **Управления сетями**

15. ЖУРНАЛ АКТИВНОСТИ ПОЛЬЗОВАТЕЛЯ

Control Center регистрирует все операции и действия, выполняемые пользователями. В зависимости от уровня ваших администраторских разрешений, список действий пользователя может включать в себя следующие события:

- Вход и выход (в/из аккаунта)
- Создание, редактирование, переименование и удаление отчетов
- Добавление и удаление портлетов информационной панели
- Запуск, завершение, отмена и остановка процессов устранения неполадок на зараженных компьютерах
- Редактирование параметров аутентификации для учетных записей GravityZone.

Чтобы проверить записи активности пользователей, перейдите на страницу **Аккаунт > Активность пользователя**.



Страница действий пользователя

Для отображения записанных событий, которые вас интересуют, вы должны задать искомые слова. Заполните имеющиеся поля критериями поиска и нажмите кнопку **Поиск**. Все записи, соответствующие вашим критериям, будут отображены в таблице.

В столбцах таблицы будут представлены полезные сведения о перечисленных событиях:

- Имя пользователя, который совершил действие.

- Роль пользователя.
- Действие, которое вызвало событие.
- Тип объекта консоли, затронутый действием.
- Конкретный объект консоли, затронутый действием.
- Время, когда произошло событие.

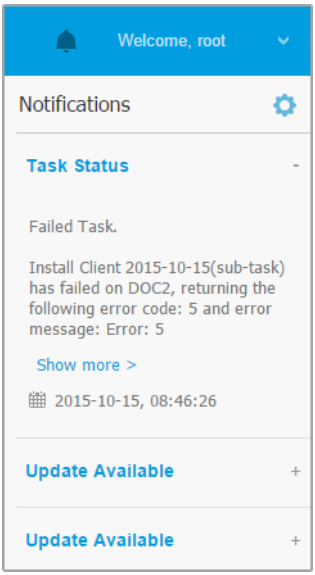
Чтобы отсортировать события по конкретному столбцу, просто нажмите на заголовок этого столбца. Щелкните заголовок столбца еще раз, чтобы изменить порядок сортировки.

Для просмотра подробной информации о событии, выберите его и проверьте раздел под таблицей.

16. ИСПОЛЬЗОВАНИЕ ИНСТРУМЕНТОВ

17. УВЕДОМЛЕНИЯ

В зависимости от событий, которые могут произойти в вашей сети, Control Center отобразит различные уведомления, чтобы проинформировать вас о состоянии безопасности вашей среды. Уведомления будут отображаться в **Область уведомлений**, расположенной в правой части Control Center.



Область уведомлений

Когда будут обнаружены новые события в сети, значок 11 в правом верхнем углу Control Center будет отображать количество недавно выявленных событий. Нажав на значок, отобразится область уведомлений, содержащая список обнаруженных событий.

17.1. Типы уведомлений

Список доступных типов уведомлений:

Вспышка вредоносного ПО

Это уведомление направляется пользователям при заражении не менее 5% устройств от числа всех управляемых объектов сети, зараженных одной и той же вредоносной программой.

Вы можете сконфигурировать порог срабатываний на вредоносное ПО в окне **Параметры уведомлений**. Для получения более подробной информации, обратитесь к «Настройка параметров уведомлений» (p. 493).

Угрозы, обнаруженные HyperDetect, выходят за рамки этого уведомления.

Истечение срока действия лицензии

Это уведомление отправляется за 30, 7 и 1 день до истечения срока действия лицензии.

Для просмотра этого уведомления необходимо иметь права **Управление компанией** .

Развертывание превысило лимит лицензии партнера

Это уведомление отправляется, когда все доступные лицензии использованы. В случае, если количество установок превышает лицензионный лимит, уведомление будет отображать нелицензированные конечные точки в течение последних 24 часов.

Для просмотра этого уведомления необходимо иметь права **Управление компанией** .

Срок действия лицензии подходит к концу

Это уведомление отправляется, когда использовано 90% имеющихся лицензий.

Для просмотра этого уведомления необходимо иметь права **Управление компанией** .

Достигнут лимит использования лицензий для серверов.

Это уведомление отправляется, когда количество защищаемых серверов достигает предела, указанного в вашем лицензионном ключе.

Для просмотра этого уведомления необходимо иметь права **Управление компанией** .

Лимит лицензирования серверов почти достигнут.

Это уведомление отправляется, когда использовано 90% имеющихся серверных лицензий.

Для просмотра этого уведомления необходимо иметь права **Управление компанией** .

Лимит использования лицензий Exchange достигнут

Это уведомление срабатывает каждый раз, когда количество защищаемых почтовых ящиков на сервере Exchange достигает предельного значения, указанного в лицензионном ключе.

Для просмотра этого уведомления необходимо иметь права **Управление компанией** .

Не верные учетные данные пользователя Exchange

Данное уведомление отправляется, когда задача сканирования по требованию не может быть запущена на выбранном сервере Exchange из-за неправильных учетных данных пользователя Exchange.

Состояние обновления версии продуктов

Это уведомление запускается еженедельно, если в сети обнаружены старые версии продукта.

Advanced Anti-Exploit

Это уведомление информирует вас, когда Advanced Anti-Exploit обнаружил попытки использования в вашей сети.

Событие Антифишинга

Это уведомление информирует вас каждый раз, когда агент конечного устройства блокирует несанкционированный доступ к известному фишинговому сайту. Это уведомление также содержит такие детали, как попытки конечного устройства получить доступ к небезопасным веб-сайтам (имя и IP-адрес), установленный агент или заблокированый URL.

События межсетевого экрана

Данное уведомление информирует вас каждый раз, когда модуль межсетевого экрана установленного агента блокирует какие-нибудь сетевые приложения или попытки сканирования портов, в соответствии с применяемой политикой безопасности.

События ATC/IDS

Это уведомление отправляется каждый раз, когда потенциально опасное приложение обнаружено и заблокировано на конечном устройстве в вашей сети. Вы найдете подробную информацию о типе приложения,

имени и пути, а также ID родительского процесса и его путь, и командную строку, которая запустила процесс в данном случае.

События контроля пользователя

Это уведомление срабатывает каждый раз, когда активность пользователя, такая как просмотр веб-страниц или используемое программное обеспечение, блокируется клиентом конечного устройства в соответствии с применяемой политикой безопасности.

События защиты данных

Это уведомление формируется каждый раз, когда трафик блокируется на конечном устройстве в соответствии с правилами защиты данных.

События модуля приложений

Это уведомление направляется каждый раз, когда модуль безопасности в установленном агенте отключается или включается.

События состояния Security Server

Этот тип уведомлений содержит информацию об изменениях статуса определенного Security Server, установленного в вашей сети. Изменение статуса Security Server может быть вызвано следующими причинами: сервер выключается или включается, выполняется обновление продукта, обновляются механизмы защиты и требуется перезагрузка.

Событие о перегрузке Security Server

Это уведомление отправляется, когда нагрузка при сканировании на Security Server в вашей сети превышает установленный порог.

События регистрации продуктов

Это уведомление информирует вас, когда статус регистрации агента, установленного в вашей сети, изменяется.

Аудит аутентификации

Это уведомление информирует вас, когда другая учетная записьGravityZone, исключая вашу собственную, была использована, чтобы войти в Control Center с нераспознанного устройства.

Вход в систему с нового устройства

Это уведомление сообщает вам, что ваша учетная запись GravityZone была использована, чтобы войти в Control Center с устройства, которое вы не использовали для этих целей ранее. Уведомление автоматически настраивается таким образом, чтобы передаваться как в Control Center, так и по электронной почте и только вы сможете просмотреть его.

Статус задачи

Данное уведомление предупредит вас, когда статус задания изменен или только при завершении задания, в соответствии с вашими настройками.

Вы также можете получить это уведомление для задач сканирования, запущенных через [NTSA_ SHORT].

Сервер обновлений устарел

Это уведомление отправляется, когда сервер обновлений в вашей сети имеет устаревшие механизмы защиты.

Событие сетевых инцидентов

Это уведомление отправляется каждый раз, когда модуль Network Attack Defense обнаруживает попытку атаки в вашей сети. Это уведомление также информирует вас о том, была ли предпринята попытка атаки извне сети или из скомпрометированной конечной точки в сети. Другие сведения включают данные о конечной точке, технике атаки, IP-адресе злоумышленника и действиях предпринятых Network Attack Defense.

Sandbox Analyzer обнаружение

Это уведомление будет появляться каждый раз, когда Sandbox Analyzer обнаружит новую угрозу среди среди представленных файлов. Вам предоставляются такие данные, как название компании, имя хоста или IP конечной точки, время и дата обнаружения, тип угрозы, путь, имя, размер файлов и действия по исправлению, принятые для каждого из них.

Примечание

Вы не будете получать уведомления о чистых проанализированных образцах. Информация о всех отправленных Вашей компанией образцах доступна в отчете **Результаты Sandbox Analyzer (Устаревшие)** Информация о всех отправленных Вашей компанией образцах также доступна в разделе **Sandbox Analyzer**, в главном меню Control Center.

активность по обнаружению гипервизора

Это уведомление информирует вас при обнаружении в сети любых вредоносных или незаблокированных событий. Это уведомление отправляется при каждом событии HyperDetect и содержит следующие данные:

- Сведения об уязвимой конечной точке (имя, IP-адрес, установленный агент)

- Тип и имя вредоносного по
- Зараженный путь к файлу. Для атак с меньшим количеством файлов предоставляется имя исполняемого файла, используемого в атаке.
- Состояние заражения
- Хэш SHA256 исполняемого вредоносного файла
- Тип предполагаемой атаки (целевая атака, нежелательная программа, эксплойты, программы-вымогатели, подозрительные файлы и сетевой трафик)
- Уровень обнаружения (Рекомендуемый, Нормальный, Интенсивный)
- Время и дата обнаружения

Вы можете просматривать сведения об инфекции и продолжать изучать проблему, создав отчет **Активность HyperDetect** на странице **Уведомления**. Для этого:

1. В Control Center, нажмите кнопку **Уведомления** чтобы отобразить область уведомлений.
2. Нажмите ссылку **Показать больше** в конце уведомления, чтобы открыть страницу **Уведомления**.
3. Нажмите кнопку **Просмотр отчета** в деталях уведомлений. Это действие открывает окно конфигурации отчета.
4. Если необходимо, проведите конфигурацию отчета. Для получения более подробной информации, обратитесь к «Создание отчетов» (p. 452).
5. Нажмите **Создать**.

Примечание
Чтобы избежать спама, вы будете получать максимум одно уведомление в час.

Проблема интеграции со службой каталогов Active Directory
Это уведомление информирует вас о проблемах, которые влияют на синхронизацию со службой каталогов Active Directory

Ошибка патча отсутствует
Это уведомление появляется,когда в конечных точках вашей сети отсутствуют 1 или 2 доступных патча.

GravityZone автоматически отправляет уведомление, содержащее все результаты за последние 24 часа, до даты уведомления. Уведомление отправляется всем пользователям.

Вы можете просмотреть какая конечная точка находится в этой ситуации, нажав кнопку **Просмотреть отчет** в деталях уведомления.

По умолчанию уведомление отсылает к исправлениям безопасности, но вы можете настроить его так, чтобы оно также сообщало вам о исправлениях, не относящихся к безопасности.

Новый инцидент

Это уведомление информирует Вас о появлении нового инцидента. После включения уведомления генерируются каждый раз, когда новый инцидент отображается в разделе **Инциденты** Центра управления. Для получения большей информации нажмите на **Название инцидента**.

Обнаружение программы-вымогателя

Это уведомление информирует вас, когда GravityZone обнаруживает атаку вымогателей в Вашей сети. Вам будет предоставлена подробная информация о целевой конечной точке, пользователе, который вошел в систему, источнике атаки, количестве зашифрованных файлов, времени и дате атаки.

На момент получения уведомления атака была уже заблокирована.

Ссылка в уведомлении перенаправит Вас на страницу **Активность вымогателей**, где Вы можете просмотреть список зашифрованных файлов и восстановить их, если это необходимо.

Хранение вредоносных программ

Это уведомление отправляется при обнаружении вредоносного ПО на устройстве хранения, совместимом с ICAP. Это уведомление создается при каждом обнаружении вредоносных программ и предоставляет сведения о зараженном устройстве хранения (имя, IP-адрес, тип), вредоносном ПО и времени обнаружения.

Функция устранения неполадок

Данное уведомление появится тогда, когда устранение неисправностей будет завершено. Вы можете просмотреть подробную информацию о типе и статусе события, цели устранения неполадок, месте хранения, в котором можно найти архив журналов, и другие сведения.

Изменен партнер

Данное уведомление Вас информирует, когда управляемая компания меняет партнера. Сведения включают тип лицензии, дату окончания подписки, автоматическое продление (если активировано), минимальное использование и включенные услуги для этой компании.

Для просмотра этого уведомления необходимо иметь права **Управление компанией** .

Политика срока действия пароля включена

Данное уведомление информирует Вас о сроке истечения пароля в Вашем аккаунте.

Напоминание о сроке действия пароля

Это уведомление отправляют 10 дней подряд до истечения срока действия пароля GravityZone, чтобы напомнить Вам о необходимости его смены. Для быстрого обновления пароля нажмите на **Мой аккаунт** кнопку уведомления Control Center.

Доступна блокировка аккаунта

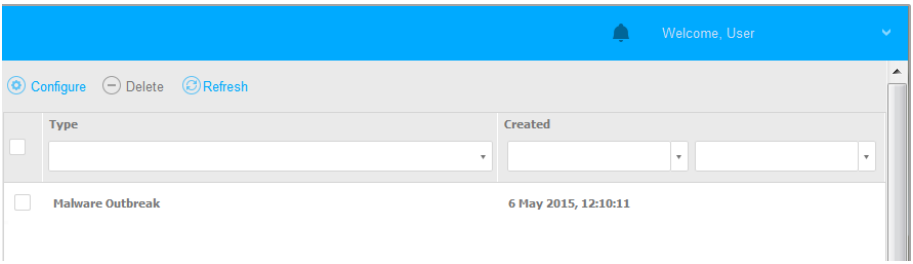
Это уведомление сообщает Вам о включении политики блокировки учетной записи для Вашего аккаунта.

Аккаунт заблокирован

Это уведомление отправляется по электронной почте, чтобы сообщить Вам о том, что его учетная запись была заблокирована из-за повторных попыток входа в систему с недействительными паролями.

17.2. Просмотр уведомлений

Для просмотра уведомлений нажмите кнопку **Уведомления** и далее нажмите **Посмотреть все уведомления**. Появится таблица, содержащая все уведомления.



Страница уведомлений

В зависимости от количества уведомлений, таблица может занимать несколько страниц (по умолчанию отображается по 20 записей на странице).

Для перемещения по страницам используйте кнопки навигации в нижней части таблицы.

Чтобы изменить количество записей отображаемых на странице, введите другое значение в поле рядом с кнопками навигации.

Если записей слишком много, вы можете использовать поисковые поля под заголовками столбцов или меню фильтра в верхней части таблицы, чтобы отфильтровать отображаемые данные.

- Чтобы отфильтровать уведомления, выберите тип уведомлений, которые вы хотите увидеть, в меню **Тип**. По желанию, можно выбрать временной интервал, в течение которого уведомления были сгенерированы, чтобы уменьшить количество записей в таблице, особенно при большом количестве сгенерированных уведомлений.
- Для просмотра деталей уведомления, нажмите на его имя в таблице. Раздел **Подробная информация** отображается ниже таблицы, где вы можете увидеть событие, которое сгенерировало уведомление.

17.3. Удаление уведомлений

Чтобы удалить уведомления:

1. Нажмите кнопку **Уведомления** в правой части панели меню, затем нажмите **Просмотреть все уведомления**. Появится таблица, содержащая все уведомления.
2. Выберите уведомления, которые вы хотите удалить.

3. Нажмите кнопку ⊖ **Удалить** в верхней части таблицы.

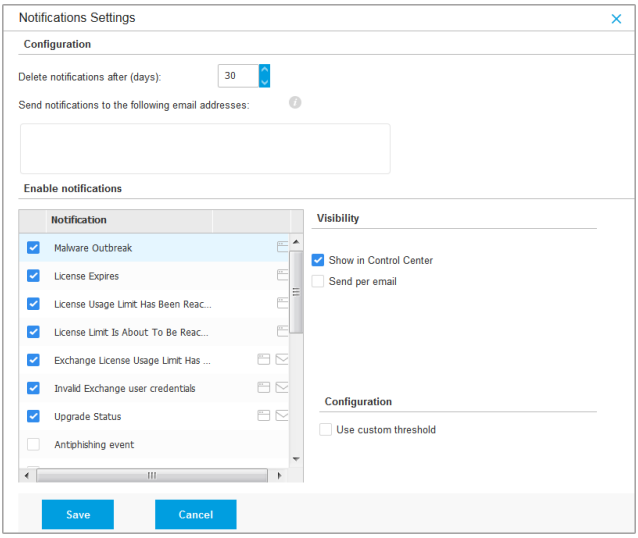
Вы также можете настроить уведомления для автоматического удаления после определенного количества дней. Для получения более подробной информации, обратитесь к «Настройка параметров уведомлений» (p. 493).

17.4. Настройка параметров уведомлений

Тип уведомлений для отправки и адреса электронной почты, на которые они отправляются, могут быть настроены для каждого пользователя.

Чтобы настроить параметры уведомлений:

1. Нажмите кнопку **Уведомления** в правой части панели меню, затем нажмите **Просмотреть все уведомления**. Появится таблица, содержащая все уведомления.
2. Нажмите кнопку ⚙ Настроить в верхней части таблицы. Отобразится окно **Настройки уведомлений**.



Настройки уведомлений

Примечание
Вы также можете получить доступ к окну **Параметры уведомлений** напрямую, используя значок **Настроить** в правом верхнем углу окна **Область уведомлений**.

3. В разделе **Настройки** вы можете задать следующие настройки:
   - Автоматическое удаление уведомлений по истечении определенного периода времени. Установите любое желаемое число от 1 до 365 в поле **Удалить уведомления через (дней)**.
   - Кроме того, вы можете отправлять уведомления определенным получателям по электронной почте. Введите адреса электронной почты в соответствующее поле, нажав `Enter` после каждого адреса.
4. В разделе **Включить уведомления** вы можете выбрать тип уведомлений, которые хотите получать от GravityZone. Вы также можете настроить видимость и параметры отправки индивидуально, для каждого типа уведомлений.

   Выберите желаемый тип уведомлений из списка. Для получения более подробной информации, обратитесь к «Типы уведомлений» (p. 484). Когда выбран тип уведомлений, вы можете настроить его конкретные параметры (если доступно) в правой части:

Видимость

- **Показ в Control Center** обозначает, что этот тип событий отображается в Control Center с помощью значка **Область уведомлений**.
- **Отправить по электронной почте** указывает, что этот тип событий будет также отправляться на некоторые адреса электронной почты. В этом случае вы должны ввести адреса электронной почты в выделенном поле, нажав `Enter` после каждого адреса.

Конфигурация

- **Использовать пользовательский порог** - позволяет определить порог для количества произошедших событий, после которого выбранные уведомления будут отправлены.

Например, уведомление о вспышках заражения вредоносным ПО отправляется по умолчанию пользователям, если не менее 5% всех управляемых объектов сети заражены одним и тем же вредоносным ПО. Чтобы изменить порог срабатывания о вспышках заражения, разрешите опцию **Использовать пользовательский порог**, затем введите желаемое значение в поле **Порог вспышки вредоносного ПО**.

- Для **Статус задачи**, вы можете выбрать тип статуса, который будет вызывать следующий тип уведомлений:
  - **Любой статус** - уведомляет каждый раз, когда задача Control Center завершена с любым статусом.
  - **Только незавершенные** - уведомляет каждый раз, когда задача Control Center завершилась неудачей.

5. Нажмите **Сохранить**.

18. ПОЛУЧЕНИЕ СПРАВКИ

Bitdefender стремится предоставить своим клиентам быструю и качественную техподдержку. Если у вас возникли проблемы или если у вас есть какие-либо вопросы о продуктах Bitdefender, перейдите в наш Онлайн центр поддержки. В нем доступны ресурсы, с помощью которых можно быстро найти решение или ответ. Или при необходимости можно обратиться в службу поддержки клиентов Bitdefender. Представители службы поддержки быстро ответят на все вопросы и окажут необходимую помощь.

Примечание
В центре техподдержки можно найти информацию о предоставляемых услугах техподдержки, а также правилах их предоставления.

18.1. Центр поддержки Bitdefender

Bitdefender Центр поддержки это раздел, где вы найдете всю необходимую помощь по продуктам Bitdefender.

Доступные ресурсы можно использовать для быстрого нахождения решения или ответа:

- Статьи базы знаний
- Форум поддержки Bitdefender
- Документация по продукту

Также можно воспользоваться поисковой системой для получения дополнительных сведений о компьютерной безопасности, продуктах Bitdefender и самой компании.

Статьи базы знаний

База знаний Bitdefender - онлайн хранилище информации о продуктах Bitdefender. Здесь хранятся в удобном для доступа формате отчеты о результатах текущих операций по технической поддержке и исправлению ошибок, выполняемых службой поддержки и разработки Bitdefender, а также статьи по предотвращению заражения вирусами, управлению решениями Bitdefender с подробными разъяснениями, а также другая информация.

База знаний Bitdefender открыта для общего доступа с возможностью свободного поиска. Bitdefender содержит обширную информацию,

предоставляя клиентам необходимые технические сведения. Все действующие информационные запросы или отчеты об ошибках, поступающие от клиентов Bitdefender, могут быть найдены в базе знаний Bitdefender, такие как отчеты по исправлениям, устранению неполадок и информационные статьи, дополняющие файлы справок продуктов.

База знаний Bitdefender для бизнес-продуктов доступна в любое время - http://www.bitdefender.com/support/business.html.

Форум поддержки Bitdefender

Форум техподдержки Bitdefender предоставляет пользователям Bitdefender простой способ не только получить необходимую помощь, но и помочь другим. Можно опубликовать любую проблему или вопрос, связанные с продуктом Bitdefender.

Специалисты Службы технической поддержки Bitdefender отслеживают новые сообщения на форуме, что позволяет своевременно реагировать на все вопросы пользователей. На форуме также есть возможность получить ответ или узнать о способах решения проблемы от более опытных пользователей Bitdefender.

Перед публикацией своего сообщения о проблеме или вопроса, выполните поиск похожих или связанных тем на форуме.

Форум техподдержки Bitdefender доступен по адресу http://forum.bitdefender.com, на пяти различных языках: английском, немецком, французском, испанском и румынском. Нажмите ссылку **Защита бизнеса**, чтобы перейти в раздел продуктов для бизнеса.

Документация по продукту

Документация по продукту является самым полным источником информации о продукте.

Самый простой способ получить документацию - перейти на страницу **Справка и поддержка** в Control Center. Нажмите свое имя пользователя в верхнем правом углу консоли, выберите **Справка и поддержка** , а затем ссылку интересующего вас руководства. Руководство откроется на новой вкладке вашего браузера.

18.2. Обращение за помощью

Вы можете обратиться за помощью в наш онлайн Центр поддержки. Заполните контактная форма и примите.

18.3. Использование инструментов поддержки

Инструменты поддержки GravityZone созданы, чтобы помочь пользователям и специалистам поддержки упростить предоставление необходимой информации для устранения неполадок. Запустите инструмент поддержки на действующих компьютерах и отправьте архив с информацией о выявленных неполадках в представительство поддержки Bitdefender.

18.3.1. Использование инструмента поддержки на операционных системах Windows

Запуск приложения Инструмент поддержки

Чтобы создать журнал на зараженном компьютере, используйте один из следующих способов:

- Командная строка

  Для любых проблем с BEST, установленным на компьютере.

- Проблема с установкой

  Для ситуаций, когда BEST не установлен на компьютере и установка завершается неудачно.

Метод командной строки

Используя командную строку, вы можете собирать журналы прямо с зараженного компьютера. Этот метод полезен в ситуациях, когда у вас нет доступа к Центру управления GravityZone или компьютер не взаимодействует с консолью.

1. Откройте командную строку с правами администратора.
2. Перейдите в папку установки продукта. Путь по умолчанию:

   ```
   C:\Program Files\Bitdefender\Endpoint Security
   ```

3. Соберите и сохраните журналы, выполнив эту команду:

```
Product.Support.Tool.exe collect
```

Журналы по умолчанию сохраняются в `C: \ Windows \ Temp .`

При желании, если вы хотите сохранить журнал средства поддержки в произвольном месте, используйте путь к параметру:

```
Product.Support.Tool.exe collect [path="<path-to-file>"]
```

Пример:

```
Product.Support.Tool.exe collect path="D:\Test"
```

Пока команда выполняется, вы можете заметить индикатор выполнения на экране. Когда процесс завершен, в выходных данных отображается имя архива, содержащего журналы, и его местоположение.

Чтобы отправить журналы в службу поддержки Bitdefender Enterprise, перейдите в `C:\Windows\Temp` или в пользовательское местоположение и найдите архивный файл с именем `ST_[computername]_[currentdate]`. Прикрепите архив к заявке в службу поддержки для дальнейшего устранения неполадок.

Проблема с установкой

1. Чтобы загрузить Инструмент поддержки BEST, нажмите здесь.
2. Запустите исполняемый файл от имени администратора. Появится окно.
3. Выберите место для сохранения архива журналов.

   Пока журналы собираются, вы увидите на экране индикатор выполнения. Когда процесс завершен, в выходных данных отображается имя архива и его местоположение.

Чтобы отправить журналы в службу поддержки Bitdefender Enterprise, перейдите в выбранное местоположение и найдите архивный файл с именем `ST_[computername]_[currentdate]`. Прикрепите архив к заявке в службу поддержки для дальнейшего устранения неполадок.

18.3.2. Использование инструмента поддержки на операционных системах Linux

Для операционных систем Linux инструмент поддержки интегрирован в агент безопасности Bitdefender.

Для сбора информации о системе Linux с использованием инструмента поддержки, запустите следующую команду:

```
# /opt/BitDefender/bin/bdconfigure
```

используя следующие доступные опции:

- `--help` составить список всех команд инструмента поддержки
- `enablelogs` для включения журналирования продукта и коммуникационного модуля (все сервисы будут автоматически перезапущены)
- `disablelogs` для отключения журналирования продукта и коммуникационного модуля (все сервисы будут автоматически перезапущены)
- `deliverall` чтобы создать:
  - Архив, содержащий журналы продукта и модуля связи, доставленный в папку `/tmp` в следующем формате: `bitdefender_machineName_timeStamp.tar.gz`.

    После того как создан архив:

    1. При отключении журналирования вам будет выдан запрос. При необходимости службы автоматически перезапустятся.
    2. При удалении журналов вам будет выдан соответствующий запрос.
- `deliverall -default` предоставляет такую же информацию, как и в предыдущей опции, но действия по умолчанию будут отображены в логах без запроса пользователя (журналы отключены и удалены).

Вы также можете запустить команду `/bdconfigure` прямо из пакета [BEST_SHORT] (полный или загрузчик) без установки продукта.

Для сообщения о проблеме GravityZone, воздействующей на вашу систему Linux, выполните следующие шаги, используя ранее описанные опции:

1. Включите журналирование продукта и коммуникационного модуля.
2. Попытайтесь воспроизвести проблему.
3. Отключите журналы.
4. Создайте архив журналов.
5. Откройте обращение в службу поддержки, используя форму, которая доступна на странице **Помощь &Поддержка** в Control Center, с описанием проблемы и прикрепленным архивом журналов.

Инструмент поддержки для Linux предоставляет следующую информацию:

- `etc`, `var/log`, `/var/crash` (если доступно) и `var/epag` папки из папки `/opt/BitDefender`, которые содержат журналы и настройки Bitdefender
- Файл `/var/log/BitDefender/bdinstall.log` содержит информацию по установке
- Файл `network.txt`, который содержит информацию о сетевых настройках / о доступности машин
- Файл `product.txt`, включая содержимое всех файлов `update.txt` из `/opt/BitDefender/var/lib/scan` и полный рекурсивный список всех файлов из `/opt/BitDefender`
- Файл `system.txt`, который содержит общую системную информацию (версия дистрибутива и ядра, доступная оперативная память и свободное место на жестком диске)
- Файл `users.txt`, который содержит информацию о пользователе
- Другую системную информацию, касающуюся продукта, такую как внешнее сетевое взаимодействие процессов и использование процессора
- Системные журналы

18.3.3. Использование инструментов поддержки на операционных системах Mac

При отправке запроса в группу технической поддержки Bitdefender, необходимо предоставить следующую информацию:

- Подробное описание проблемы, с которой вы столкнулись.

- Скриншот (если возможно) сообщения об ошибке, которое появляется.
- Журнал инструмента поддержки.

Чтобы собрать информацию о Mac-системе с помощью инструмента поддержки:

1. Скачайте ZIP-архив, содержащий инструмент поддержки.
2. Извлеките файл **BDProfiler. Tool** из архива.
3. Откройте окно терминала.
4. Перейдите к папке, содержащей файл **BDProfiler.tool**.

   Например:

   ```
   cd /Users/Bitdefender/Desktop;
   ```

5. Добавьте разрешение на выполнение файла:

   ```
   chmod +x BDProfiler.tool;
   ```

6. Запустите инструмент.

   Например:

   ```
   /Users/Bitdefender/Desktop/BDProfiler.tool;
   ```

7. Нажмите `Y` и введите пароль, когда появится запрос ввода пароля администратора.

   Подождите пару минут, пока инструмент не закончит создание журнала. Полученный файл архива (**Bitdefenderprofile_ output. Zip**) появится на рабочем столе.

18.4. Контактная информация

Эффективное взаимодействие с клиентами является залогом успешного бизнеса. За последние 18 лет Bitdefender удалось завоевать бесспорный авторитет среди своих клиентов и партнеров за счет опережения их ожиданий и постоянного улучшения отношений с ними. Мы будем рады ответить на

все ваши вопросы и решить ваши проблемы – не стесняйтесь, обратитесь к нам за помощью.

18.4.1. Адреса веб-сайтов

Отдел продаж: enterprisesales@bitdefender.com
Центр поддержки:http://www.bitdefender.com/support/business.html
Документация: gravityzone-docs@bitdefender.com
Местные дистрибьюторы:http://www.bitdefender.com/partners
Партнерские программы: partners@bitdefender.com
Отдел по связям со СМИ: pr@bitdefender.com
Вирусная лаборатория: virus_submission@bitdefender.com
Спам-лаборатория: spam_submission@bitdefender.com
Сообщение о нарушениях: abuse@bitdefender.com
Веб-сайт: http://www.bitdefender.com

18.4.2. Местные дистрибьюторы

Местные дистрибьюторы Bitdefender готовы ответить на все вопросы коммерческого и общего характера, находящиеся в их компетенции.

Чтобы найти дистрибьютора Bitdefender в вашей стране:

1. Перейдите к http://www.bitdefender.com/partners.
2. Перейдите к **Поиск партнеров**.
3. Контактная информация местных дистрибьюторов Bitdefender будет отображена автоматически. Если это не произошло, выберите вашу страну, чтобы просмотреть информацию.
4. Если не удалось найти дистрибьютора Bitdefender в вашей стране, свяжитесь с нами по адресу электронной почты enterprisesales@bitdefender.com.

18.4.3. Офисы Bitdefender

Офисы компании Bitdefender готовы ответить на все вопросы коммерческого и общего характера, находящиеся в их компетенции. Ниже приведены адреса и контактная информация офисов.

США

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Телефон (продажи & техническая поддержка): 1-954-776-6262
Продажи: sales@bitdefender.com
Сайт: http://www.bitdefender.com
Центр поддержки: http://www.bitdefender.com/support/business.html

Франция

Bitdefender
49, Rue de la Vanne
92120 Montrouge
Факс: +33 (0)1 47 35 07 09
Телефон: +33 (0)1 47 35 72 73
E-mail: b2b@bitdefender.fr
Сайт: http://www.bitdefender.fr
Центр поддержки: http://www.bitdefender.fr/support/business.html

Испания

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Факс: (+34) 93 217 91 28
Телефон (office & sales): (+34) 93 218 96 15
Телефон (техническая поддержка): (+34) 93 502 69 10
Продажи: comercial@bitdefender.es
Сайт: http://www.bitdefender.es
Центр поддержки: http://www.bitdefender.es/support/business.html

Германия

Bitdefender GmbH
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte

Deutschland
Телефон (office & sales): +49 (0) 2304 94 51 60
Телефон (техническая поддержка): +49 (0) 2304 99 93 004
Продажи: firmenkunden@bitdefender.de
Сайт: http://www.bitdefender.de
Центр поддержки: http://www.bitdefender.de/support/business.html

Великобритания и Ирландия

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Телефон (продажи & техническая поддержка): (+44) 203 695 3415
E-mail: info@bitdefender.co.uk
Продажи: sales@bitdefender.co.uk
Сайт: http://www.bitdefender.co.uk
Центр поддержки: http://www.bitdefender.co.uk/support/business.html

Румыния

BITDEFENDER SRL
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Факс: +40 21 2641799
Телефон (продажи & техническая поддержка): +40 21 2063470
Продажи: sales@bitdefender.ro
Сайт: http://www.bitdefender.ro
Центр поддержки: http://www.bitdefender.ro/support/business.html

Объединенные Арабские Эмираты

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Телефон (продажи & техническая поддержка): 00971-4-4588935 / 00971-4-4589186
Факс: 00971-4-44565047

Продажи: sales@bitdefender.com
Сайт: http://www.bitdefender.com
Центр поддержки: http://www.bitdefender.com/support/business.html

A. Приложения

A.1. Поддерживаемые типы файлов

Механизмы сканирования на наличие вредоносных программ, включенные в решения безопасности Bitdefender, могут сканировать все типы файлов, которые могут содержать угрозы. Список ниже включает наиболее распространенные типы файлов, которые анализируются.

{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;

```
xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf;
xsn; xtp; xz; z; zip; zl?; zoo
```

A.2. Типы сетевых объектов и статусы

A.2.1. Типы сетевых объектов

Все типы сетевых объектов доступны в разделе **Сеть** и представлены соответствующими значками.

Ниже в таблице приведены значки и описание для всех доступных типов сетевых объектов.

Значок	Тип
	Сетевая группа
	Компьютер
	Компьютер ретранслятор
	Компьютер интегратора Active Directory
	Компьютер сервера Exchange
	Компьютер ретранслятор сервера Exchange
	Виртуальная машина
	Виртуальная машина ретранслятора
	Золотой образ
	Виртуальная машина сервера Exchange
	Виртуальная машина ретранслятор сервера Exchange
	Security Server

A.2.2. Состояние сетевых объектов

Каждый сетевой объект может находится в различных состояниях, в зависимости от состояния управляемости, проблем безопасности, подключения и так далее. Ниже в таблице приведены значки всех возможных состояний и их описание.

Примечание
Таблица ниже содержит несколько общих примеров возможных состояний. Аналогичные состояния могу применяться (одиночные или комбинированные) ко всем типам сетевых объектов, таких как сетевые группы, компьютеры и так далее.

Значок	Состояние
	Виртуальная машина, офлайн, неуправляемая
	Виртуальная машина, онлайн, неуправляемая
	Виртуальная машина, онлайн, управляемая
	Виртуальная машина, онлайн, управляемая, с проблемами
	Виртуальная машина, Ожидает перезагрузки
	Виртуальная машина, приостановлена (Suspended)
	Виртуальная машина, удалена

A.3. Типы файлов приложений

Движки сканирования вредоносного ПО, включенные в решения безопасности Bitdefender, могут быть настроены на сканирование только файлов приложений (или программ). Файлы приложений более уязвимы для вирусных атак, чем другие типы файлов.

Эта категория включает в себя файлы со следующими расширениями:

```
386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt;
accdu; acl; acr; action; ade; adp; air; app; as; asd; asp;
awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl;
csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm;
dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv;
hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; iso; isu;
jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat;
mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms;
msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one;
onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm;
potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf;
prg; ps1; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx;
```

rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

A.4. Фильтрация вложений по типу файлов

Модуль управления контентом, предлагаемый Security for Exchange, может фильтровать вложения электронной почты в зависимости от типа файлов. Типы, доступные в Control Center, включают следующие расширения:

Исполняемые файлы

386; acm; ax; com; cpl; dll; drv; exe; flt; fon; lrc; ocx; scr; sys; vxd; x32

Образы

bmp; cal; dcx; drw; ds4; eps; gif; gx2; ico; img; jfif; jpe; jpeg; jpg; pat; pcx; pgm; png; psd; psp; rgb; sdr; sh3; shw; sym; tif; tiff; wpg

Мультимедиа

3g2; 3gg; asf; au; avi; mid; mmf; mov; mp3; mpeg; mpg; ogg; qt; ra; ram; rm; swf; wav; wpl

Архивы.

7z; ain; arc; arj; bz; bz2; cab; cpio; cru; crush; gz; hap; img; jar; lha; lzh; pak; ppz; rar; rpm; sit; snp; tar; tar.z; tb2; tbz2; tgz; ufa; z; zip; zoo

Электронные таблицы

fm3; ods; wk1; wk3; wks; xls; xlsx

Презентации

odp; pps; ppt; pptx

Документы

doc; docx; dtd; htm; html; odt; pcx; pdf; qxd; rtf; wks; wpf; ws; ws2; xml

A.5. Системные переменные

Некоторые из настроек, присутствующие в консоли, требуют указания путей на компьютерах. Желательно использовать системные переменные (в соответствующих случаях), чтобы быть уверенным, что путь действителен для всех нужных компьютеров.

Ниже приведен список предопределенных системных переменных:

`%ALLUSERSPROFILE%`

Папка профиля All Users. Типовой путь:

```
C:\Documents and Settings\All Users
```

`%APPDATA%`

Папка Application Data вошедшего пользователя. Типовой путь:

```
C:\Users\{username}\AppData\Roaming
```

`%LOCALAPPDATA%`

Временные файлы приложений. Типовой путь:

```
C:\Users\{username}\AppData\Local
```

`%PROGRAMFILES%`

Папка Program Files. Типовой путь `C:\Program Files`.

`%PROGRAMFILES(X86)%`

Папка Program Files для 32-битных приложений (на 64-битных системах). Типовой путь:

```
C:\Program Files (x86)
```

`%COMMONPROGRAMFILES%`

Папка Common Files. Типовой путь:

```
C:\Program Files\Common Files
```

`%COMMONPROGRAMFILES(X86)%`

Папка Common Files для 32-битных приложений (на 64-битных системах). Типовой путь:

```
C:\Program Files (x86)\Common Files
```

`%WINDIR%`

Каталог Windows или SYSROOT. Типовой путь `C:\Windows`.

`%USERPROFILE%`

Путь к папке профиля пользователя. Типовой путь:

`C:\Users\{username}`

В macOS папка профиля пользователя соответствует домашней папке. При настройке исключений используйте `$HOME` or `~`.

A.6. Объекты Sandbox Analyzer

A.6.1. Поддерживаемые Типы и Расширения Фалов для Отправки Вручную

Поддерживаются следующие расширения, которые могут быть проверены вручную в Sandbox Analyzer:

`Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.`

Sandbox Analyzer может обнаруживать вышеупомянутые типы файлов, если они включены в архивы следующих типов: `7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.`

A.6.2. Типы Файлов Поддерживаемые Предварительной Фильтрацией Контента при Автоматической Отправке

Предварительная фильтрация контента определит конкретный тип файла с помощью комбинации, которая включает в себя содержимое объекта и расширение. Это означает, что исполняемый файл с расширением `.tmp` будет распознан как приложение и, если он окажется подозрительным, будет отправлен в Sandbox Analyzer.

- Приложения - файлы формата PE32, включая, но не ограничиваясь следующими расширениями: `exe, dll, com`.
- Документы - файлы формата документа, включая, но не ограничиваясь следующими расширениями: `xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm, dotm, potm, potx, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf, pdf`.
- Сценарии: `ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe`.
- Архивы: `zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00`.
- Почту (сохраненную в файловой системе):`eml, tnef`.

A.6.3. Исключения По Умолчанию в Автоматической Отправке

`asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt`.

A.7. Сбор данных о человеческом риске

Мы позаботимся о временном сборе и хранении конфиденциальных данных исключительно на локальном уровне - на рабочей станции пользователя, с единственной целью повышения уровня оповещения о потенциальных угрозах, с которыми может столкнуться Ваша компания в результате нежелательного поведения пользователя. Мы не сохраняем личные данные, такие как имена пользователей и пароли в виде обычного текста, ни в одной облачной базе данных.

Локальные данные, которые мы собираем, периодически удаляются и могут включать в себя только хэши имен пользователей и паролей, общее количество опасных веб-сайтов, к которым был получен доступ за определенный период времени, а также URL некоторых из этих подозрительных веб-сайтов, а также IP-адреса их доменов.

В следующей таблице описывается поведение пользователей, которое отслеживается при помощи ERA, а также обработка и сбор данных пользователя.

Имя правила	Описание	Тип	Собранные данные
Простые учетные данные HTTP	Проверяет, отправил ли пользователь учетные данные через незащищенные HTTP-соединения с момента последнего сканирования.	Пароли	Проверяет, использует ли пользователь одни и те же пароли на разных внешних сайтах. Данный сценарий становится доступным, когда мы обнаруживаем минимум два внешних веб-сайта с тем же паролем.
Общий HTTP-пароль Внешний	Мы запускаем поверку в том случае, когда пользователь получает доступ к небезопасным веб-сайтам, а также сохраняем количество доступных веб-сайтов и соответсвующие временные отметки,	Пароли	Мы храним локально хэш паролей (формат CRC32), введенных на внешних сайтах, а также URL доступа, IP домена и имя пользователя.
Общий HTTP-пароль, внутренний с внешним	Проверяет, использует ли пользователь одинаковые пароли, общие и для внутренних и внешних веб-сайтов.	Пароли	Мы храним локально хэш паролей (формат CRC32), введенных на внешних и внутренних сайтах, а также URL доступа, IP домена.
Просмотр сайтов высокого риска	Осуществляется проверка в том случае, если пользователь просматривал сайты, помеченные как фишинг или мошенничество с момента последнего сканирования. Сценарий становится активным в случае,	браузер	Мы храним локально в течение определенного периода времени лишь те веб-сайты и их URL, которые могут представлять угрозу.

Имя правила	Описание	Тип	Собранные данные
	когда число посещенных небезопасных веб-сайтов превышает допустимое количество.		
Высокий уровень обнаружения	Проверяет, подвергался ли пользователь большому количеству угроз с момента последнего сканирования. Сценарий становится активным, когда количество угроз, распространяющихся на пользователя, превышает допустимое количество..	обнаружения	Мы храним локально количество обнаружений, сработавших в определенный период времени.
Заражение съемного устройства	Проверяет, подвергался ли пользователь угрозе со стороны съемного устройства (например, флэш-накопителя, внешнего жесткого диска) с момента последнего сканирования.	обнаружения	Мы храним локально обнаружения, сработавшие в определенные периоды времени, при источниках заражения (USB/CD/ISO файлы).
Заражение SMB	Проверяет, получил ли пользователь доступ к каким-либо вредоносным файлам через общую сетевую	обнаружения	Мы храним локально события доступа к файлам, полученные из общих сетевых папок или точек общего доступа.

Имя правила	Описание	Тип	Собранные данные
	папку с момента последнего сканирования.		
Заражение браузера	Проверяет, получил ли пользователь какие-либо вредоносные URL-адреса с момента последнего сканирования.	обнаружения	Мы храним локально зловредные/подозрительные URL и считаем их.
Высокий уровень обнаружения с течением времени.	Осуществляется проверка в том случае, если пользователь подвергается огромному количеству угроз в течение определенного периода времени.	обнаружения	Мы храним локально некоторое количество инфекций в течение определенного периода времени.
Общий HTTP-пароль Внешний	Осуществляется проверка в том случае, если пользователю не удается менять пароли периодически при входе на внешние веб-сайты.	Пароли	Мы храним локально: хэши паролей (формат CRC32), хэши имен пользователей и URL внешних веб-сайтов, которые вызвали это поведение, а также IP-адреса доменов.
Старый пароль пользователя	Проверяет, не изменял ли пользователь пароль для входа в учетную запись (локальную или доменную) в течение более 30 дней.	Пароли	Мы ничего не храним локально Мы осуществляем запрос функции Active Directory, которая возвращает пользователя к тому моменту, когда пароль был изменен в предыдущий раз.

Глоссарий

Anti-Detour

Обнаружение попыток обойти проверки безопасности для создания новых процессов

Anti-Meterpreter

Обнаружение попыток создания обратной оболочки путем сканирования страниц исполняемой памяти

Antimalware Scanning Storm

Интенсивное использование системных ресурсов, которое может происходить, когда антивирусное программное обеспечение сканирует одновременно нескольких виртуальных машин на одном физическом хосте.

Greyware-вирусы

Класс программных приложений между законным программным обеспечением и вредоносным ПО. Хотя они не так вредны, как вредоносное ПО, которое влияет на целостность системы, их поведение по-прежнему приводит к нежелательным ситуациям, таким как кража данных и несанкционированное использование, нежелательная реклама. Наиболее распространенными программными приложениями являются шпионское ПО и рекламное ПО .

IOR

Индикатор Риска относится к значению ключа реестра или данным конкретной системной настройке или к известной уязвимости приложения.

IP-адрес

Сокращение от Internet Protocol – Интернет-протокол – маршрутизируемый протокол семейства TCP/IP, отвечающий за адресацию, маршрутизацию, фрагментацию и повторную компоновку IP-пакетов.

ROP Незаконный вызов

Обнаруживает попытки перехвата потока кода, используя метод ROP,путем проверки инициаторов вызова чувствительных системных функций.

ROP Эмуляция
Злоумышленник пытается сделать страницы памяти для данных исполняемыми, а затем пытается выполнить их с помощью метода программирования, ориентированного на возврат (ROP).

ROP сделать стек исполняемым
Обнаружение попыток повредить стек, используя технику ROP, проверяя защиту страницы стека

ROP стек поворота
Обнаруживает попытки перехвата потока кода, использующих метод ROP, путем проверки местоположения стека.

Shellcode EAF (экспорт фильтрации адресов)
Обнаруживает попытки получения вредоносным кодом доступа к чувствительным системным функциям из экспорта DLL.

Shellcode Выполнение
Обнаружение попыток создания новых процессов или загрузки файлов, используя шеллкод

Shellcode угроза
Обнаружение попыток внедрения вредоносного кода путем проверки вновь созданных потоков

VBScript универсальный
Пытается использовать VBScript.

Windows Загрузчик
Это общее имя для программ, основная функция которых - загрузка содержимого для нежелательных или злонамеренных целей.

Библиотека загрузки shellcode
Обнаружение попыток выполнить код через сетевые пути, используя шеллкод

Боковое движение
злоумышленник исследует сеть, часто перемещаясь по нескольким системам, чтобы найти основную цель. Злоумышленник может использовать специальные инструменты для достижения цели. Например:

эксплойты с использованием командных инъекций, эксплойты Shellshock, эксплойты с двойным расширением.

Браузер
Веб-браузер – приложение, которое находит и выводит на экран веб-страницы.

Буткит
Буткит - это вредоносная программа, способная заражать главную загрузочную запись (MBR), загрузочную запись тома (VBR) или загрузочный сектор. Буткит остается активным даже после перезагрузки системы.

Веб-мошенничество
Веб-мошенничество включает в себя и другие виды мошенничества, помимо фишинга. Например, от веб-сайтов, представляющих поддельные компании, которые непосредственно не запрашивают конфиденциальную информацию, но вместо этого пытаются представиться в качестве законных предприятий и получить прибыль, обманывая людей в деловых отношениях с ними.

Вирусы-Вымогатели
Вредоносная программа, которая блокирует вас на вашем компьютере или блокирует доступ к файлам и приложениям. Вирусы-вымогатели будут требовать от вас определенную плату (выкуп) в обмен на ключ дешифрования, который позволяет получить доступ к вашему компьютеру или файлам.

Вредоносное ПО
Malware - обобщённый термин для программного обеспечения, который обозначает нанесения вреда - сокращение от "malicious software" (вредоносное программное обеспечение). Это не универсальное обозначение, но его популярность в качестве обобщённого термина для вирусов, троянских коней, червей и вредоносного мобильного кода постоянно растет.

Вредоносное ПО
Программа или часть кода, которая загружается в ваш компьютер без вашего ведома и запускается без вашего участия. Многие вирусы также

могут копировать себя. Все компьютерные вирусы создаются людьми. Очень легко написать простой вирус, который копирует себя снова и снова. Даже такой простой вирус очень опасен, так как он быстро использует всю свободную память и система зависает. Более опасные вирусы могут передавать себя по сети и прорываться через системы защиты.

Вредоносные веб-программы

Веб-вредоносное ПО представляет собой программное обеспечение, разработанное с вредоносной целью для работы на веб-страницах и веб-серверах. Веб - страницы могут содержать, распространять или даже загружать вредоносные программы на Ваш компьютер.

Вредоносный процесс

Разрушительная программа, которая может получить доступ к несанкционированным ресурсам

Доступ к учетным данным

злоумышленник крадет такие учетные данные, как имена пользователей и пароли, чтобы получить доступ к системам. Например: атаки методом перебора, эксплойты несанкционированной аутентификации, программы для кражи паролей.

Загрузочный вирус

Вирус, заражающий загрузочный сектор жесткого или гибкого диска. Попытка загрузиться с зараженной дискеты приводит к тому, что вирус активизируется в памяти. Каждый раз, когда вы загружаете систему с этого места, вирус будет активизироваться в памяти.

Загрузочный сектор:

Сектор в начале каждого диска, в котором хранится информация о структуре диска (размер сектора, размер кластера и т.д.) На загрузочном диске загрузочный сектор содержит программу, загружающую операционную систему.

Защита процесса LSASS

Защищает процесс LSASS от утечки секретной информации, такой как хеши паролей и настройки безопасности.

Клавиатурный шпион (Keylogger)

Клавиатурные шпионы — это приложения, которые регистрируют все, что вводится с клавиатуры.

Клавиатурные шпионы по сути не являются вредоносным ПО. Их можно использовать в законных целях, например для контроля за действиями сотрудников или детей. Однако все чаще они используются кибер-мошенниками в злонамеренных целях (например, для сбора частных данных, таких как учетные данные и номера карт социального страхования).

Командная строка

В командной строке пользователь вводит нужные команды на специальном командном языке.

Лазейки в системе (Backdoor)

Брешь в защите системы, специально оставленная разработчиками или специалистами по сопровождению. Это не всегда делается со злым умыслом: например, в некоторых операционных системах предусмотрены учетные записи, которые могут использоваться персоналом службы технической поддержки или программистами разработчика.

Ложное срабатывание

Событие «ложного срабатывания» появляется, когда программа считает зараженным файл, который таковым на самом деле не является.

Макро-вирус

Компьютерный вирус, который кодируется как встроенный в документ макрос. Многие приложения, такие как Microsoft Word и Excel, поддерживают сложные макро-языки.

Эти приложения позволяют встраивать макросы в документ и эти макросы выполняются всякий раз, когда вы открываете документ.

Мошенническое ПО

Эта категория включает в себя методы, предназначенные для автоматизации киберпреступности. Например, методы мошенничества: ядерные эксплойты, различные вредоносные программы, такие как трояны и боты.

Нарушение правил политики

Следующие типы угроз представляют собой нарушения политики в соответствии с правилами, которые устанавливает администратор:

- **Веб-категория с ограниченным доступом**: Доступный веб-адрес является частью веб-категории с ограниченным доступом.
- **Ограниченный веб-трафик**: указанный веб-трафик возник в течение ограниченного интервала времени.
- **Ограниченный веб-адрес**: доступ к веб-адресу ограничен в соответствии с применяемой политикой.
- **Ограниченный доступ к данным**: сообщалось о трафике данных, соответствующем правилам защиты данных.
- **Ограниченный веб-адрес**: доступ к приложению ограничен в соответствии с применяемой политикой.
- **Ограниченные вложения электронной почты**: электронное письмо содержит несколько вредоносных вложений с различными типами вредоносных программ.
- **Содержимое с ограниченным доступом**: электронное письмо содержит строки символов с ограниченным доступом в соответствии с применяемой политикой.
- **Тип вложения с ограниченным доступом**: электронное письмо содержит вложение с ограниченным доступом в соответствии с применяемой политикой.
- **Подключенное устройство**: устройство было подключено к конечной точке
- **Попытка сканирования порта**: обнаружена попытка сканирования порта.
- **Сетевой трафик, инициированный процессом**: исходящий сетевой трафик и процесс, который его инициировал, ограничены в соответствии с применяемой политикой.
- **Входящий сетевой трафик**: входящий сетевой трафик ограничен в соответствии с применяемой политикой.

Начальный доступ

Злоумышленник получает доступ в сеть различными способами, включая уязвимости общедоступных веб-серверов. Например: эксплойты для раскрытия информации, эксплойты SQL-инъекций, векторы заражения посредством скрытой загрузки.

Неэвристический анализ (Non-heuristic)

Этот метод проверки основан на использовании определенных сигнатур вирусов. Основное преимущество этого метода состоит в том, что его нельзя обмануть похожей на вирус программой, а, следовательно, не возникает ложное срабатывание.

Номеронабиратель

Термин дозвонщик используется для описания программы, которая использует модем компьютера для установления удаленного подключения через Интернет. Соединение создается путем набора заранее определенного телефонного номера и подключения к международным или местным телефонным номерам с премиальным тарифом. Программа может осуществлять несанкционированные подключения, минуя местного интернет-провайдера. Цель этой деятельности - увеличить телефонный счет жертв и в конечном итоге заставить их потерять деньги.

Область уведомлений

Область уведомлений впервые появилась в операционной системе Windows 95. Она расположена на панели задач Windows обычно в нижней части экрана рядом с часами и содержит маленькие значки, обеспечивающие быстрый доступ к таким функциям, как факс, принтер, модем, регулировка громкости и т. д Чтобы просмотреть подробную информацию о программе и ее настройки, просто дважды щелкните мышкой на значке.

Обнаружение

после проникновения злоумышленник пытается получить информацию о системах и внутренней сети, прежде чем решить, что делать дальше. Например: эксплойты выхода в файловую систему сервера, эксплойты выхода в файловую систему HTTP.

Обновления

Новая версия программного обеспечения или оборудования, разработанная на замену устаревшей версии этого продукта. Кроме того, многие обновления часто определяют, установлена ли на компьютере старая версия данного программного продукта. Если нет – обновление невозможно.

Bitdefender имеет свой собственный модуль обновления, который позволяет вручную проверять наличие обновлений или автоматически обновлять программные продукты.

Повышение прав

процессы, направленные на получение несанкционированных привилегий и доступа к ресурсам.

Подозрительные файлы и трафик сети

Подозрительными являются файлы с сомнительной репутацией. Данное ранжирование определяется многими факторами, среди которых можно назвать: наличие цифровой подписи, количество вхождений в компьютерных сетях, используемый упаковщик и т. д. Сетевой трафик воспринимается как подозрительный, если он отклоняется от шаблона. Например, ненадежный источник, запросы на подключение к необычным портам, увеличение использования полосы пропускания, случайное время соединения и т. д.

Полезная нагрузка flash

Обнаружение попыток выполнить вредоносный код в Flash Player путем сканирования объектов Flash в памяти

Полиморфный вирус

Вирус, изменяющий свою форму всякий раз, заражая новый файл. Поскольку у таких вирусов нет бинарной закономерности, их трудно обнаружить.

Порт

Компьютерный интерфейс, с помощью которого подключается внешнее устройство. У персональных компьютеров есть несколько видов портов. Внутри корпуса есть несколько портов для подключения дисководов, монитора и клавиатуры. Снаружи есть порты для подключения модемов, принтеров, мыши и других внешних устройств.

В сетях на базе протоколов TCP/IP и UDP, порт – это конечная точка логического подключения. Номер порта указывает на его тип. Например, порт номер 80 используется для HTTP трафика.

Потенциально нежелательное приложение (PUA)

Потенциально нежелательные приложения (PUA) это программы, которые могут быть нежелательными для ПК, а иногда и поставляться в комплекте с программным обеспечением бесплатного. Такие программы могут быть установлены без согласия (также называются рекламными) или включены по умолчанию в комплект экспресс-установки (как дополнение). Потенциальное воздействие этих программ заключается в показе всплывающих окон, установке нежелательных панелей инструментов в браузере по умолчанию или работе нескольких процессов в фоновом режиме, что замедляет производительность компьютера.

Потенциально опасное приложение

Потенциально вредоносное приложение-это программа, которая может иметь значительное количество нежелательных аспектов, которые могут повлиять на системные ресурсы и производительность, а также поставить под угрозу безопасность Ваших личных и рабочих данных.

Программа-шпион

Любого рода программа-шпион, которая тайно и без ведома пользователя - чаще всего в рекламных целях - собирает информацию о пользователе во время его соединения с сетью Интернет. Шпионские программы обычно маскируют как скрытые компоненты бесплатных или условно бесплатных (shareware) приложений, которые можно скачать из сети Интернет, хотя следует отметить, что большинство бесплатных или условно бесплатных приложений не содержит программ-шпионов. Программа-шпион после своей установки отслеживает адреса в сети Интернет, к которым обращается пользователь, и тайно пересылает эту информацию третьим лицам. Программы-шпионы могут собирать информацию об адресах электронной почты, паролях и номерах кредитных карт.

Программы-шпионы аналогичны вирусам-троянам в том смысле, что и те и другие устанавливаются самими пользователями во время установки других программ. Жертвами программ-шпионов обычно становятся при скачивании известных программных продуктов из файлообменных сетей.

Действия программ-шпионов являются не только нарушением этики и конфиденциальности, но и кражей ресурсов компьютерной памяти и ресурсов канала соединения с сетью Интернет, за счет передачи информации программой-шпионом своему источнику при подключении пользователя к сети Интернет. За счет потребления памяти и системных ресурсов программами-шпионами, работа последних в фоновом режиме может приводить к неустойчивой работе системы и ее сбоям.

Протокол TCP/IP

Протокол управления передачей/интернет-протокол (Transmission Control Protocol/Internet Protocol) — набор сетевых протоколов, широко используемых в сети Интернет. Они объединяют в одну большую сеть множество взаимосвязанных сетей, состоящих из компьютеров с различной архитектурой и с различными операционными системами. Протокол TCP/IP включает в себя стандарты связи между компьютерами, общепринятые правила объединения сетей и маршрутизации трафика.

Расширение имени файла

Часть названия файла после точки, обозначающая тип данных, хранящихся в нем.

Многие операционные системы, такие как Unix, VMS и MSDOS используют расширения имен файлов. Обычно они состоят из трех букв, потому что устаревшие ОС не имеют поддержки более длинных расширений. Например, "c" текст программы на языке C (C source code), "ps" – язык PostScript, а "txt" – любой текстовый файл.

Рекламное ПО

Рекламное ПО часто устанавливается «в качестве нагрузки» к основным приложениям, которые предоставляются бесплатно, при условии, что пользователь соглашается установить adware-программу. Поскольку Adware-приложения обычно устанавливаются только после того, как пользователь принимает условия, содержащиеся в соответствующем лицензионном соглашении с указанием функций данного приложения, то их функционирование не является каким-либо нарушением прав пользователя.

Однако, всплывающие рекламные объявления могут причинять неудобства пользователю, а в некоторых случаях и ухудшать производительность системы. Кроме того, информация, собираемая

некоторыми из этих приложений, может нарушить неприкосновенность частной жизни пользователей, которые не были в полной мере осведомлены об условиях лицензионного соглашения.

Руткит

Руткиты - это набор программных инструментов, позволяющих получить доступ к системе на уровне администратора. Термин впервые использовался для операционных систем UNIX и относился к инструментам перекомпиляции, которые позволяли получить права администратора, при этом их присутствие оставалось скрытым для системных администраторов.

Основной целью руткитов является скрытие процессов, файлов, логинов и журналов. Они также могут перехватывать данные с терминалов, сетевых соединений или перифирийных устройств, если их встроить в соотвествующее программное обеспечение.

По своей природе руткиты не вредоносны. Например, системы, а также некоторые приложения, скрывают важные файлы при помощи руткитов. Однако, чаще всего, их используют как вредоносные программы либо для скрытия присутствия в системе. При совмещении с вредоносными программами руткиты представляют серьезную угрозу для целостности и безопасности системы. Они могут отслеживать трафик, создавать бреши в системе, изменять файлы и журналы, избегая выявления.

Сверхсжатый архив

Архивная бомба - это многократно сжатый файл. При распаковке это может привести к сбоям антивирусной программы или системы из-за большого потребления ресурсов.

Сигнатуры вредоносных программ

Сигнатуры вирусов представляют собой фрагменты кода, извлеченные из образцов настоящих вирусов. Они используются антивирусными программами для поиска по шаблону и распознавания вредоносных программ. Сигнатуры также используются для удаления вредоносного кода из зараженных файлов.

База данных вирусных сигнатур Bitdefender представляет собой набор вирусных сигнатур, обновляемый каждый час специалистами Bitdefender по анализу вредоносных программ.

Слои защиты

GravityZone обеспечивает защиту при помощи ряда модулей и функций, которые можно назвать слоями защиты, делящимися на защиту на конечных точках или защиту ядра и на другие дополнения. Защита на конечных точках включает в себя антивредоносные программы, расширенный контроль угроз, расширенный Anti-Exploit, Firewall, контроль контента, контроль устройств, Network Attack Defense, Power user и Relay. Дополнения включают в себя слои защиты, такие как Security for Exchange и Sandbox Analyzer.

Для получения более подробной информации о слоях защиты, доступных для GravityZone решения, обращайтесь к «Уровни защиты GravityZone » (p. 2).

События (Events)

Действие или событие, обнаруженное программой. Событиями могут быть действия пользователя, например щелчок кнопкой мыши, или нажатие клавиши, или системные события, например, переполнение памяти.

Создание дочернего процесса

Попытка создания какого-либо дочернего процесса.

Создание процесса устарело

Обнаружение попыток создания новых процессов с использованием устаревших методов

Спам

"Мусорная" электронная почта или "мусорная" новостная рассылка. Более известна как нежелательная электронная почта.

Средство кражи паролей

Программа для кражи паролей собирает фрагменты данных, которые могут быть именами учетных записей и связанными с ними паролями. Эти украденные учетные данные затем используются для злонамеренных целей, таких как захват аккаунтов.

Стек ROP смещен

Обнаружение попыток повредить стек, используя технику ROP, проверяя выравнивание адреса стека.

Стек возврата ROP

Обнаружение попыток выполнить код непосредственно в стеке, используя технику ROP, путем проверки диапазона адресов возврата.

Сценарий

Еще один термин, обозначающий макрос или командный файл. Сценарий – это набор команд, выполняющихся без участия пользователя.

Троян

Вредоносная программа, маскирующаяся под безвредное приложение. В отличие от обычных вирусов, вирус класса Троян не копирует себя, однако, он может быть не менее разрушительным. Вирусы-трояны одни из наиболее опасных типов, обещающие избавить ваш компьютер от всех вирусов, но, на самом деле, загружают вирусы в компьютер.

Этот термин взят из поэмы Гомера «Илиада», где в одной из глав описывается как греки подарили своим врагам, жителям Трои, огромного деревянного коня, якобы в знак мира. Но после того, как троянцы втащили статую в город, греческие солдаты выскочили из полости в теле коня и открыли городские врата, после чего их соратники ворвались в Трою и захватили город.

Универсальная вспышка

Пытается использовать Flash-плеер.

Файл отчета

Файл, в котором перечислены совершенные действия. Bitdefender включает в отчеты путь к проверенным файлам, папки, количество проверенных архивов и файлов, а также сколько подозрительных и зараженных файлов обнаружено.

Файлы Cookie

В сфере интернет-технологий под файлами cookie подразумеваются небольшие файлы, содержащие информацию о компьютере, которую можно проанализировать и использовать для того, чтобы выяснить ваши интересы и предпочтения. Поэтому технология создания таких файлов набирает обороты и сейчас вы можете получать рекламу товаров, основанную на ваших интересах. Но это "палка о двух концах" - с одной стороны вы видите именно то, что может вам пригодиться. Но с другой – за вами постоянно следят и знают, на какой странице вы находитесь

и на какой кнопке щелкаете мышкой. Понятно, почему сейчас так широко обсуждается конфиденциальность данных пользователей и многие чувствуют себя ущемленными в своих правах, будучи уверенными, что их «считывают» как кассир в магазине считывает штрих-код на этикетке. Порой эта точка зрения кажется крайностью, но иногда она полностью отражает действительность.

Фишинг

Попытка мошенников захватить важные данные. Обычно фальшивые веб-сайты создаются для того, чтобы войти в доверие пользователей и предлагают обновить личную информацию, такую как пароли и номера кредитных карт, социального страхования и банковских счетов, в попытке обмануть их.

Целевые атаки

Кибер-атаки, которые в основном направлены на получение финансовой выгоды или порчу репутации. Целью может быть частное лицо, компания, программное обеспечение или система, данные о которых тщательно изучаются до проведения атаки. Такие атаки развертываются в течение длительного периода времени и поэтапно, используя одну или несколько точек проникновения. Они действуют незаметно и чаще всего обнаруживаются уже после нанесения повреждения.

Червь

Программа, которая распространяется по сети, копируя и отправляя себя дальше. Она не может присоединяться к другим программам.

Эвристический анализ (Heuristic)

Способ обнаружения новых вирусов, основанный на правилах. Этот способ проверки не связан напрямую с определенными сигнатурами вирусов. Преимущество эвристической проверки состоит в том, что новый вирус не может "обмануть" фильтр. Однако он может принять подозрительный код в обычных программах за вирус и вызвать так называемое «ложное срабатывание».

инструмент эксплуатации уязвимости

Эксплоитом обычно евзывают любой метод, используемый для получения несанкционированного доступа к компьютерам или к взлому безопасности системы, который открывает систему для атаки.