Bitdefender

GravityZone

РУКОВОДСТВО АДМИНИСТРАТОРА

Bitdefender GravityZone
Руководство администратора

Дата публикации 2021.09.29

Авторские права© 2021 Bitdefender

Правовое положение

Все права защищены. Никакая часть этой публикации не может быть воспроизведена или передана в любой форме или любыми средствами, электронными или механическими, включая фотокопирование, запись, использование средств хранения и поиска информации, без получения письменного разрешения уполномоченного представителя компании Bitdefender Использование цитат в обзорах разрешается только со ссылкой на цитируемый источник. Запрещено вносить какие-либо изменения в данный материал.

Предупреждение и ограничение ответственности. Данный программный продукт и документация к нему защищены авторским правом. Данный программный продукт и документация к нему защищены авторским правом. Информация в этом документе предоставляется «как есть», без гарантии. Хотя в ходе подготовки этого документа были приняты все меры предосторожности, авторы не несут никакой ответственности перед любым лицом или организацией в отношении каких-либо потерь или ущерба, причиненных или предположительно вызванных прямо или косвенно информацией, содержащейся в документе.

Данная книга содержит ссылки на сторонние веб-сайты, не находящихся под контролем Bitdefender ,поэтому Bitdefender не несет ответственности за их содержание Переходя на сторонние сайты, указанные в документе, вы делаете это на свой страх и риск. Bitdefender приводит эти ссылки только для удобства читателя, но наличие этих ссылок не означает, что Bitdefender берет на себя ответственность за содержание какого-либо стороннего веб-сайта.

Торговые марки. В этом документе могут упоминаться различные торговые марки. В этом документе могут упоминаться различные торговые марки. Все зарегистрированные и незарегистрированные торговые марки, упоминаемые в этом документе, принадлежат только их законным владельцам.

Содержание

Предисловие vii
1. Обозначения, используемые в данном руководстве vii
1. О GravityZone 1
2. Уровни защиты GravityZone 2
2.1. Защита от вредоносного ПО 2
2.2. Расширенный контроль угроз (Advanced Threat Control) 4
2.3. Advanced Anti-Exploit 4
2.4. Брандмауэр 4
2.5. Контроль контента 4
2.6. Network Attack Defense 5
2.7. Управление исправлениями 5
2.8. Контроль устройств 5
2.9. Полное шифрование диска 6
2.10. Sandbox Analyzer 6
2.11. Network Traffic Security Analytics (NTSA) 6
2.12. Доступность уровней защиты GravityZone 7
3. Архитектура GravityZone 8
3.1. GravityZone VA 8
3.1.1. База данных GravityZone 9
3.1.2. Сервер обновлений GravityZone 9
3.1.3. Коммуникационный Сервер GravityZone 9
3.1.4. Веб-консоль (GravityZone Control Center) 9
3.2. Агенты безопасности 9
3.2.1. Bitdefender Endpoint Security Tools 10
3.2.2. Endpoint Security for Mac 12
3.3. Sandbox Analyzer Архитектура 12
4. Начало работы 14
4.1. Подключение к Control Center 14
4.2. Интуитивно понятная Control Center 15
4.2.1. Обзор Control Center 15
4.2.2. Таблица данных 17
4.2.3. Панели инструментов 19
4.2.4. Контекстное меню 19
4.2.5. Выбор просмотра 20
4.3. Управление вашей учетной записью 21
4.4. Изменение пароля для входа в систему 24
5. Учетные записи пользователей 25
5.1. Роли пользователей 26
5.2. Права пользователя 28
5.3. Управление учетными записями пользователей 28
5.3.1. Индивидуальное управление учетными записями пользователей 29
5.3.2. Управление несколькими учетными записями пользователей 32

5.4. Сброс паролей входа . . . 37
5.5. Управление двухфакторной аутентификацией . . . 37

6. Управление сетевыми объектами . . . 39
6.1. Виды сетей . . . 41
6.1.1. Компьютеры и виртуальные машины . . . 41
6.1.2. Виртуальные машины . . . 42
6.2. Компьютеры . . . 43
6.2.1. Проверка статуса компьютера . . . 44
6.2.2. Получение сведений о компьютере . . . 47
6.2.3. Организация компьютеров в группы . . . 61
6.2.4. Сортировка, фильтрация и поиск компьютеров . . . 63
6.2.5. Запущенные Задачи . . . 68
6.2.6. Формирование быстрых отчетов . . . 81
6.2.7. Назначение политик . . . 81
6.2.8. Синхронизация со службой каталогов Active Directory . . . 83
6.3. Виртуальные машины . . . 83
6.3.1. Проверять статусы виртуальных машин . . . 85
6.3.2. Просмотр подробной информации о виртуальной машине . . . 89
6.3.3. Организация виртуальных машин в группы . . . 96
6.3.4. Сортировка, фильтрация и поиск виртуальных машин . . . 98
6.3.5. Запуск задач на виртуальных машинах . . . 102
6.3.6. Формирование быстрых отчетов . . . 126
6.3.7. Назначение политик . . . 127
6.3.8. Использование Менеджер восстановления (Recovery Manager) для зашифрованных томов . . . 128
6.4. Просмотр и управление задачами . . . 129
6.4.1. Проверить статус задачи . . . 130
6.4.2. Просмотр отчетов задач . . . 132
6.4.3. Перезапуск задач . . . 132
6.4.4. Удаление задач . . . 132
6.5. Удаление конечных точек из сетевого содержимого . . . 133
6.6. Настройка параметров сети . . . 135
6.6.1. Настройки инвентаризации сети . . . 135
6.6.2. Автономное удаление машин . . . 136
6.7. Диспетчер учетных данных (Credentials Manager) . . . 138
6.7.1. Операционная система . . . 138
6.7.2. Виртуальная среда . . . 139
6.7.3. Удаление учетных данных из диспетчера учетных данных . . . 140

7. Политики безопасности (Security Policies) . . . 141
7.1. Управление политиками . . . 142
7.1.1. Создание политик . . . 143
7.1.2. Назначение политик . . . 143
7.1.3. Изменение настроек политики . . . 153
7.1.4. Изменение имен политик . . . 153
7.1.5. Удаление политик . . . 154
7.2. Политики компьютеров и виртуальных машин . . . 154
7.2.1. Основные . . . 155

7.2.2. Защита от вредоносного ПО . . . 164
7.2.3. Sandbox Analyzer . . . 202
7.2.4. Брандмауэр . . . 207
7.2.5. Защита сети . . . 222
7.2.6. Управление исправлениями . . . 240
7.2.7. Контроль устройств . . . 244
7.2.8. Ретранслятор . . . 249
7.2.9. Шифрование . . . 251

8. Информационная панель мониторинга . . . 257
8.1. Панель управления . . . 257
8.1.1. Обновление данных портлета . . . 258
8.1.2. Редактирование настроек портлета . . . 259
8.1.3. Добавление нового портлета . . . 259
8.1.4. Удаление портлета . . . 259
8.1.5. Расположение портлетов . . . 259

9. Использование отчетов . . . 261
9.1. Типы отчетов . . . 261
9.2. Создание отчетов . . . 264
9.3. Просмотр и управление отчетами по расписанию . . . 267
9.3.1. Просмотр отчетов . . . 268
9.3.2. Редактирование отчетов по расписанию . . . 268
9.3.3. Удаление отчета по расписанию . . . 270
9.4. Выполнение действий, основанные на данных отчета . . . 270
9.5. Сохранение отчетов . . . 271
9.5.1. Экспорт отчетов . . . 271
9.5.2. Загрузка отчетов . . . 271
9.6. Отправка отчетов . . . 272
9.7. Печать отчетов . . . 272

10. Использование Sandbox Analyzer . . . 273
10.1. Фильтрация карточек отправки . . . 273
10.2. Просмотр подробностей анализа . . . 275
10.3. Повторное представление образца . . . 277
10.4. Удаление карточек подачи . . . 278
10.5. Manual Submission . . . 278
10.6. Инфраструктура управления Sandbox Analyzer . . . 281
10.6.1. Проверка статуса Sandbox Analyzer . . . 281
10.6.2. Настройка одновременных детонаций . . . 283
10.6.3. Проверка состояния VM. . . . 283
10.6.4. Настройка и управление VM . . . 284

11. Журнал активности пользователя . . . 285

12. Уведомления . . . 287
12.1. Типы уведомлений . . . 287
12.2. Просмотр уведомлений . . . 294
12.3. Удаление уведомлений . . . 295
12.4. Настройка параметров уведомлений . . . 295

13. Статус системы 299
13.1. Состояние ОК 300
13.2. Статус учетной записи 300
13.3. Параметры 301

14. Получение справки 304
14.1. Центр поддержки Bitdefender 304
14.2. Обращение за помощью 306
14.3. Использование инструментов поддержки 306
14.3.1. Использование инструмента поддержки на операционных системах Windows 306
14.3.2. Использование инструмента поддержки на операционных системах Linux . . . 308
14.3.3. Использование инструментов поддержки на операционных системах Mac . . . 310
14.4. Контактная информация 311
14.4.1. Адреса веб-сайтов 311
14.4.2. Местные дистрибьюторы 311
14.4.3. Офисы Bitdefender 312

A. Приложения 315
A.1. Поддерживаемые типы файлов 315
A.2. Типы сетевых объектов и статусы 316
A.2.1. Типы сетевых объектов 316
A.2.2. Состояние сетевых объектов 317
A.3. Типы файлов приложений 318
A.4. Системные переменные 318
A.5. Объекты Sandbox Analyzer 320
A.5.1. Поддерживаемые Типы и Расширения Фалов для Отправки Вручную 320
A.5.2. Типы Файлов Поддерживаемые Предварительной Фильтрацией Контента при Автоматической Отправке 320
A.5.3. Исключения По Умолчанию в Автоматической Отправке 321
A.5.4. Рекомендуемые приложения для детонации виртуальных машин 321
A.6. Процессоры данных 322

Глоссарий 325

Предисловие

Это руководство предназначено для сетевых администраторов, отвечающий за управление защитой GravityZone в своих организациях.

Цель данного документа объяснить, как применять и просматривать параметры безопасности конечных точек сети, под своей учетной записью, используя GravityZone Control Center. Вы узнаете, как просматривать инвентаризацию сети в Control Center, как создавать и применять политику на управляемых конечных точках, как создавать отчеты, как управлять карантином и как использовать панель управления.

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. vii)	В кавычках приводятся внутренние ссылки на другие материалы в пределах этого документа.
опция	Все параметры продукта выделены **жирным** шрифтом.

Виды шрифтов и стилей	Описание
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

Решение GravityZone было разработано специально для виртуализированных сред и облаков, с помощью которых можно предоставлять услуги по защите бизнеса для физических конечных устройств и виртуальных машин в частных и общедоступных облаках.

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 защиты для конечных точек: защита от вирусов с поведенческим мониторингом, защита от угроз нулевого дня, перемещение приложений в черный список и безопасную среду, файервол, управление устройствами и управление контентом.

2. УРОВНИ ЗАЩИТЫ GRAVITYZONE

GravityZone обеспечивает следующие уровни защиты:

- Защита от вредоносного ПО
- Расширенный контроль угроз (Advanced Threat Control)
- Advanced Anti-Exploit
- Брандмауэр
- Контроль контента
- Управление исправлениями
- Контроль устройств
- Полное шифрование диска
- Network Traffic Security Analytics (NTSA)

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).**

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. 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.

2.4. 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.

2.5. 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.

2.6. 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.

2.7. 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.

2.8. 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.).

2.9. 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.

2.10. Sandbox Analyzer

Bitdefender Sandbox Analyzer обеспечивает мощный уровень защиты от продвинутых угроз путем автоматического и глубокого анализа подозрительных файлов, не подписанных антивирусным движком Bitdefender. Безопасная среда использует обширный набор технологий Bitdefender для размещения полезных данных в развернутой локально виртуальной среде, , анализирует их поведение и сообщает о небольших системных изменениях, которые могут свидетельствовать о вредоносной природе.

Sandbox Analyzer использует ряд сенсоров для проверки данных от сетевых потоков трафика, централизованного карантина и ICAP серверов.

Кроме того, Sandbox Analyzer позволяет передать образцы вручную и через API.

Примечание
Функциональность этого модуля обеспечивает Sandbox Analyzer On-Premises, который доступен по отдельному лицензионному ключу.

2.11. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) - сетевое решение безопасности, которое анализирует потоки трафика IPFIX на наличие подозрительного поведения и вредоносного ПО.

Bitdefender NTSA предназначен для того, чтобы действовать наряду с вашими существующими мерами безопасности как дополнительная гарантия, которая

способна покрыть слепые зоны, не отслеживаемые традиционными инструментами.

Традиционные инструменты безопасности сетей обычно пытаются предотвратить вредоносные заражения анализируя входящий трафик (с помощью песочницы, брандмауэра, антивируса и т.д.) Bitdefender NTSA фокусируется исключительно на анализе исходящего сетевого трафика на наличие подозрительного поведения.

2.12. 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

Уникальная архитектура GravityZone позволяет с легкостью масштабировать решение и защитить любое количество систем. GravityZone может быть настроена на использование нескольких виртуальных устройств и множество экземпляров конкретных ролей (база данных, коммуникационный сервер, сервер обновлений и веб-консоль), чтобы обеспечить надежность и масштабируемость.

Каждый экземпляр роли может быть установлен на разных устройствах. Встроенные балансировщики ролей позволяют доказать, что развертывание GravityZone защитит даже самые крупные корпоративные сети, не вызывая замедления или узкие места. Уже существующие программные или аппаратные балансировщики также могут быть использованы вместо встроенной балансировки, если они присутствуют в сети.

Поставляясь в качестве виртуального контейнера, GravityZone может быть импортирована на любую платформу виртуализации, включая VMware, Citrix, Microsoft Hyper-V, Nutanix Prism, Microsoft Azure.

Интеграция с VMware vCenter, Citrix XenServer, Microsoft Active Directory, Nutanix Prism Element и Microsoft Azure упрощает развертывание защиты как для физических, так и для виртуальных машин.

Решение GravityZone включает в себя следующие компоненты:

- Виртуальные устройства GravityZone
- Агенты безопасности

3.1. GravityZone VA

Локальное решение GravityZone поставляется как настроенное виртуальное устройство на базе Linux Ubuntu, встроенное в образ виртуальной машины, которое можно легко установить и настроить через CLI (Интерфейс командной строки). Виртуальное устройство доступно в нескольких вариантах, совместимых с основными платформами виртуализации (OVA, XVA, VHD, OVF, RAW).

3.1.1. База данных GravityZone

Центральная логика архитектуры GravityZone. Bitdefender использует не-реляционную базу данных MongoDB, которую легко масштабировать и реплицировать.

3.1.2. Сервер обновлений GravityZone

Сервер обновлений играет важную роль в обновлении решения GravityZone и конечных агентов путем репликации и публикации необходимых пакетов или установочных файлов.

3.1.3. Коммуникационный Сервер GravityZone

Коммуникационный Сервер является связующим звеном между агентами безопасности и базами данных, передавая политики и задачи для защиты конечных точек, а также генерируя отчеты от агентов безопасности.

3.1.4. Веб-консоль (GravityZone Control Center)

Решения безопасности Bitdefender управляются в GravityZone из единой точки управления - веб-консоли Control Center, которая обеспечивает более легкое управление и доступ к полным настройкам безопасности, глобальным угрозам безопасности, а также полный контроль над всеми модулями безопасности, защищающих виртуальные или физические настольные компьютеры и серверы. Работая на архитектуре Gravity, Control Center способна удовлетворить потребности даже самых крупных организаций.

Control Center интегрируется с существующими системами управления и мониторинга, чтобы упростить автоматическое применение защиты к неуправляемым рабочим станциям или серверам, находящимся в службе каталогов Microsoft Active Directory, или которые были просто обнаружены в сети.

3.2. 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

3.2.1. 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).

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)
- Брандмауэр
- Контроль контента
- Network Attack Defense
- Управление исправлениями
- Контроль устройств
- Полное шифрование диска

Роли конечных точек

- Привилегированный пользователь
- Ретранслятор
- Сервер кэширования патчей

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 распределенными сетями, агенты-ретрансляторы помогают снизить использование полосы пропускания, предотвращая непосредственное подключение защищаемой конечной точки к устройству 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.
- 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.

3.2.2. 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)

3.3. 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.

Чтобы использовать данный модуль совместно с GravityZone, вам необходимо установить Sandbox Analyzer On-Premises.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises представляет собой виртуальное устройство Linux Ubuntu, встроенное в образ виртуальной машины, его можно легко установить и сформировать при помощи интерфейса командной строки (CLI). Sandbox Analyzer On-Premises доступен в формате OVA, также может быть развернут в VMWare ESXi.

ЭкземплярSandbox Analyzer On-Premises содержит в себе следующие компоненты:

- **Менеджер песочницы**. Это компонент является оркестром песочницы. Sandbox Manager связывается с гипервизором ESXi посредством API и использует их технические оснащение для постройки и эксплуатации среды анализа вредоносных программ.
- **Виртуальная машины детонации**. Данный компонент состоит из машин, используемых Sandbox Analyzer, для создания файлов и анализа их режима работы. Виртуальные машины детонации могут управлять Windows 7, а также 64-разрядной версией системы Windows 10.

GravityZone Control Center работает как консоль управления и отчетности, где вы настраиваете политики безопасности и просматриваете аналитические отчеты и уведомления.

Sandbox Analyzer On-Premises управляет следующими датчики подачи:

- **Сетевой датчик**. Виртуальное устройство сетевой безопасности (NSVA) - это виртуальное устройство, которое можно развернуть в той же виртуализированной среде ESXi, что и экземпляр Sandbox Analyzer. Датчик сети извлекает контент из сетевых потоков и передает его в Sandbox Analyzer.
- **Датчик ICAP**. Развернутая на устройствах с сетевым хранилищем (NAS) по протоколу ICAP, Bitdefender Security Server поддерживает отправку содержимого в Sandbox Analyzer.

В дополнение к этим датчикам Sandbox Analyzer On-Premises поддерживает ручную отправку и через API. Подробнее см. Главу **Использование Sandbox Analyzer** в Руководстве администратора GravityZone.

4. НАЧАЛО РАБОТЫ

Решения GravityZone могут быть сконфигурированы и управляться с помощью централизованной платформы управления под названием Control Center. Control Center имеет веб-интерфейс, к которому вы можете получить доступ с помощью имени пользователя и пароля.

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:

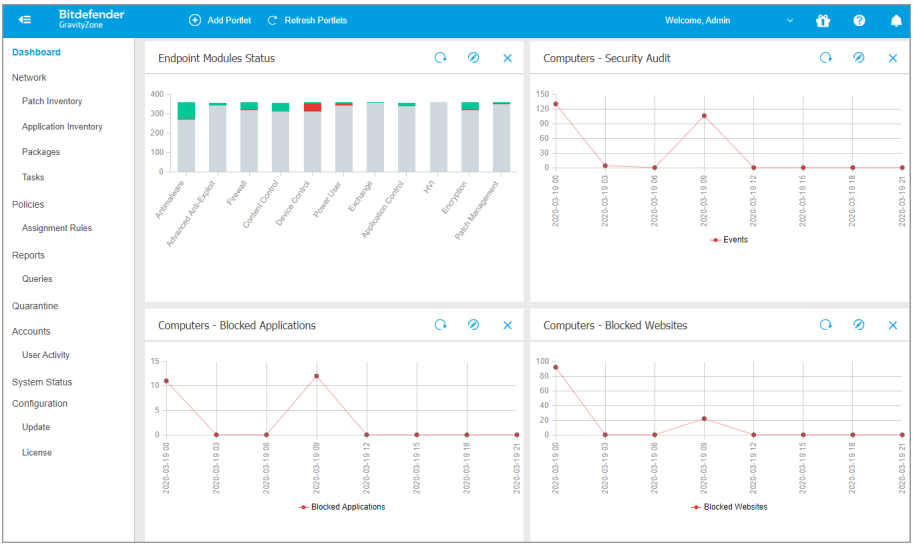
1. В адресной строке веб-браузера введите IP-адрес или DNS-имя хоста Control Center (используя префикс `https://`).
2. Введите имя пользователя и пароль.
3. Введите шестизначный код из Google Authenticator, Microsoft Authenticator или любого двухфакторного TOTP (Time-Based One-Time Password Algorithm) аутентификатора, совместимого со стандартом RFC6238. Дополнительные сведения см. в разделе «Управление вашей учетной записью» (p. 21).
4. Нажмите **Войти**.

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.

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

Пользователи с ролью администратора компании имеют полные права на конфигурацию Control Center и сетевых настроек безопасности, в то время как пользователи, с ролью администратора имеют доступ к функциям сетевой безопасности, включая управление пользователями.

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.

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 Control Center, такие как почтовый сервер, интеграция с Active Directory или средами виртуализации, сертификаты безопасности и параметры инвентаризации сети, включая запланированные правила для автоматической очистки неиспользуемых виртуальных машин.

Примечание
Это меню доступно только пользователям с правами **Управление решениями**.

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

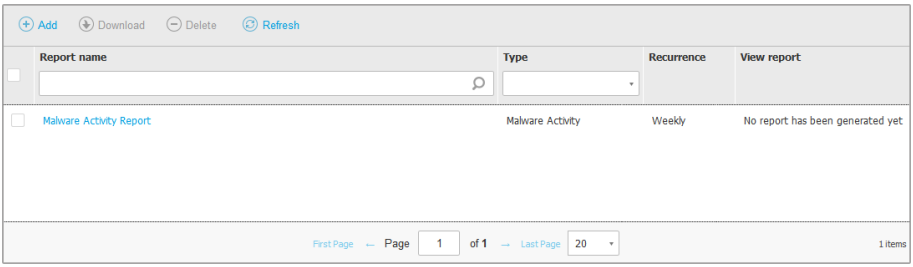
- **Моя учетная запись**. Выберите этот параметр, чтобы управлять своими реквизитами пользователя и настройками.
- **Диспетчер учетных данных**. Выберите этот параметр для добавления и управления учетными данными, необходимыми для задач удаленной установки.
- **Помощь & Поддержка**. Выберите данную опцию, 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

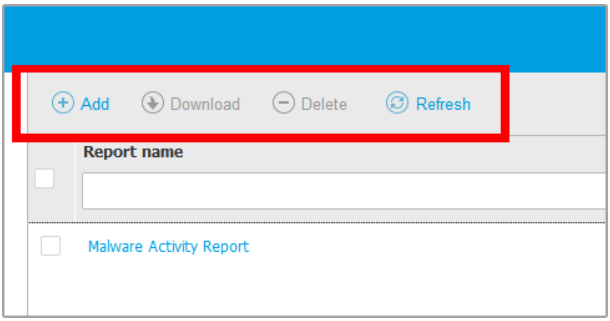
Чтобы убедиться, что консоль отображает последнюю информацию, нажмите кнопку **Обновить** в верхней части таблицы.

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:

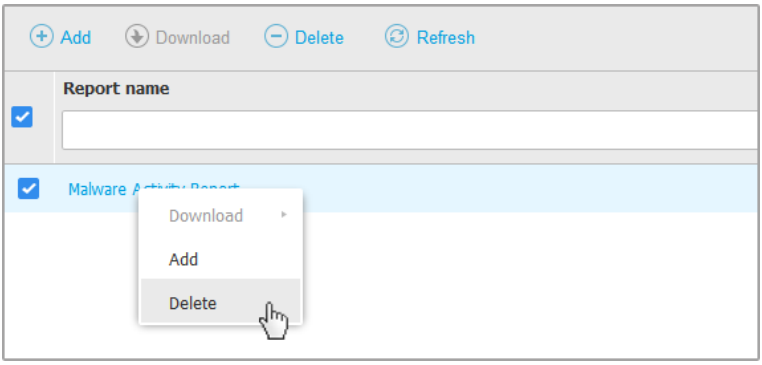
- Создать новый отчет.
- Загрузить отчет по расписанию.
- Удалить отчет по расписанию.



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.



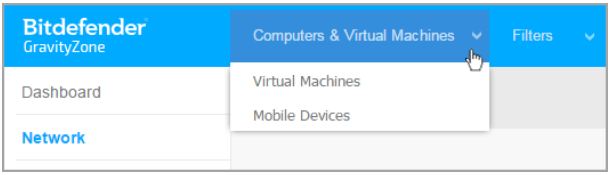
Страница отчетов - Контекстное меню

4.2.5. Выбор просмотра

Если вы работаете с различными типами конечных устройств, вы можете получить доступ к ним на странице **Сеть**, где они сгруппированы по типу устройств, в виде нескольких сетей.

- **Компьютеры & и виртуальные машины**: отображает группы и компьютеры в службе каталогов Active Directory, а также физические и виртуальные рабочие станции вне Active Directory, обнаруженные в сети.
- **Виртуальные машины**: отображает инфраструктуру виртуального окружения интегрированного с Control Center и содержит все виртуальные машины.

Чтобы выбрать отображение нужной сети, нажмите меню просмотра в правом верхнем углу страницы.



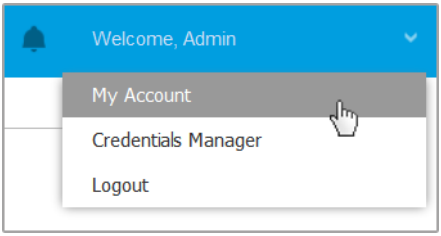
Выбор просмотра

Примечание
Вы сможете видеть только те конечные устройства, которые предусмотрены разрешениями, назначенные администратором, который добавил вашу учетную запись в Control Center.

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. Если вы используете учетную запись в службе каталогов Active Directory, вы не можете изменить данные о ней.
   - **Имя пользователя.** Имя пользователя является уникальным идентификатором учетной записи и не может быть изменено.
   - **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 Впшей 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.

Если вы не используете учетные данные Active Directory, чтобы получить доступ к Control Center, рекомендуется сделать следующее:

- 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:

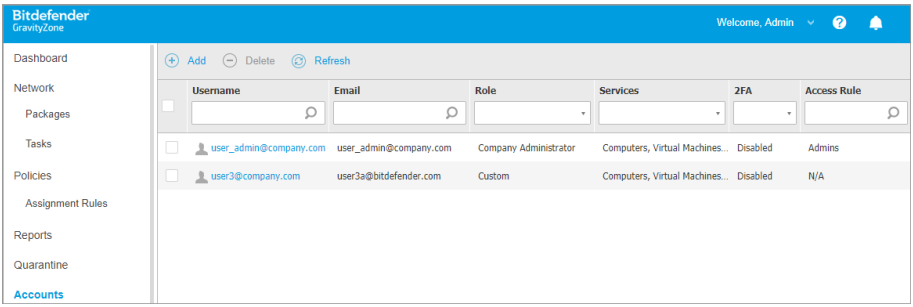
1. Нажмите на ваше имя пользователя в правом верхнем углу консоли и выберите **Мой аккаунт**.
2. В **Account Details** нажмите **Change password**.
3. Введите текущий пароль и новый пароль в соответствующие поля.
4. Нажмите **Сохранить**, чтобы сохранить изменения.

5. УЧЕТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ

Вы можете создать первую учетную запись пользователя GravityZone во время начальной настройки Control Center, после развертывания устройства GravityZone. Начальная учетная запись пользователя Control Center имеет роль администратора компании, с полными правами на конфигурацию Control Center и управление сетью. Из этого аккаунта вы можете создать все другие учетные записи, необходимые для управления сетью вашей компании.

Вот, что вам нужно знать об учетных записях GravityZone:

- Чтобы разрешить другим сотрудникам компании доступ к Control Center, вы можете создать учетные записи пользователей по отдельности или включить динамический доступ для нескольких учетных записей посредством интеграции Active Directory или правил доступа. 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 (используется для входа в Control Center).
- Адрес электронной почты учетной записи (используется в качестве контактного адреса). 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).
- Службы безопасности GravityZone позволяют пользователю осуществлять управление (компьютерами, виртуальными машинами).
- Статус двухфакторной аутентификации, который позволяет быстро проверить, включена ли у пользователя двухфакторная аутентификация.
- Статус Правила Доступа показывает учетную запись пользователя, созданную с помощью правила разрешения доступа. Учетные записи, созданные вручную, будут отображаться как **N/A**.

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. **Администратор компании** - Обычно, уникальная учетная запись пользователя, с ролью Администратора компании, создается для каждой компании отдельно, с полным доступом ко всем функциям управления решением GravityZone. Администратор компании конфигурирует настройки Control Center, управляет лицензионными ключами служб безопасности, управляет учетными записями пользователей, также имея административные привилегии по настройке сетевой безопасности всей компании. 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. 28).

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

Роль аккаунта	Разрешения дочерних учетных записей	Права пользователя
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 решением**. Позволяет сконфигурировать настройки Control Center (сервер электронной почты и настройки прокси-сервера, интеграции с Active Directory и платформами виртуализации, сертификаты безопасности и обновления GravityZone). Эти права только для учетных записей администраторов компании.
- **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

Для создания, редактирования, удаления и настройки учетных записей пользователей используйте следующие методы:

- Индивидуальное управление учетными записями пользователей. Используйте этот метод для добавления учетных записей локальных пользователей или учетных записей Active Directory. Чтобы настроить интеграцию с Active Directory, обратитесь к Руководству по установке GravityZone.

  Перед тем как создать учетную запись пользователя, убедитесь, что у вас под рукой есть требуемый адрес электронной почты. Пользователь получит регистрационные данные GravityZone на предоставленный адрес электронной почты.

- Управление несколькими учетными записями пользователей. Используйте этот метод для включения динамического доступа посредством правила доступа. Данный метод требует интеграции домена Active Directory. Для получения дополнительной информации об интеграции Active Directory см. Руководство по установке GravityZone.

5.3.1. Индивидуальное управление учетными записями пользователей

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

Зависимости

- Локально созданные учетные записи могут поспособствовать удалению аккаунтов, созданных путем интеграции Active Directory независимо от их роли.
- Локально созданные учетные записи не могут способствовать удалению таких же аккаунтов независимо от их роли.

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:

- Для учетных записей пользователей Active Directory настройте следующие данные:

  Имя пользователя для учетных записей пользователей Active Directory (AD). Выберите учетную запись пользователя из выпадающего списка и перейдите к шагу 4.

  Вы можете добавлять учетные записи пользователей AD только при настроенной интеграции. При добавлении учетной записи пользователя AD данные пользователя импортируются из соответствующего домена. Пользователь входит в Control Center, используя имя пользователя и пароль AD.

  Примечание

  – Чтобы убедиться, что последние изменения Active Directory импортированы в Control Center, нажмите кнопку **Синхронизировать**.

  – Пользователи с правом **Управление решением** могут настроить интервал синхронизации Active Directory с помощью параметров, доступных на вкладке **Конфигурация > Active Directory** . Для получения дополнительной информации см. главы **Установка защиты > Установка GravityZone** и **Настройка > Настройка параметров центра Control Center** из Руководства по установке GravityZone.

- Для локальных учетных записей настройте следующие данные:

  – **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.

  – **Пароль**. Введите пароль, который пользователь может использовать для входа.

Пароль должен содержать, по крайней мере, один символ верхнего регистра, по крайней мере, одну строчную букву и, по крайней мере, одну цифру или специальный символ.

– **Подтвердите пароль**. Подтвердите пароль для проверки.

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.
- **Роль**. Выберите роль пользователя. Для получения подробной информации относительно ролей пользователей, обратитесь к «Роли пользователей» (p. 26).
- **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. 28).
- **Выбрать цель**. Выберите сетевые группы, в которых пользователь будет иметь доступ к каждой доступной службе безопасности. Вы можете ограничить доступ пользователей к определенным службам безопасности GravityZone или к конкретным областям сети.

Примечание
Опция выбора объекта не будет отображаться для пользователей с правами Управления решением, которые, по умолчанию, имеют полномочия на всю сеть и службы безопасности.

5. Нажмите **Save**, чтобы добавить пользователя. Новая учетная запись появится в списке учетных записей пользователей.

   Control Center автоматически отправляет пользователю электронное письмо с данными регистрации, если настройки почтового сервера были правильно введены. Более подробную информацию о конфигурации почтового сервера см. в разделе **Установка защиты > GravityZone**

Установка и настройка > Настройка Control Center Настройки центра из раздела GravityZone Руководство по установке.

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.

5.3.2. Управление несколькими учетными записями пользователей

Создайте правила доступа, чтобы предоставить GravityZone Control Center доступ к пользователям Active Directory на основе групп безопасности.

Требования к системе

Чтобы управлять несколькими учетными записями пользователей, вам нужна интеграция домена Active Directory с GravityZone. Чтобы интегрировать и

синхронизировать домен Active Directory, см. главу **Active Directory** в Руководстве по установке GravityZone.

Зависимости

Правила разрешения доступа связаны с группами безопасности Active Directory (AD) и соответствующими учетными записями пользователей. Любые изменения, внесенные в домены Active Directory, могут повлиять на соответствующие правила доступа. Вот что необходимо знать об отношении между правилами, пользователями и доменами Active Directory:

- Правило разрешения доступа добавляет учетную запись пользователя, только если электронная почта еще не связана с существующей учетной записью.
- Для одинаковых адресов электронной почты в группе безопасности правило разрешения доступа создает учетную запись пользователя GravityZone только для первой учетной записи пользователя Active Directory, которая входит в систему Control Center.

  Например, группа безопасности содержит повторяющийся адрес электронной почты для разных пользователей, и все они пытаются войти в Control Center, используя свои учетные данные Active Directory. Если правило разрешения доступа связано с этим конкретным доменом Active Directory, оно создаст учетную запись пользователя только для первого пользователя, который вошел в систему Control Center с использованием повторяющегося адреса электронной почты.
- Учетные записи пользователей, созданные с помощью правил доступа, становятся неактивными, если они удаляются из связанной с ними группы безопасности AD. Те же пользователи могут стать активными, если они связаны с новым правилом доступа.
- Правила доступа становятся доступными только для чтения, когда связанный домен Active Directory больше не интегрируется с GravityZone. Пользователи, связанные с этими правилами, становятся неактивными.
- Аккаунты пользователей, созданные посредством правил доступа, не могут поспособствовать удалению локально созданных пользователей
- Аккаунты, созданные посредством правила доступа, не могут способствовать удалению аккаунтов Администраторов компании.

Создание нескольких учетных записей пользователей

Чтобы добавить несколько учетных записей пользователей, создайте правила доступа. Правила разрешения доступа связаны с группами безопасности Active Directory.

Чтобы добавить правило разрешения доступа:

1. Перейдите на страницу **Конфигурация > Active Directory > Разрешения на доступ**.
2. Если у вас несколько интеграций, выберите домен в верхней левой части таблицы.
3. Нажмите ⊕ **Добавить** в левой части таблицы.
4. Настройте следующие параметры разрешений на доступ:
   - **Приоритет**. Правила обрабатываются в приоритетном порядке. Чем меньше число, тем выше приоритет.
   - **Имя**. Название правила доступа.
   - **Домен**. Домен, с которого необходимо добавить группы безопасности.
   - **Группы Безопасности**. Группы безопасности, которые содержат ваших будущих пользователей GravityZone. Вы можете использовать поле автозаполнения. Группы безопасности, добавленные в этот список, не подлежат изменению, добавлению или удалению после сохранения правила доступа.
   - **Часовой пояс**. Часовой пояс пользователя.
   - **Язык**. Язык отображения консоли.
   - **Роль**. Предопределенные роли пользователей. Для получения дополнительной информации см. главу **Учетные записи пользователей** в Руководстве администратора GravityZone.

     Примечание
     Вы можете предоставлять и отзывать привилегии другим пользователям с такими же или меньшими привилегиями, чем ваша учетная запись.

   - **Права**. Каждая предопределенная роль пользователя имеет определенную конфигурацию прав. Для получения дополнительной информации см. главу **Учетные записи пользователей** в Руководстве администратора GravityZone.

- **Выберите цели** Выберите сетевые группы, в которых пользователь будет иметь доступ к каждой доступной службе безопасности. Вы можете ограничить доступ пользователей к определенным службам безопасности GravityZone или к конкретным областям сети.

  Примечание
  Опция выбора объекта не будет отображаться для пользователей с правами Управления решением, которые, по умолчанию, имеют полномочия на всю сеть и службы безопасности.

5. Нажмите **Сохранить**.

   Правило доступа сохраняется при отсутствии влияния пользователя. В противном случае вам будет предложено указать пользовательские исключения. Например, когда вы добавляете правило с более высоким приоритетом, затронутые пользователи, связанные с другими правилами, привязываются к прежнему правилу.
6. При необходимости выберите пользователей, которых вы хотите исключить. Для получения дополнительной информации см. Исключения учетной записи пользователя.
7. Нажмите **Подтвердить**. Правило отображается на странице **Разрешения на доступ**.

Пользователи в группах безопасности, указанных в правилах доступа, теперь могут получить доступ к GravityZone Control Center со своими учетными данными домена. Control Center автоматически создает новые учетные записи пользователей при первом входе в систему, используя пользовательские адрес электронной почты Active Directory и пароль.

Учетные записи пользователей, созданные с помощью правила доступа, имеют имя правила доступа, отображаемое на странице **Учетные записи** в столбце **Правило доступа**.

Редактирование нескольких учетных записей пользователей

Чтобы изменить правило разрешения доступа:

1. Перейдите на страницу **Конфигурация > Active Directory > Разрешения на доступ**.
2. Выберите имя правила доступа, чтобы открыть окно конфигурации.
3. Изменить настройки разрешения на доступ. Для получения дополнительной информации см. Добавление разрешений на доступ.

4. Нажмите **Сохранить**. Правило сохраняется при отсутствии влияния пользователя. В противном случае вам будет предложено указать исключения учетной записи пользователя. Например, если вы обновите приоритет правила, затронутые пользователи могут переключиться на другое правило.
5. При необходимости выберите пользователей, которых вы хотите исключить. Для получения дополнительной информации см. Исключения учетной записи пользователя.
6. Нажмите **Подтвердить**.

Примечание
Вы можете открепить учетные записи пользователей, созданные с помощью правил доступа, изменив их права в системе Control Center. Учетную запись пользователя невозможно снова привязать к правилам доступа.

Удаление нескольких учетных записей пользователей

Чтобы удалить правило доступа:

1. Перейдите на страницу **Конфигурация > Active Directory > Разрешения на доступ**.
2. Выберите правило доступа, которое вы хотите удалить, и нажмите ⊖ **Удалить**. , Появившееся окно предложит вам подтвердить ваши действия. Если есть влияние на пользователя, вам будет предложено указать исключения учетной записи пользователя. Например, вы можете указать исключения для пользователей, на которых повлияло удаление правила.
3. При необходимости выберите пользователей, которых вы хотите исключить. Для получения дополнительной информации см. Пользовательские исключения.
4. Нажмите **Подтвердить**.

Удаление правила аннулирует доступ к соответствующим учетным записям пользователей. Все пользователи, созданные через него, будут удалены, если другие правила не предоставляют им доступ.

Исключения учетной записи пользователя

Когда вы добавляете, редактируете или удаляете правила доступа, которые влияют на пользователя, вы можете указать исключения учетной записи

пользователя. Вы также можете просмотреть причины и последствия влияния пользователей.

Укажите пользовательские исключения следующим образом:

1. Выберите пользователей, которых вы хотите исключить. Или установите флажок в верхней части таблицы, чтобы добавить всех пользователей в список.
2. Нажмите **X** в поле имени пользователя, чтобы удалить его из списка.

5.4. 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.

5.5. 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. Дополнительную информацию можно найти в Руководстве по установке в разделе **Установка защиты > Установка и настройка GravityZone > Настройка параметров Центра управления**.

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.

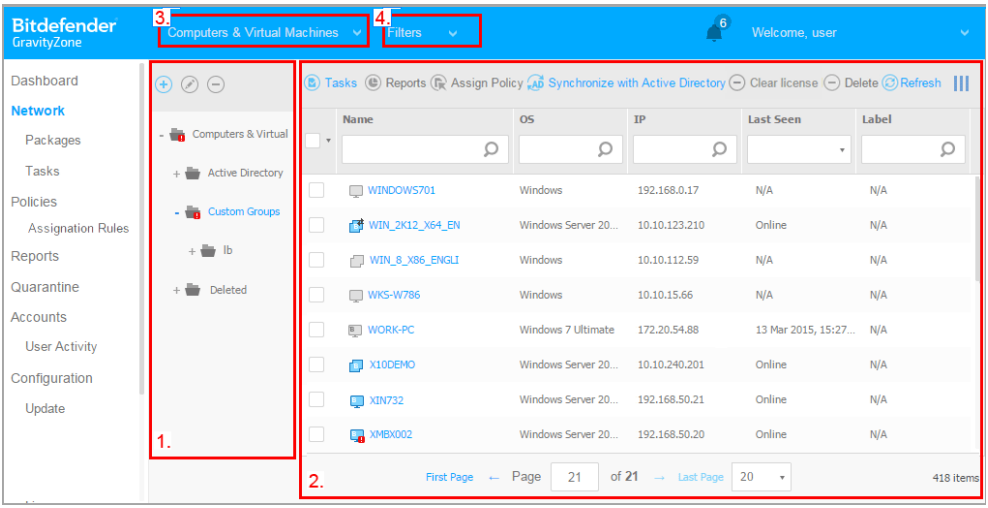
Другой метод проверки изменений двухфакторной аутентификации, связанных с учетными записями пользователей, заключается в том, чтобы получить доступ к странице **Учетные записи > Активность пользователя** и просмотреть журналы активности с помощью следующего фильтра:

- Область > Учетные записи / Компания
- Действие > Изменено

Чтобы получить больше информации о включении двухфакторной аутентификации, оращайтесь к«Управление вашей учетной записью» (p. 21)

6. УПРАВЛЕНИЕ СЕТЕВЫМИ ОБЪЕКТАМИ

Страница **Сеть** предоставляет несколько возможностей для изучения и управления всеми компьютерами и виртуальными машинами доступными в сети. Интерфейс раздела **Сеть** состоит из двух панелей, которые в реальном времени отображают состояние сетевых объектов:



Раздел - Сеть

1. Левая панель отображает дерево имеющейся сети. В зависимости от выбранного вида сети, эта панель отображает сетевую инфраструктуру, интегрированную с Control Center, такую как Active Directory, vCenter Server или Xen Server.

   В то же время, все компьютеры и виртуальные машины, обнаруженные в сети, которые не принадлежат к какой-либо интегрированной инфраструктуре, отображаются в **Custom Groups**.

   Все удаленные конечные точки хранятся в папке **Deleted**. Чтобы узнать больше, обратитесь к «Удаление конечных точек из сетевого содержимого» (p. 133).

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

2. Правая панель отображает содержимое группы, выбранной в левой панели. 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. Наведите курсор мыши на значок, чтобы просмотреть всплывающую информацию. 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. 316).
   - 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 видов в верхней части сетевой панели, позволяет переключаться между различным содержимым сетевых элементов, в зависимости от типов конечных точек, с которами вы хотите работать.
4. Меню **Фильтры**, доступное в верхней части сетевой панели, легко позволяет отображать только определенные сетевые объекты, предоставляя несколько способов фильтрации. Опции меню **Фильтры** связаны с вариантами отображения выбранной сети.

Из раздела **Сеть** вы также можете управлять инсталляционными пакетами и задачами для каждого типа сетевых объектов.

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

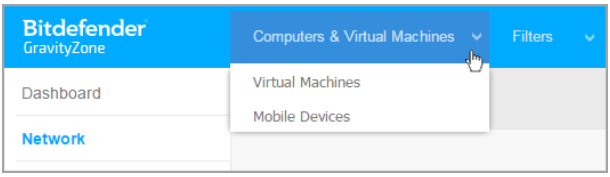
Для получения подробной информации о сетевых объектах, обратитесь к:

- «Виды сетей» (p. 41)
- «Компьютеры» (p. 43)
- «Виртуальные машины» (p. 83)
- «Просмотр и управление задачами» (p. 129)
- «Удаление конечных точек из сетевого содержимого» (p. 133)
- «Настройка параметров сети» (p. 135)
- «Диспетчер учетных данных (Credentials Manager)» (p. 138)

6.1. Виды сетей

Различные типы конечных точек, доступных в Control Center, сгруппированы в разделе **Сеть**, как различные виды сетей. Каждый вид сети отображает определенный тип сетевой инфраструктуры, содержащей типы конечных точек, которыми можно управлять.

Чтобы выбрать вид сети, перейдите в левую верхнюю часть раздела **Сеть** и нажмите меню видов:



Выбор просмотра

Доступны следующие виды сетей:

- Компьютеры и виртуальные машины
- Виртуальные машины

6.1.1. Компьютеры и виртуальные машины

Этот вид предназначен для компьютеров и виртуальных машин, интегрированных в Active Directory и предоставляет определенные действия и параметры фильтрации для управления сетевыми компьютерами. Если интеграция с Active Directory выполнена, дерево Active Directory загружается вместе с соответствующими конечными точками.

При работе с видом **Компьютеры и виртуальные машины**, вы можете в любое время синхронизировать содержимое Control Center с Active Directory, используя кнопку **Синхронизировать с Active Directory** панели инструментов.

В то же время, все компьютеры и виртуальные машины, которые не интегрированы в Active Directory сгруппированы в пользовательские группы (Custom Groups). Эта группа может содержать следующие типы конечных точек:

- Компьютеры и виртуальные машины, доступные в вашей сети вне Active Directory.
- Виртуальные машины из виртуализированной инфраструктуры доступной в вашей сети.

Важно

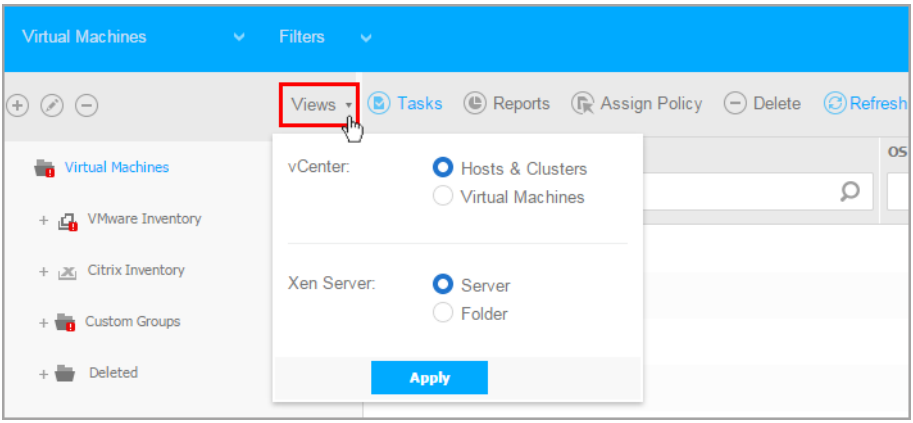
Назначение политик виртуальным машинам из меню **Компьютеры и виртуальные машины** может быть запрещена менеджером решения GravityZone при конфигурировании vCenter Server или Xen Server на странице **Конфигурация > Поставщики средств виртуализации**. Чтобы узнать больше, обратитесь к главе **Установка защиты > GravityZone Установка и настройка** из руководства по установке GravityZone.

6.1.2. Виртуальные машины

Данный вид специально разработан для отображения интеграции вашей виртуальной инфраструктуры. параметры фильтрации доступные в этом окне, позволяют задать специальные критерии для отображения объектов виртуальной среды.

Вы можете просмотреть виртуальные ресурсы Nutanix, VMware или Citrix на левой панели.

В верхней части левой панели вы также можете найти меню **Views**, позволяющее вам выбрать режим отображения виртуального содержимого.



Раздел Сеть - Меню виртуальных машин

Все виртуальные машины в вашей сети, которые не интегрированы в виртуальную инфраструктуру, отображаются как пользовательские группы (**Пользовательские группы**).

Для доступа к виртуальной инфраструктуре, интегрированной с Control Center, вы должны указать пользовательские данные для каждого доступного vCenter Server. Control Center использует ваши учетные данные для подключения к виртуальной инфраструктуре, отображая только те ресурсы, к которым у вас есть доступ (задается в vCenter Server). Если вы не указали ваши авторизационные учетные данные, вы должны будете ввести их, когда будете пытаться просматривать ресурсы любого vCenter Server. Единожды введя ваши учетные данные, они будут сохранены в вашем менеджере учетных данных и вам не придется вводить их повторно в дельнейшем.

6.2. Компьютеры

Чтобы увидеть под вашей учетной записью компьютеры, перейдите в раздел **Сеть** и выберите **Компьютеры и виртуальные машины** из меню видов.

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 отображения детальной информации о компьютерах 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 **Сеть**, вы можете выполнить следующие действия с компьютерами:

- Проверить статус компьютера
- Получить сведения о компьютере
- Организовать компьютеры в группы
- Выполнить сортировку, фильтрацию и поиск
- Управление патчами
- Запустить задачи
- Сформировать быстрые отчеты
- Назначить политики
- Синхронизироваться с Active Directory

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.

6.2.1. Проверка статуса компьютера

Каждый компьютер представлен на странице сети, иконкой определенного типа и состояния.

Обратитесь к «Типы сетевых объектов и статусы» (p. 316), чтобы просмотреть список со всеми доступными типами значков и статусов.

Для получения подробной информации о статусе, обратитесь к:

- Состояние управления
- Состояние подключения
- Статус безопасности

Состояние управления

Компьютеры могут иметь следующие статусы управления:

- **Управляемые** - компьютеры, на которых установлен агент безопасности.

- **Ожидают перезагрузки** - конечные точки, которые требуют перезагрузки системы после установки или обновления системы защиты Bitdefender.
- **Неуправляемые** - обнаруженные компьютеры, на которых агенты безопасности еще не были установлены.
- **Удаленные** - компьютеры, которые вы удалили из Control Center. Для получения более подробной информации, обратитесь к «Удаление конечных точек из сетевого содержимого» (p. 133).

Состояние подключения

Состояние подключения может отображаться только для управляемых машин. Исходя из этого управляемые компьютеры могут быть:

- **Онлайн**. Синий значок означает, что компьютер находится в сети.
- **Офлайн**. Серый значок означает, что компьютер находится в автономном режиме.

Компьютер переходит в автономный режим, если агент безопасности неактивен более 5 минут. Возможные причины, по которым компьютеры находятся в автономном режиме:

- Компьютер выключен, в режиме сна или гибернации.

  Примечание
  Компьютер остается в режиме online, даже когда он заблокирован или пользователь отключен.

- У агента безопасности нет подключения к коммуникационному серверуGravityZone:
  – Компьютер может быть отключен от сети.
  – Сетевой брандмауэр или маршрутизатор может блокировать связь между агентом безопасности и коммуникационным сервером GravityZone.
  – Компьютер находится за прокси-сервером и настройки прокси-сервера не были правильно настроены в примененной политике.

  Предупреждение
  Для компьютеров за прокси-серверером, настройки прокси-сервера должны быть правильно сконфигурированы в установочном пакете агента безопасности, в противном случае компьютер не сможет

соединиться с консолью GravityZone и всегда будет появляться в автономном режиме, независимо от того, что политика с правильными настройками прокси-сервера была применена после установки.

- Агент безопасности может быть удален вручную с компьютера, пока отсутствует соединение с GravityZone Control Center. Обычно, когда агент безопасности удаляется с компьютера вручную, Control Center уведомляется об этом событии и компьютер помечается как неуправляемый.
- Агент безопасности работает ненадлежащим образом.

Чтобы узнать, как долго компьютеры были неактивны:

1. Отобразите только управляемые компьютеры. 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 **Последний просмотр**, чтобы отсортировать компьютеры по периоду бездействия.

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

Более длительные периоды бездействия (дни, недели), как правило, указывает на проблему с компьютером.

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

Статус безопасности

Состояние безопасности может отображаться только для управляемых машин. Вы можете определить компьютеры с проблемами безопасности, проверяя значки состояния, отображающие символ предупреждения:

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

Компьютер может 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:
  - Компьютер имеет проблемы с подключением к Интернету.
  - 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 компьютер с проблемами безопасности, нажмите на его имя, чтобы отобразить окно **Информация**. 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.

6.2.2. Получение сведений о компьютере

На странице **Сеть** можно узнать подробные сведения о каждом компьютере следующим образом:

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

Проверка страницы сети

Чтобы узнать подробную информацию о компьютере, проверьте данные в таблице правой панели 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 **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемую группу в левой панели.

   Все доступных конечные точки выбранной группы выводятся в таблице правой панели.
4. Вы можете легко определить состояние компьютера, проверив соответствующий значок. Для получения дополнительной информации перейдите к «Проверка статуса компьютера» (p. 44).
5. Проверьте информацию, отображаемую в столбцах для каждого компьютера.

   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.

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"

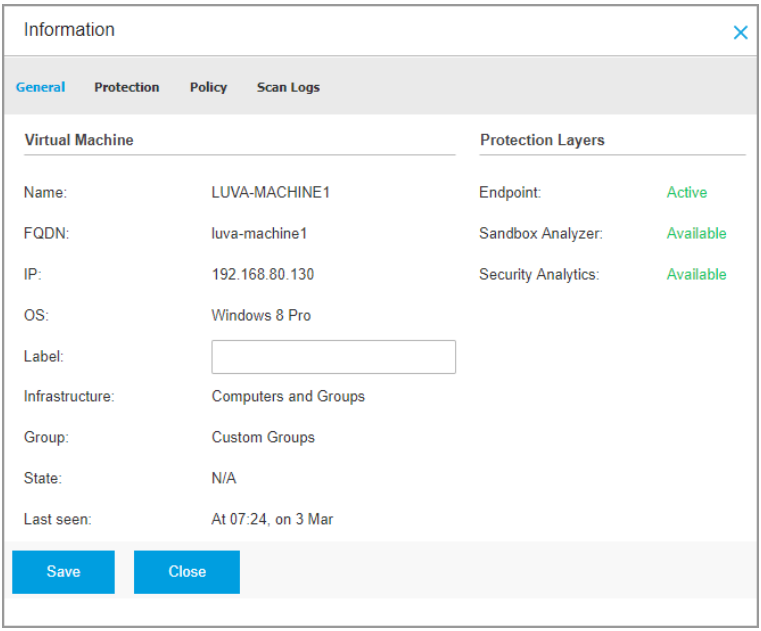
- Общие сведения о компьютере, например, имя, полное доменное имя, IP-адрес, операционная система, инфраструктура, родительская группа и текущее состояние соединения.

  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 компьютеров» (p. 63).

- 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.



Информационное окно - вкладка «Общие»

Вкладка "Защита"

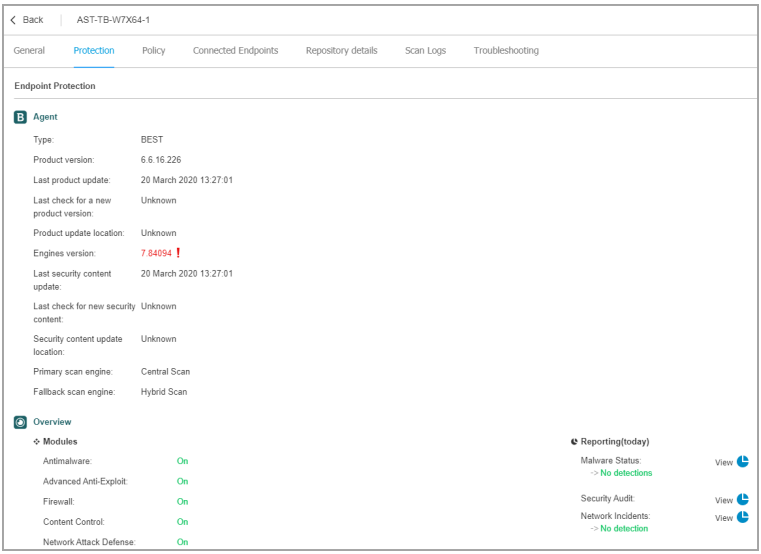
Эта вкладка содержит сведения о каждом уровне защиты, применимом на конечной точке.

- Сведения об агенте безопасности, такие как название продукта, версия, статус обновления и расположение обновлений, а также конфигурация механизмов сканирования и версии содержимого безопасности
- 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. 46).

- 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. 264)
- 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. ???.
- 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"

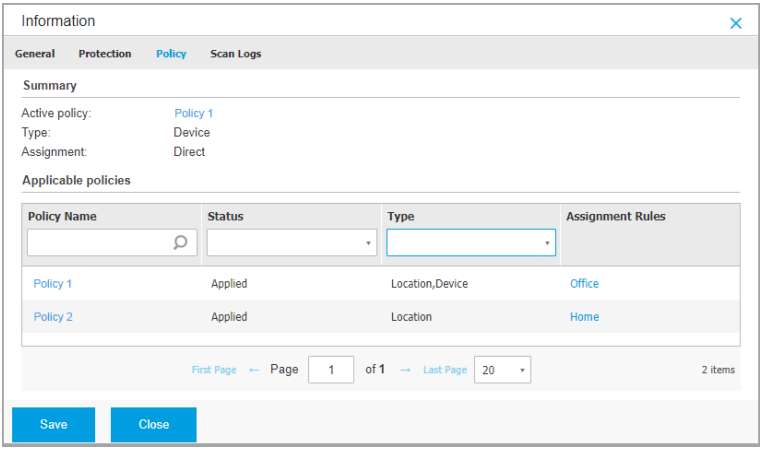
Конечная точка может применяться с одной или несколькими политиками, но одна политика может быть активна только с одной конечной точкой. На вкладке **Политика** отображаются сведения о всех политиках, применяемых к конечной точке.

- 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.
  - **Внешний (NSX)**: если политика определена в среде VMware NSX.
- 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.

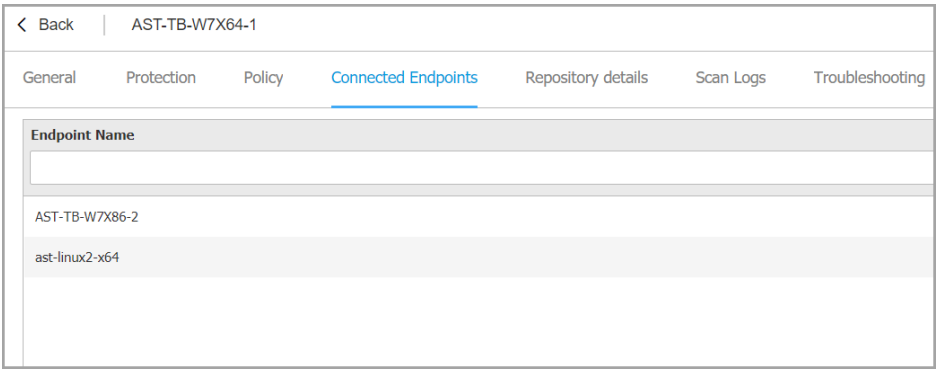


Информационное окно - вкладка «Политика»

Для получения дополнительной информации, касающейся политики, см.«Изменение настроек политики» (p. 153)

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.

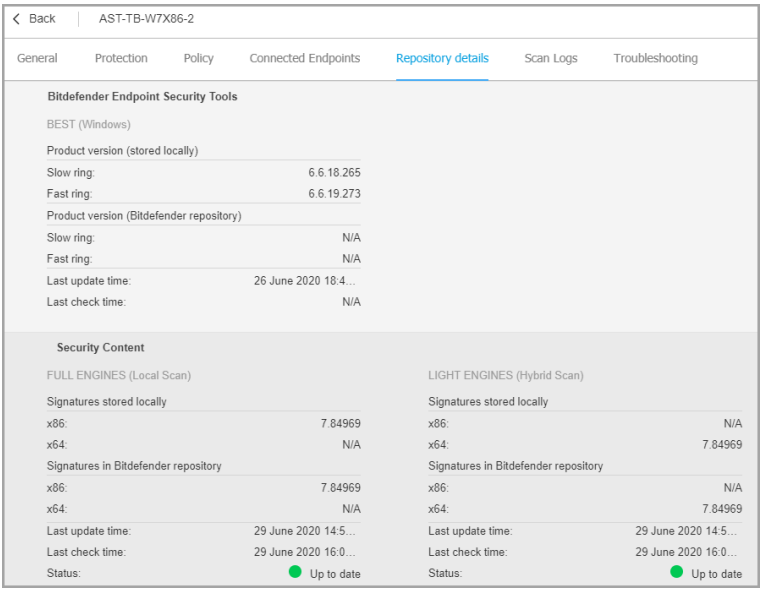


Информационное окно - вкладка подключенных конечных точек

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.



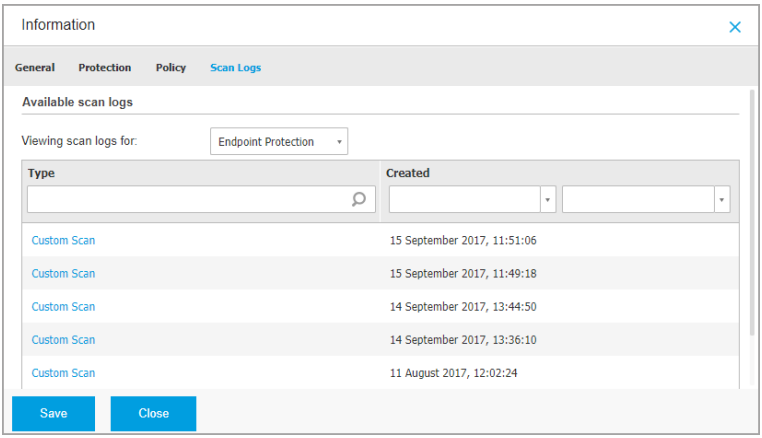
Информационное окно - вкладка содержимого репозитория

Вкладка "Журналы сканирования"

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

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.

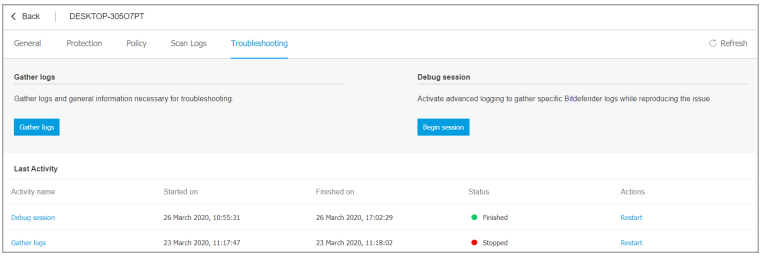


Информационное окно - вкладка «Журналы сканирования»

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 неисправностей доступно лишь для Windows,Linux, macOS и всех типов серверов безопасности.



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.

   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) в зависимости выбранного местоположения.
4. Нажмите кнопку **Сбор журналов**.

- **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
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

Тип проблемы	Сценарий использования
	– 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 – 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.

   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) 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.

6.2.3. Организация компьютеров в группы

Вы можете управлять группами компьютеров в левой панели раздела **Сеть**.

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

Компьютеры, импортированные из Active Directory, сгруппированы в папку **Active Directory**. Вы не можете редактировать группы Active Directory. Вы можете только просматривать и управлять соответствующими компьютерами.

Все обнаруженные в сети компьютеры не-Active Directory, находятся в **Пользовательские группы**, где можно организовать их в группы по вашему усмотрению. В **Пользовательские группы** вы можете создавать, удалять , переименовывать и перемещать группы компьютеров в произвольной древовидной структуре.

Примечание

- Группа может содержать как компьютеры, так и другие группы.
- При выборе группы в левой панели, вы можете просмотреть все компьютеры кроме тех, которые находятся в своих подгруппах. Для просмотра всех компьютеров, входящих в группу и в свои подгруппы, нажмите меню **Фильтры**, расположенное в верхней части таблицы и выберите **Все предметы рекурсивно** в разделе **Глубина**.

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 **Пользовательские группы** в левой панели.
2. Нажмите кнопку ⊕ **Добавить группу** в верхней части левой панели.

3. Введите подходящее имя группы и нажмите **OK**. Новая группа появится в разделе **Пользовательские группы**.

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 компьютеров

Вы можете перемещать объекты **Пользовательские группы** 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. 141).

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**.

6.2.4. Сортировка, фильтрация и поиск компьютеров

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 конкретный компьютер или выбрать для просмотра только управляемые компьютеры.

Сортировка компьютеров

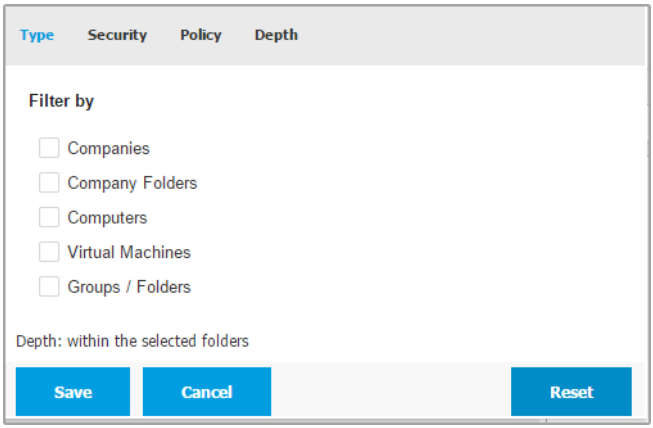
Для сортировки данных по определенному столбцу, щелкните заголовок столбца. Например, если вы хотите отсортировать компьютеры по имени, щелкните на заголовок **Имя**. При повторном нажатии на заголовок компьютеры будут отображаться в обратной последовательности.

Сортировка компьютеров

Фильтрация компьютеров

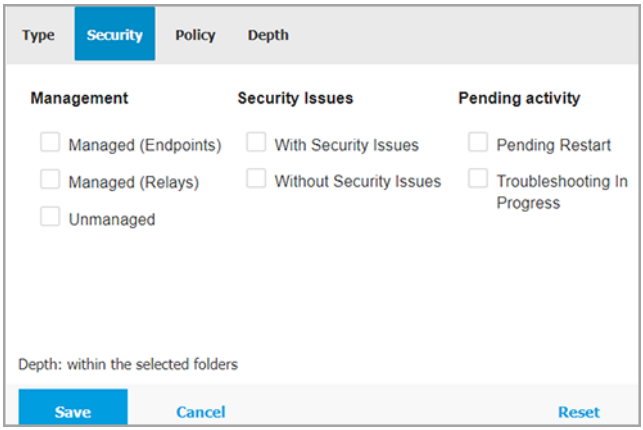
Чтобы отфильтровать ваши сетевые объекты, используйте меню **Фильтры** в правой верхней части сетевой панели.

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).



Компьютеры - Фильтрация по типу

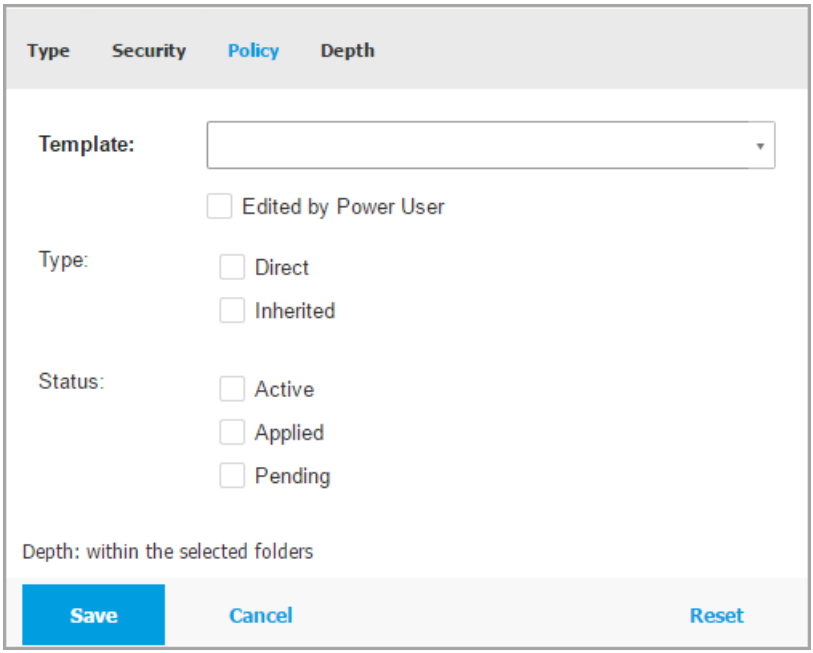
- **Безопасность**. Выберите отображение компьютеров по управлению защитой, состоянием безопасности или ожидающими действиями.



Компьютеры - Фильтрация по безопасности

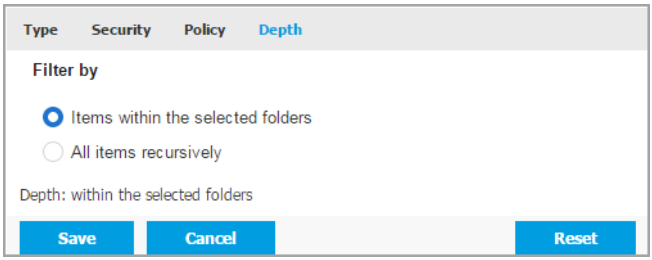
- **Политика**. Выберите шаблон политики, для которого нужно фильтровать компьютеры, тип назначения политики (прямой или наследуемый), а также статус назначения политики (активный, применяемый или в ожидании). Вы также можете выбрать для отображения объекты только

с политиками, отредактированными привилегированными пользователями.



Компьютеры - Фильтрация по политикам

- **Глубина**. При управлении структурированной сетью, компьютеры в подгруппах не будут отображаться при выборе корневой группы. Чтобы просмотреть все компьютеры, входящие в текущую группу и все подгруппы, выберите **Все элементы рекурсивно**.



Компьютеры - 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.

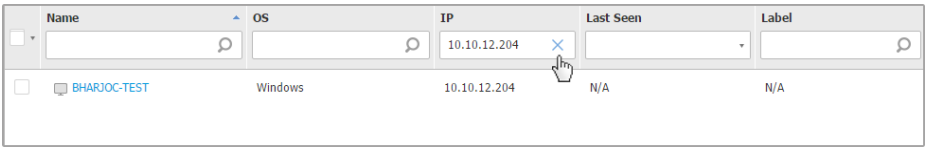
Примечание
Вы можете просмотреть все выбранные критерии фильтрации в нижней части окна **Filters**.
Если вы хотите очистить все фильтры, нажмите кнопку **сбросить**.

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

Поиск компьютеров

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 компьютера, который вы ищете в поле **IP**. В таблице отобразится только соответствующий компьютер.

   Очистите окно поиска, чтобы отобразить полный список компьютеров.



Поиск компьютеров

6.2.5. Запущенные Задачи

В разделе **Сеть** вы можете удаленно запускать на компьютерах ряд администраторских задач.

Вы можете выполнить следующие задачи:

- «Установить» (p. 69)
- «Удаление клиента» (p. 75)
- «Обновление клиента» (p. 76)
- «Перенастройка клиента» (p. 76)
- «Обслуживание клиента» (p. 78)
- «Перезагрузка машины» (p. 79)
- «Сетевое Обнаружение» (p. 80)

Вы можете создавать задачи отдельно для каждого компьютера или для групп компьютеров. Например, вы можете удаленно установить агент безопасности группе неуправляемых компьютеров. Позже, вы можете создать задачу сканирования определенного компьютера в этой группе.

Для каждого компьютера вы можете запускать только совместимые задачи. Например, если вы выберите неуправляемый компьютер, то вы можете выбрать только установку агента безопасности, все другие задачи будут недоступны.

Задача, выбранная для группы, будет выполнена только на совместимых компьютерах. Если ни один из компьютеров в группе не совместим с выбранной задачей, вы будете уведомлены, что задача не может быть выполнена.

После создания, задача запустится сразу же, когда компьютеры будут онлайн. Если компьютер находится в автономном режиме, задание начнет выполняться, как только он подключится к сети.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 129).

Установить

Для защиты компьютеров с агентом безопасности Bitdefender, необходимо установить его на каждом из них.

Важно

В изолированных сетях, которые не имеют прямой связи с устройствами GravityZone, вы можете установить агента безопасности с ролью Роь ретранслятора В этом случае, связь между устройством GravityZone и другими агентами безопасности будет осуществляться через агента ретрансляции, который также будет выступать в качестве локального сервера обновлений для агентов безопасности, защищающих изолированную сеть.
После того, как вы установили агента ретрансляции, он будет автоматически обнаруживать незащищенные компьютеры в этой же сети.

Примечание

- Рекомендуется чтобы компьютер, на котором вы установите агента ретрансляции, был всегда включен.
- Если агент ретрансляции не установлен в сети, обнаружение незащищенных компьютеров может быть сделано вручную путем запуска задачи **Обнаружение сети**.

Защита Bitdefender может быть установлена на компьютерах 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:

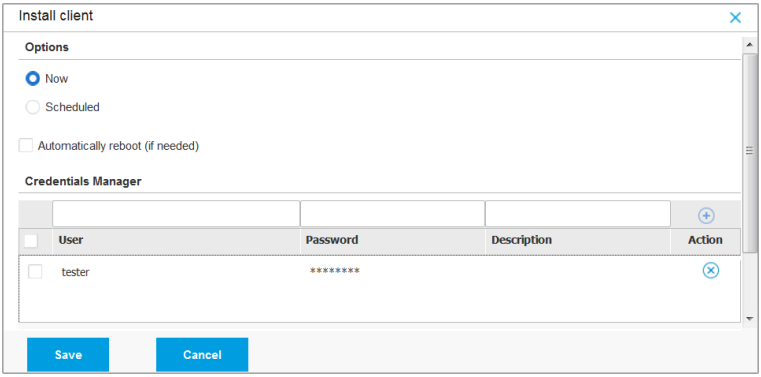
1. Подключитесь и войдите в Control Center.
2. Перейдите в раздел **Сеть**.
3. Выберите **компьютеры и виртуальные машины** из меню видов сетей.
4. Выберите нужную группу в левой панели. Объекты, содержащиеся в выбранной группе, будут отображены в таблице правой панели.

   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**.

5. Выберите объекты (конечные точки или группы конечных точек), на которых вы хотите установить защиту.

6. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Установить**.

   Отобразится мастер установки **Install Client**.



7. 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.

8. Если вы хотите, чтобы заданные конечные точки перезапустились после завершения установки, выберите **Автоматическая перезагрузка (при необходимости)** .
9. 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.

10. 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.

11. В разделе **Установщик**, выберите объект, к которому выбранные конечные точки будут подключаться для установки и обновления клиента:

- **GravityZone Appliance**, если конечные точки будут подключаться непосредственно к устройству GravityZone.

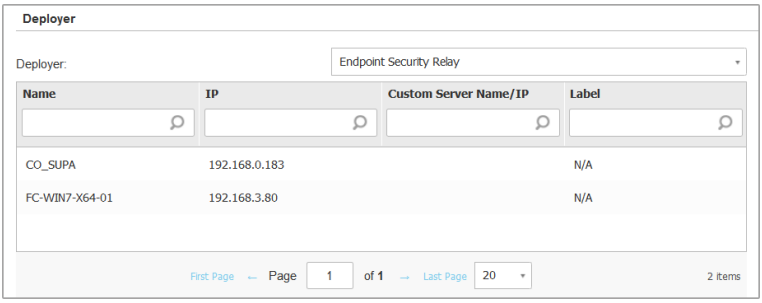
  В этом случае, вы также можете указать:

  – Пользовательский коммуникационный сервер, набрав его IP-адрес или имя хоста, в случае необходимости.

  – Настройки прокси-сервера, если требуемые конечные точки будут общаются с устройством GravityZone через прокси-сервер. В этом случае выберите **Использовать прокси для общения** и введите необходимые параметры прокси-сервера в полях ниже.

- **Ретранслятор безопасности конечной точки**, если вы хотите подключить конечные точки к клиенту Relay, установленному в вашей сети. Все машины с ролью ретранслятора, обнаруженные в вашей сети, будут отображены в таблице ниже. Выберите компьютер с ролью ретранслятора, который Вам нужен. 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.



12. Используйте раздел **Дополнительные цели**, если вы хотите развернуть клиента на определенных машинах в вашей сети, которые не отображаются в сетевом содержимом. Раскройте раздел и введите через запятую IP-адреса или имена хостов этих машин в специальном поле. Вы можете добавить столько IP-адресов, сколько вам нужно.
13. 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.
14. 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.
15. Нажмите **Сохранить**. Появится окно подтверждения.

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

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. 264).

Удаление клиента

Для удаленного удаления защиты Bitdefender:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемый контейнер в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
4. Выберите флажки на компьютерах, с которых вы хотите удалить агент безопасности Bitdefender.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Удалить клиента**.
6. Появится окно конфигурации, которое позволит вам сделать следующие настройки:
   - Вы можете выбрать хранение объектов карантина на клиентской машине.
   - Для интегрированной среды vShield, вы должны выбрать необходимые учетные данные для каждой машины, в противном случае удаление не произойдет. Выберите **Используйте учетные данные для интеграции vShield**, затем ниже проверьте все соответствующие учетные данные в таблице диспетчера учетных данных.
7. 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» (p. 129).

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

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. 46).

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 **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемый контейнер в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
4. Установите флажки на компьютерах, на которых вы хотите запустить обновление клиента.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обновить**. Появится окно настроек.
6. Вы можете обновить только продукт, только механизмы защиты или всё сразу.
7. 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» (p. 129).

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 одного или нескольких компьютеров:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемую группу в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
4. Установите флажки компьютеров, для которых вы хотите изменить параметры установки.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Перенастроить клиента**.
6. 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.
7. 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.

8. Выберите **Удалить конкурентов, если это необходимо**, чтобы убедиться, что выбранные модули не будут конфликтовать с другими решениями безопасности, установленными на целевых конечных точках.
9. 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**.

10. 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.
11. 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» (p. 129).

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.
- Задача восстановления сбросит агент безопасности до версии, опубликованной на странице **Configuration > Update > Components**.

Чтобы Repair Client task клиенту на ремонт:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемый контейнер в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
4. Установите флажки на компьютерах, на которых Вы хотите запустить исправление клиента.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Исправление клиента**. Появится окно подтверждения.
6. 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» (p. 129).

Перезагрузка машины

Вы можете удаленно перезагрузить управляемые компьютеры.

Примечание
Проверьте страницу **Сеть > Задачи** перед перезапуском определенных компьютеров. Ранее созданные задачи еще могут быть в процессе выполнения на выбранных компьютерах.

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.

3. Выберите желаемый контейнер в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
4. Отметьте флажками компьютеры, которые вы хотите перезагрузить.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Перезагрузить машину**.
6. Выберите опции перезагрузки по расписанию:
   - Выберите **Перезапустить сейчас**, чтобы немедленно перезагрузить компьютеры.
   - Выберите **Включить перезагрузку** и используйте поля ниже, чтобы запланировать перезагрузку в определенную дату и время.
7. 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» (p. 129).

Сетевое Обнаружение

Обнаружение сети выполняется автоматически агентами безопасности с ролью ТРАНСЛЯТОР . Если у вас в сети нет агента ретрансляции, вам придется вручную запускать задачу сетевого обнаружения из защищенной конечной точки.

Чтобы запустить задачу сетевого обнаружения в вашей сети:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемый контейнер в левой панели. Все компьютеры выбранного контейнера отобразятся в таблице правой панели.
4. Отметьте флажком компьютер, на котором вы хотите выполнить сетевое обнаружение.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обнаружение сети**.
6. 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» (p. 129).

6.2.6. Формирование быстрых отчетов

Вы можете создавать быстрые отчеты на управляемых компьютерах, используя страницу **Сеть**:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите требуемую группу в левой панели. Все компьютеры из выбранной группы отобразятся в таблице правой панели.

   При желании, вы можете отфильтровать содержимое выбранной группы только для управляемых компьютеров.
4. Отметьте флажками компьютеры, которые вы хотите включить в отчет.
5. Нажмите кнопку **Отчет** в верхней части таблицы и выберите из меню тип отчета.

   Для получения более подробной информации, обратитесь к «Типы отчетов» (p. 261).
6. Настройте параметры отчета. Для получения более подробной информации, обратитесь к «Создание отчетов» (p. 264).
7. Нажмите **Создать**. Отчет отобразится немедленно.

   Время, необходимое для формирования отчетов, может изменяться в зависимости от количества выбранных компьютеров.

6.2.7. Назначение политик

Вы можете управлять настройками безопасности на компьютерах с помощью политики.

В разделе **Сеть** вы можете просматривать, изменять и назначать политики для каждого компьютера или группы компьютеров.

Примечание
Настройки безопасности доступны только для управляемых компьютеров. Для облегчения просмотра и управления настройками безопасности, вы можете отфильтровать сетевое содержимое только для управляемых компьютеров.

Для просмотра политики, назначенной определенному компьютеру:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемую группу в левой панели. Все компьютеры из выбранной группы отображаются в таблице правой панели.
4. Нажмите на имя управляемого компьютера, который вам необходим. Появится информационное окно.
5. На вкладке **Общее**, в разделе **Политика**, нажмите на название текущей политики, чтобы просмотреть ее настройки.
6. Вы можете изменить настройки безопасности в случае необходимости, при условии, что владелец политики позволил другим пользователям вносить в нее изменения. Пожалуйста, обратите внимание, что любое изменение, которое вы делаете, влияет на все компьютеры с такой же политикой.

   Для получения более подробной информации о настройках политик компьютера, обратитесь к «Политики компьютеров и виртуальных машин» (p. 154).

Чтобы назначить политику компьютеру или группе:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Выберите желаемую группу в левой панели. Все компьютеры из выбранной группы отображаются в таблице правой панели.
4. Отметьте флажком компьютер или группу, которую вы хотите выбрать. Вы можете выбрать один или несколько объектов одного типа, только одного уровня.
5. Нажмите кнопку **Назначить политику** в верхней части таблицы.
6. Сделайте необходимые настройки в окне **Назначение политики**. Для получения более подробной информации, обратитесь к ???.

6.2.8. Синхронизация со службой каталогов Active Directory

Сетевое содержимое автоматически синхронизируется с Active Directory через интервал времени, заданный в разделе конфигурации Control Center. Более подробную информацию см. в главе GravityZone по установке и настройке в руководстве по установке GravityZone

Чтобы вручную синхронизировать отображаемое в данный момент содержимое сети с Active Directory:

1. Перейдите в раздел **Сеть**.
2. Выберите **Компьютеры и виртуальные машины** из меню видов.
3. Нажмите кнопку **Синхронизировать с Active Directory** в верхней части таблицы.
4. Вы должны будете подтвердить ваши действия, нажав **Да**.

Примечание

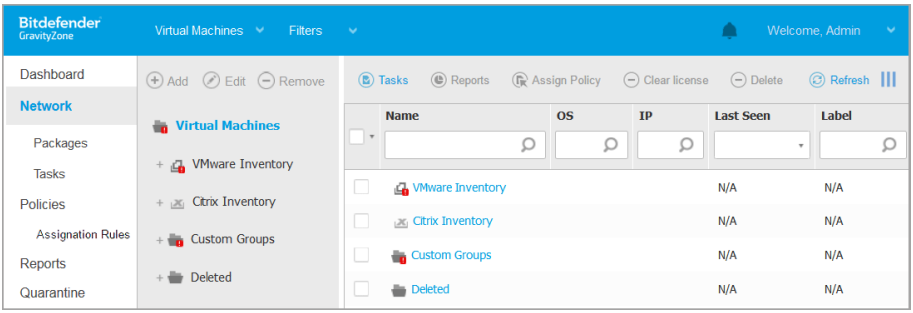
Для больших сетей со службой каталогов Active Directory завершение синхронизации может занять больше времени.

6.3. Виртуальные машины

Для просмотра виртуальной инфраструктуры под своей учетной записью, перейдите в раздел **Сеть** и выберите **Виртуальные машины** из меню видов сетей.

Примечание

Вы можете управлять виртуальными машинами также из **Компьютеры и виртуальные машины**, но просматривать виртуализированную инфраструктуру и фильтровать ее содержимое, используя специальные критерии, вы можете только используя вид **Виртуальные машины**.
За более подробной информацией о работе с видами сетей, обратитесь к «Виды сетей» (p. 41).



Сеть - Просмотр виртуальных машин

Вы можете увидеть доступные виртуальные машины в левой панели и детальную информацию о каждой виртуальной машине на панели справа.

Для настройки отображения детальной информации о виртуальных машинах в таблице:

1. Нажмите на кнопку **Колонки** в правой верхней части правой панели.
2. Выберите столбцы, которые вы хотите отобразить.
3. Нажмите кнопку **Восстановить**, чтобы вернуться к виду столбцов по умолчанию.

Левая панель отображает дерево каталогов виртуальной инфраструктуры. Корень дерева называется **Виртуальные машины** и виртуальные машины сгруппированы под корнем, в следующих категориях, основанных на технологии виртуализации поставщика:

- **Инвентаризация Nutanix .** Содержит список систем Nutanix Prism Element, к которым у вас есть доступ.
- **Содержимое VMware.** Содержит список серверов vCenter, к которым у вас есть доступ.
- **Содержимое Citrix.** Содержит список систем XenServer, к которым у вас есть доступ.
- **Пользовательские группы.** Содержит виртуальные машины, обнаруженные в вашей сети за пределами любого сервера vCenter или системы XenServer.

Левая панель также содержит вверху меню под названием **Виды**, из которого пользователь может выбрать тип представления для каждого поставщика технологии виртуализации.

Для доступа к виртуальной инфраструктуре, интегрированной с Control Center, вы должны указать пользовательские данные для каждого доступного vCenter Server. Единожды введя ваши учетные данные, они будут сохранены в вашем менеджере учетных данных и вам не придется вводить их повторно в дельнейшем. Для получения более подробной информации, обратитесь к «Диспетчер учетных данных (Credentials Manager)» (p. 138).

В разделе **Сеть**, вы можете управлять виртуальными машинами следующим образом:

- Проверять состояние виртуальных машин
- Просмотр сведений о виртуальной машине
- Организовывать виртуальные машины в группы
- Выполнить сортировку, фильтрацию и поиск
- Запустить задачи
- Сформировать быстрые отчеты
- Назначить политики

В разделе **Настройки > Настройки сети** вы можете настроить Запланированные правила для автоматической очистки неиспользованных виртуальных машин из инвентаризации сети.

6.3.1. Проверять статусы виртуальных машин

Каждая виртуальная машина представленая на странице сети, иконкой определенного типа и состояния.

Обратитесь к «Типы сетевых объектов и статусы» (p. 316), чтобы просмотреть список со всеми доступными типами значков и статусов.

Для получения подробной информации о статусе, обратитесь к:

- Состояние управления
- Состояние подключения
- Статус безопасности

Состояние управления

Виртуальные машины могут иметь следующие статусы управления:

- **Управляемые** - виртуальные машины, на которых установлена защита Bitdefender.
- **Ожидание перезапуска** - виртуальные машины, которые требуют перезагрузки системы после установки или обновления системы защиты Bitdefender.
- **Неуправляемые** - обнаруженные виртуальные машины, на которых защита Bitdefender еще не была установлена.
- **Удаленные** - виртуальные машины, которые вы удалили из Control Center. Для получения более подробной информации, обратитесь к «Удаление конечных точек из сетевого содержимого» (p. 133).

Состояние подключения

Состояние подключения относится только к управляемым виртуальным машинам. Следовательно, управляемые виртуальные машины могут быть:

- **Онлайн**. Синий значок означает, что компьютер находится в сети.
- **Офлайн**. Серый значок означает, что компьютер находится в автономном режиме.

Виртуальная машина переходит в автономный режим, если агент безопасности неактивен более 5 минут. Причины, по которым виртуальные машины могут находится в автономном режиме:

- Виртуальная машина выключена, в режиме сна или гибернации.

  Примечание
  Виртуальные машины продолжают оставаться в статусе online, даже если они заблокированы или пользователь отключен.

- У агента безопасности нет подключения к коммуникационному серверуGravityZone:
  – Виртуальные машины могут быть отключены от сети.
  – Сетевой брандмауэр или маршрутизатор может блокировать связь между агентом безопасности и коммуникационным сервером GravityZone.
  – Виртуальная машина находится за прокси-сервером и настройки прокси-сервера не были правильно настроены в примененной политике.

Предупреждение
Для виртуальных машин за прокси-серверером, настройки прокси-сервера должны быть правильно сконфигурированы в установочном пакете агента безопасности, в противном случае виртуальная машина не будет общаться с кансолью GravityZone и всегда будет появляться в автономном режиме, независимо от того, что политика с правильными настройками прокси была применена после установки.

- Агент безопасности может быть удален вручную с виртуальной машины, пока виртуальная машина не имеет соединения с GravityZone Control Center. Обычно, когда агент безопасности вручную удален из виртуальной машины, Control Center уведомляет об этом событии, и виртуальная машина помечается как неуправляемая.
- Агент безопасности работает ненадлежащим образом.

Чтобы узнать, как долго виртуальные машины были неактивны:

1. Показывать только управляемые виртуальные машины. 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. Щелкните на столбец **Последняя активность**, чтобы отсортировать виртуальные машины по периоду бездействия.

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

Более длительные периоды бездействия (дни, недели), как правило, указывает на проблему с виртуальной машиной.

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

Статус безопасности

Состояние безопасности относится только к управляемым виртуальным машинам. Вы можете определить виртуальные машины или Security Serverы

с проблемами безопасности, проверяя значки состояния, отображающие символ предупреждения:

- Имеются проблемы.
- Проблем не обнаружено.

Виртуальная машина или Security Server имеет проблемы с безопасностью, предусмотренные по крайней мере в одной из следующих ситуациях:

- Защита от вредоносных программ отключена.
- Срок действия лицензии истек.
- Продукт Bitdefender устарел.
- Механизмы защиты устарели.
- Обнаружены вредоносные программы.
- Связь с Bitdefender Cloud Services не может быть установлена из-за следующих возможных причин:
  - Виртуальная машина имеет проблемы с подключением к Интернету.
  - 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 виртуальную машину с проблемами безопасности, нажмите на ее имя, чтобы отобразить окно **Информация**. 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.

Конечные точки, которые не получают обновлений в течение последних 24 часов, автоматически помечаются как **Содержит угрозы**, независимо от версии содержимого безопасности, присутствующей на ретрансляторе или в GravityZone Update Server.

6.3.2. Просмотр подробной информации о виртуальной машине

Подробные сведения о каждой виртуальной машине можно узнать на странице **Сеть** следующим образом:

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

Проверка страницы сети

Для того, чтобы узнать подробную информацию о виртуальной машине, проверьте информацию в таблице правой панели на странице **Сеть**.

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

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемую группу в левой панели.

   Все виртуальные машины, доступные в выбранной группе, отображаются в правой панели таблицы.
4. Вы можете легко определить состояние виртуальной машины, проверив соответствующий значок. Для получения дополнительной информации перейдите к «Проверять статусы виртуальных машин» (p. 85).
5. Проверьте информацию, отображаемую в столбцах для каждой виртуальной машины.

   Используйте строку заголовка для поиска определенных виртуальных машин в соответствии с доступными критериями:

   - **Имя**: имя виртуальной машины.
   - **FQDN**: полное доменное имя, которое включает в себя имя хоста и имя домена.
   - **OS**: операционная система установленая на виртуальной машине.
   - **IP**: IP-адрес виртуальной машины.
   - **Последняя активность**: дата и время, когда виртуальная машина была в последний раз онлайн.

Примечание
Важно следить за полем **последняя активность**, длительные периоды бездействия могут указывать на проблему связи или отключенную виртуальную машину.

- **Ярлык** : настраиваемая строка с дополнительной информацией о рабочей станции. Можете добавить метку в **Окно** Информации виртуальной машины и затем использовать ее в поиске.
- **Политика**: политика, применяемая к виртуальной машине, содержит ссылку для просмотра или изменения параметров политики.

Проверка информационного окна

Для того, чтобы отобразить окно **Сведения**, щелкните имя интересующей вас виртуальной машины в правой боковой панели страницы **Сеть**. В этом окне отображаются сгруппированные по нескольким вкладкам данные, которые доступны только для выбранной виртуальной машины.

В окне **Информация** приведен полный список сведений в соответствии с типом виртуальной машины (виртуальная машина, экземпляр Security Server) и информация о ее безопасности.

Вкладка "Общие"

- Основная информация о виртуальной машине, например, имя, информация FQDN, IP-адрес, операционная система, инфраструктура, родительская группа и текущее состояние.

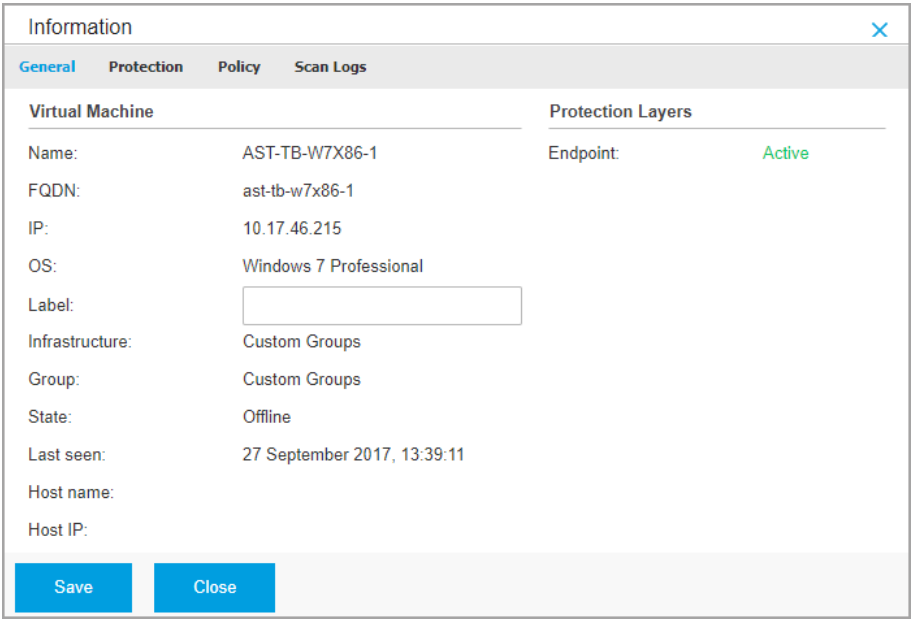
  В этом разделе вы можете поставить метку к виртуальной машине. Вы сможете быстро находить виртуальные машины с одной и той же меткой и принимать меры по отношению к ним, независимо от их расположения в сети. Для получения дополнительных сведений о фильтрации виртуальной машины перейдите к «Сортировка, фильтрация и поиск виртуальных машин» (p. 98).
- Сведения об уровнях защиты, в том числе список технологий безопасности, приобретенных при помощи решения GravityZone, и статус их лицензии, которые могут быть:
  - **Доступен/Активный** - на виртуальной машине активен лицензионный ключ для данного уровня защиты.

– **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 виртуальная машина.



Информационное окно - вкладка «Общие»

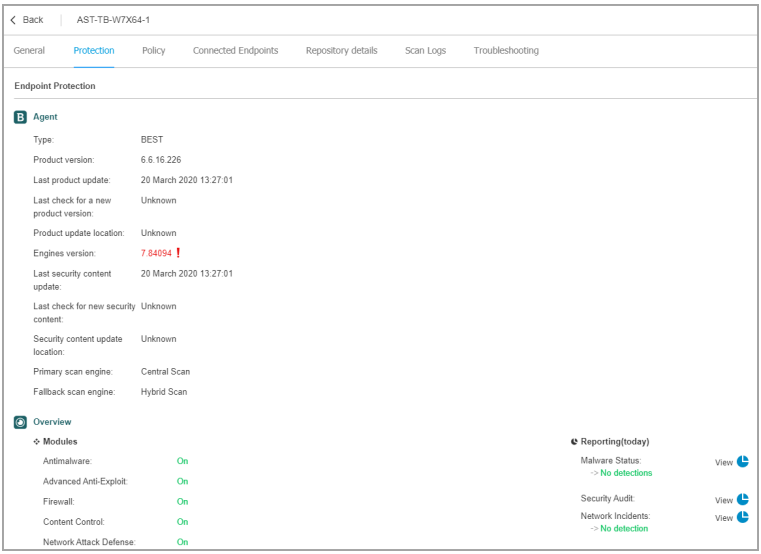
Вкладка "Защита"

Эта вкладка содержит сведения о каждом уровне защиты, лицензированном на конечной точке. Подробности содержат информацию о:

- Сведения о агентах безопасности, такие как название и версия продукта, состояние ядра сканирования и состояние обновлений.
- 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. 87).
- 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. 264)
- 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. 128).



Информационное окно - вкладка "Защита"

Вкладка "Политика"

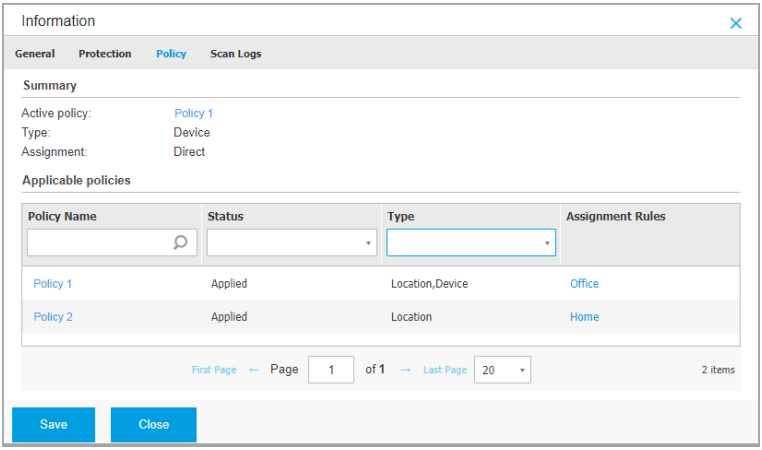
Виртуальная машина может применяться с одной или несколькими политиками, но одна политика может быть активна только с одной виртуальной машиной. Сведения о всех политиках, применяемых к виртуальной машине, отображены на вкладке **Политика**.

- 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 виртуальной машины.
  - **Местоположение**: политика, основываясь на правилах, автоматически назначается виртуальной машине в том случае, если сетевые настройки конечной точки соответствуют заданным условиям правил назначения .

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

    Например, машине может быть назначено две политики, зависящие от пользователя, одна для администраторов и одна для других сотрудников. Одна из политик становится активной, в зависимости от прав пользователя зашедшего на машину.

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

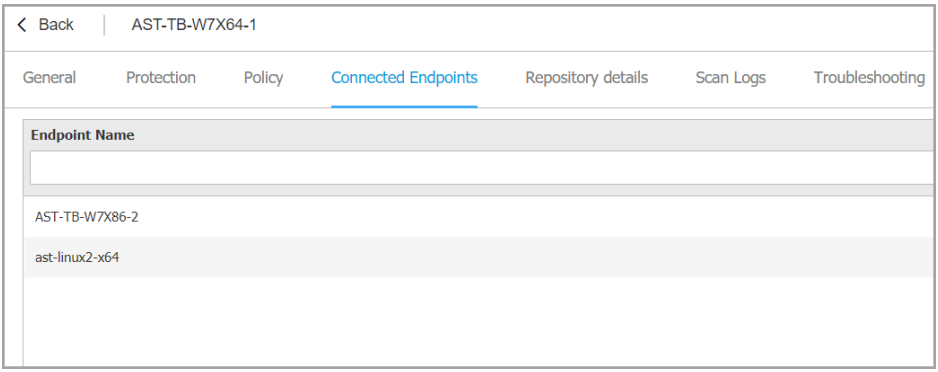


Информационное окно - вкладка «Политика»

Для получения дополнительной информации, касающейся политики, см.«Управление политиками» (p. 142)

Вкладка «Ретранслятор»

Вкладка **Ретранслятор** доступна только для виртуальных машин с ролями ретранслятора. Эта вкладка отображает информацию о конечных точках, подключенных к текущему ретранслятору, такую как имя, IP-адрес и метка.



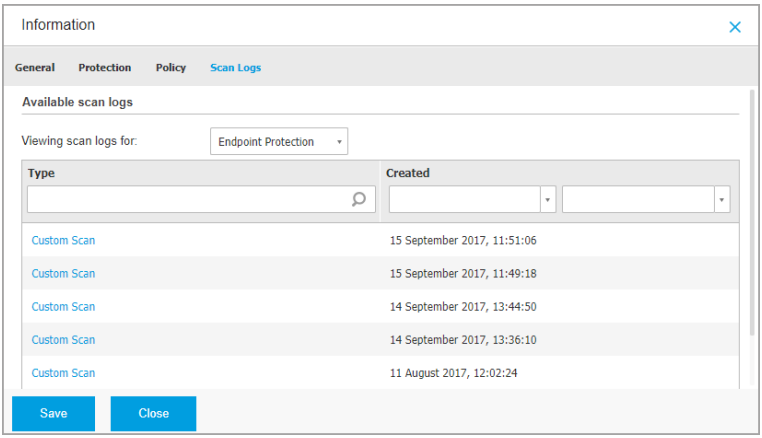
Информационное окно - вкладка «Ретранслятор»

Вкладка "Журналы сканирования"

Таблица **Сканирование журнаов** выводит подробные сведения обо всех задачах сканирования, выполненных на виртуальной машине.

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»

Каждое свойство , которое создает проблемы безопасности в этом окне помечено значком **!** . Наведите мышь на значок для появления подсказки, чтобы выяснить подробности. Могут потребоваться дальнейшие локальные расслдеования.

6.3.3. Организация виртуальных машин в группы

Вы можете управлять группами виртуальных машин в левой панели раздела **Сеть** из папки **Пользовательские группы**.

Виртуальные машины, импортированные из Nutanix Prism Element, сгруппированы в папке **Инвентаризация Nutanix**. Виртуальные машины, импортированные из VMware vCenter сгруппированы в папке **VMware Inventory**. Виртуальные машины, импортированные из XenServer сгруппированы в папке **Citrix Inventory**. Вы не можете редактировать Инвентаризацию Nutanix, Инвентаризацию VMware или Инвентаризацию Citrix. Вы можете только просматривать и управлять соответствующими виртуальными машинами.

Все виртуальные машины, которые не управляются системами Nutanix Prism, vCenter или XenServer, определяются Network Discovery и помещаются в **Пользовательские группы**, где вы можете организовать их в группы по своему усмотрению. Основным преимуществом этой возможности является то, что вы можете использовать групповые политики для решения различных требований безопасности.

В **Пользовательские группы** вы можете создавать, удалять, переименовывать и перемещать группы виртуальных машин, создавая требуемую древовидную структуру.

Примечание

- Группа может содержать как виртуальные машины, так и другие группы.
- При выборе группы в левой панели, вы можете просмотреть все виртуальные машины кроме тех, которые находятся в своих подгруппах. Для просмотра всех виртуальных машин, входящих в группу и в дочерние подгруппы, нажмите меню **Фильтры**, расположенное в верхней части таблицы и выберите **Все элементы рекурсивно** в разделе **Глубина**.

Создание групп

Прежде чем начать создавать группы, подумайте о причине создания, зачем они вам нужны и продумайте схему группировки. Например, вы можете сгруппировать виртуальные машины 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 **Пользовательские группы** в левой панели.
2. Нажмите кнопку ⊕ **Добавить группу** в верхней части левой панели.
3. Введите подходящее имя группы и нажмите **OK**. Появится новая группа в **Пользовательские группы**.

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 виртуальных машин

Вы можете перемещать объекты в любое расположение внутри иерархии **Пользовательские группы**. Для перемещения объекта, перетащите его из правой панели в желаемую группу левой панели.

Примечание

Объект, который перемещается, наследует параметры политик новой родительской группы, если наследование не было запрещено или другая политика не была непосредственно применена к нему. Для получения более подробной информации о наследовании политик, обратитесь к «Политики безопасности (Security Policies)» (p. 141).

Удаление групп

Группа не может быть удалена, если она содержит по меньшей мере одну виртуальную машину. Переместите все виртуальные машины из группы, которую вы хотите удалить, в другую группу. Если группа включает в себя подгруппы, вы можете выбрать для перемещения все подгруппы, а не отдельные виртуальные машины.

Чтобы удалить группу:

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

6.3.4. Сортировка, фильтрация и поиск виртуальных машин

В зависимости от количества виртуальных машин, правая панель может занимать несколько страниц (всего по умолчанию отображается 20 записей на каждой 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 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 виртуальную машину или выбрать для просмотра только управляемые виртуальные машины.

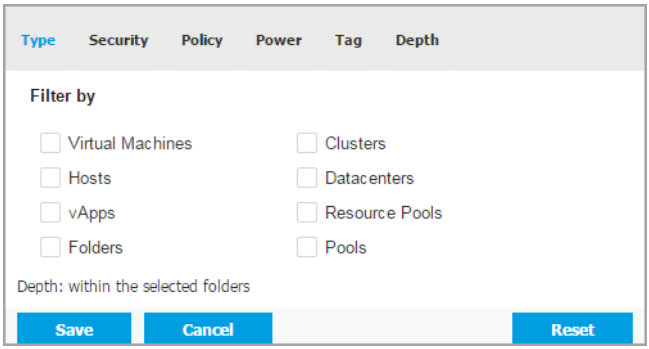
Сортировка виртуальных машин

Для сортировки данных по определенному столбцу, щелкните заголовок столбца. Например, если вы хотите отсортировать виртуальные машины по имени, щелкните на заголовок **Имя**. При повторном нажатии на заголовок виртуальные машины будут отображаться в обратной последовательности.

Сортировка компьютеров

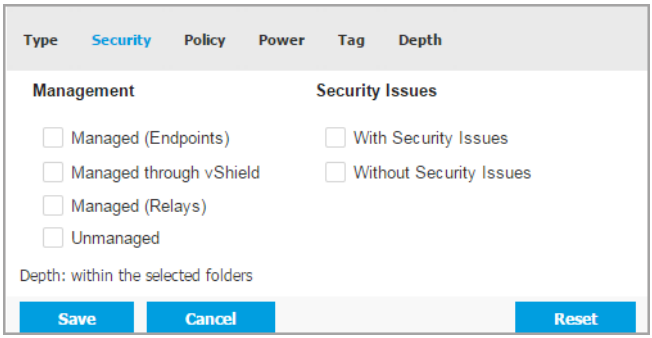
Фильтрация виртуальных машин

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 виртуальных объектов, которые будут отображаться.



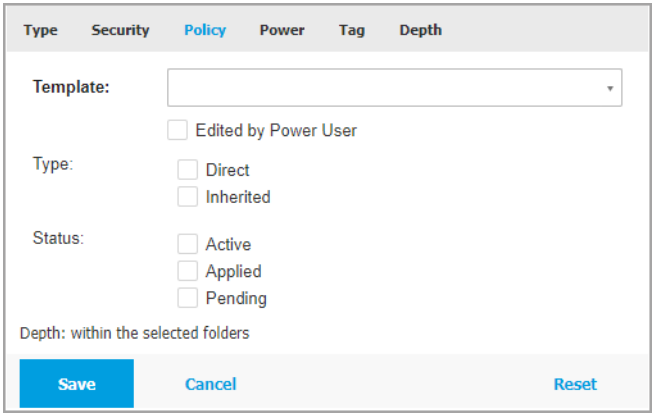
Виртуальные машины - Фильтрация по типу

   - **Безопасность**. Выберите управление защитой и/или статус безопасности, чтобы отфильтровать виртуальные машины.



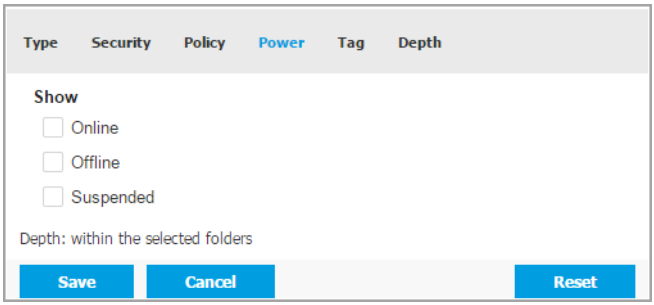
Виртуальные машины - Фильтрация по безопасности

- **Политика**. Выберите шаблон политики, для которого нужно фильтровать виртуальные машины, тип назначения политики (прямой или наследуемый), а также статус назначения политики (активный, применяемый или в ожидании).



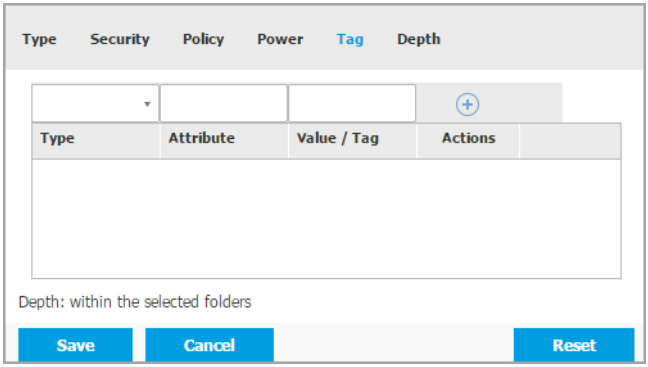
Виртуальные машины - Фильтрация по политикам

- **Питание**. Вы можете выбрать отображение виртуальных машин в режимах онлайн, офлайн и ожидания.



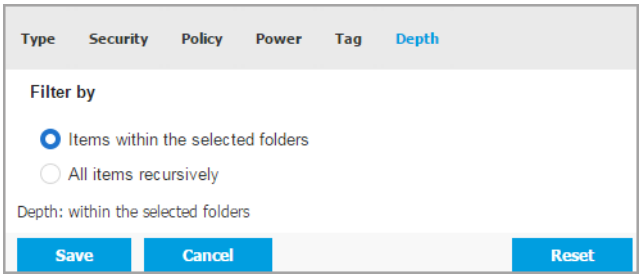
Виртуальные машины - Фильтрация по питанию

- **Метки**. Вы можете выбрать фильтрацию виртуальных машин с помощью тегов и атрибутов, которые вы определили в вашей среде виртуализации.



Виртуальные машины - Фильтрация по тэгам

- **Глубина**. При управлении деревом сетевой структуры виртуальных машин, виртуальные машины, размещенные в подгруппах, не отображаются по умолчанию. Выберите **Все предметы рекурсивно**, чтобы просмотреть все виртуальные машины, входящие в текущую группу и все подгруппы.



Виртуальные машины - Фильтрация по глубине

Примечание
Нажмите **Сбросить**, чтобы очистить фильтры и отобразить все виртуальные машины.

4. Нажмите **Сохранить**, чтобы отфильтровать виртуальные машины по выбранным критериям.

Поиск виртуальных машин

1. Выберите нужный контейнер в левой панели.
2. Введите слово для поиска в соответствующем поле под заголовками столбцов (Имя, ОС или IP) в правой панели. Например, введите IP-адрес виртуальной машины, которую вы ищете, в поле **IP**. Только соответствующая виртуальная машина появится в таблице.

   Очистите окно поиска, чтобы отобразить полный список виртуальных машин.

6.3.5. Запуск задач на виртуальных машинах

В разделе **Сеть**, вы можете удаленно запускать ряд администраторских задач на виртуальных машинах.

Вы можете выполнить следующие задачи:

- «СКАНИРОВАТЬ» (p. 103)
- «Задачи патчей» (p. 113)
- «Установить» (p. 116)
- «Удаление клиента» (p. 122)

- «Обновления» (p. 122)
- «Перенастройка клиента» (p. 123)
- «Сетевое Обнаружение» (p. 125)
- «Перезагрузка машины» (p. 126)

Вы можете создавать задачи отдельно для каждой виртуальной машины или для групп виртуальных машин. Например, вы можете удаленно установить Bitdefender Endpoint Security Tools на группу неуправляемых виртуальных машин. Позже, вы можете создать задачу сканирования определенной виртуальной машины в той же группе.

Для каждой виртуальной машины, вы можете запускать только совместимые задачи. Например, если вы выберите неуправляемую виртуальную машину, вы можете выбрать только установку агента безопасности, все другие задачи будут недоступы.

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

После создания, задача запустится сразу же, когда виртуальные машины будут онлайн. Если компьютер находится в автономном режиме, задание начнет выполняться, как только он подключится к Интернету.

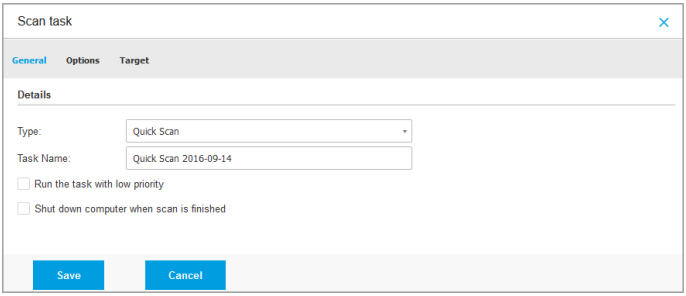
Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 129).

СКАНИРОВАТЬ

Для удаленного запуска задачи сканирования на одной или нескольких виртуальных машинах:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все объекты, содержащиеся в выбранной группе, выводятся в таблице правой панели.
4. Отметьте флажками соответствующие объекты, которые вы хотите просканировать.

5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Сканировать**. Появится окно настроек.
6. Настройте параметры сканирования:
   - На вкладке **Общее** вы можете выбрать тип сканирования и ввести имя для задачи проверки. Имя задачи сканирования предназначено, чтобы помочь вам легче определить текущее сканирование на странице **Задачи**.



Задача сканирования виртуальных машин - Настройка общих параметров

Выберите тип сканирования из меню **Тип**:

– **Быстрое сканирование** предварительно сконфигурировано для сканирования только важных системных местоположений и новых файлов. 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».

– **Сканирование памяти** проверяет программы, запущенные в памяти виртуальной машины.

– **Сканирование сети** тип пользовательского сканирования, позволяющий сканировать сетевые диски, используя агента безопасности Bitdefender, установленного на выбранной виртуальной машине.

  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)

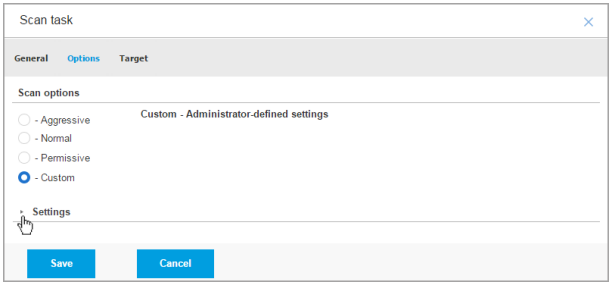
– **Выключить компьютер после завершения сканирования** Установите этот флажок, чтобы выключить машину, если вы не собираетесь использовать ее некоторое время.

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

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, выберите опцию **Пользователь** и затем раскройте раздел **Настройки**.



Задания по сканированию виртуальных машин - Настройка пользовательского режима сканирования

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. 318).

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 заданий по сканированию виртуальных машин - 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 код виртуальной машины 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. По своей природе кейлогеры не являются вредоносным ПО, но они могут быть использованы злоумышленниками. В украденных данных хакер может найти личную информацию, такую как номера банковских счетов и пароли, и использовать ее в личных целях.

– **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 компьютеру.

- **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.

    Если зараженный файл обнаружен, агент безопасности Bitdefender автоматически попытается его вылечить. 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 **Цель**, чтобы настроить расположения, которые вы хотите просканировать на требуемых виртуальных машинах.

  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 `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.

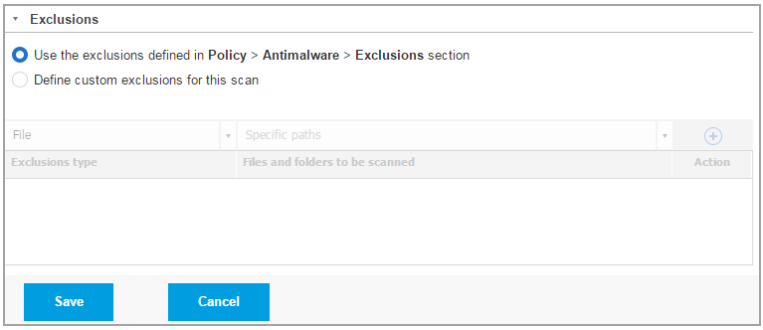
     - Если вы выбрали **Конкретные пути**, введите полный путь к объекту проверки. Желательно использовать системные переменные (в определенных случаях), чтобы убедиться, что путь действителен для всех выбранных виртуальных машин. Для получения более подробной информации о системных переменных, обратитесь к «Системные переменные» (p. 318).

  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.



Задание по сканированию виртуальных машин - Определение 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. 196).

7. 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» (p. 129).

Примечание
Чтобы запланировать задание сканирования, перейдите на страницу **Политики**, выберите политику, назначенную виртуальным машинам, и добавьте задачу проверки в раздел **Защита от вредоносных программ > По требованию**. Для получения более подробной информации, обратитесь к «Сканирование по запросу (On-Demand)» (p. 175).

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 сразу обновить программное обеспечение на определенных виртуальных машинах, 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

Виртуальные машины с устаревшим программным обеспечением уязвимы для атак. Рекомендуется регулярно проверять и устанавливать обновление ПО на конечных точках. Чтобы проверить виртуальные машины на наличие неустановленных исправлений:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
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 ???.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 129).

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. 240).

Установка патча

Чтобы установить одно или несколько исправлений на целевые виртуальные машины:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
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 исправления, отсутствующие на целевых виртуальных машинах.
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 виртуальной машины.

Вы можете просматривать и управлять задачами в разделе **Сеть > Задачи**. Для получения более подробной информации, обратитесь к «Просмотр и управление задачами» (p. 129).

Примечание

- Чтобы запланировать установку исправлений, измените политики, назначенные целевым машинам, и настройте параметры в разделе **Управление исправлениями**. Для получения более подробной информации, обратитесь к «Управление исправлениями» (p. 240).
- 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 ???.
- 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 машине. В этом случае вам необходимо войти в систему как администратор конечной точки и запустить деинсталлятор вручную.

Установить

Чтобы защитить ваши виртуальные машины с помощью Security for Virtualized Environments, необходимо установить агентов безопасности Bitdefender на каждой из них. Агент безопасности Bitdefender управляет защитой на виртуальных машинах. Он также общается с Control Center, чтобы принимать

команды администратора и отправлять результаты своих действий. После того, как вы подключите агента безопасности Bitdefender к сети, он будет автоматически обнаруживать незащищенные виртуальные машины в этой сети. Затем защита Security for Virtualized Environments может быть установлена на этих виртуальных машинах удаленно из Control Center. Удаленная установка выполняется в фоновом режиме, без ведома пользователя.

В изолированных сетях, которые не имеют прямой связи с устройствами GravityZone, вы можете установить агента безопасности с ролью Роь ретранслятора В этом случае, связь между устройством GravityZone и другими агентами безопасности будет осуществляться через агента ретрансляции, который также будет выступать в качестве локального сервера обновлений для агентов безопасности, защищающих изолированную сеть.

Примечание
Рекомендуется, чтобы виртуальная машина, на которой вы установите агента ретрансляции, была всегда включена.

Предупреждение
Перед установкой убедитесь, что удалили существующее программное обеспечение для защиты от вредоносного ПО и брандмауэр на виртуальной машине. 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.

Для удаленной установки защиты Security for Virtualized Environments на одной или нескольких виртуальных машинах:

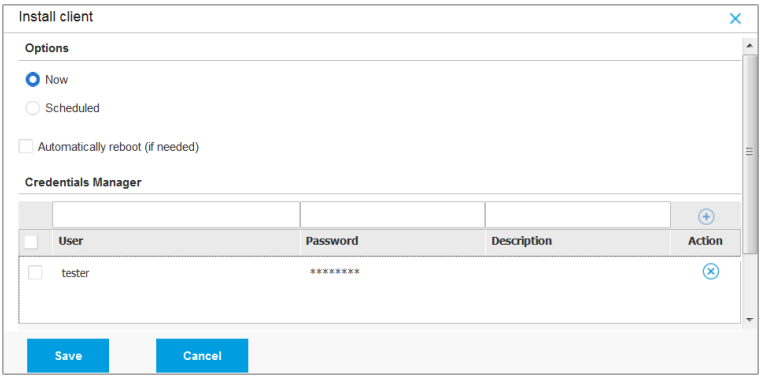
1. Подключитесь и войдите в Control Center.
2. Перейдите в раздел **Сеть**.
3. Выберите **Виртуальные машины** из меню видов сетей.
4. Выберите желаемый контейнер в левой панели. Объекты, содержащиеся в выбранной группе, будут отображены в таблице правой панели.

   Примечание
   При желании, вы можете применять фильтры для отображения только неуправляемых виртуальных машин. Нажмите меню **Фильтры** и выберите

следующие параметры: **Неуправляемые** на вкладке **Безопасность** и **Все предметы рекурсивно** на вкладке **Глубина**.

5. Выберите объекты (виртуальные машины, хосты, кластеры или группы), на которых вы хотите установить защиту.
6. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Установить > BEST**.

   Отобразится мастер установки **Install Client**.



Установка Bitdefender Endpoint Security Tools из меню задач

7. 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.

8. Если вы хотите, чтобы заданные конечные точки перезапустились после завершения установки, выберите **Автоматическая перезагрузка (при необходимости)** .
9. 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.

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

Чтобы добавить необходимые учетные данные ОС:

a. Введите имя пользователя и пароль учетной записи администратора для каждой выбранной операционной системы в соответствующих полях заголовков таблицы. При желании, вы можете добавить описание, которое поможет вам проще определить каждый аккаунт.

   Если виртуальные машины 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.

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.

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

10. В разделе **Установщик**, выберите объект, к которому выбранные машины будут подключаться для установки и обновления клиента:

- **GravityZone Appliance**, когда машины подключаются непосредственно к устройству GravityZone.

  В этом случае вы можете также определить пользовательский коммуникационный сервер, введя, в случае необходимости, его IP-адрес или имя хоста.

- **Endpoint Security Relay**, если вы хотите подключить машины к клиенту-ретранслятору, установленному в вашей сети. Все машины с ролью ретранслятора, обнаруженные в вашей сети, будут отображены в таблице ниже. Выберите компьютер с ролью ретранслятора, который Вам нужен. 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.

– 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.

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 для вашей компании.
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.

    Предупреждение
    Пожалуйста, обратите внимание, что модуль брандмауэр доступен только для поддерживаемых рабочих станций Windows.

    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.

Удаление клиента

Для удаленного удаления защиты Bitdefender:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все объекты из выбранного контейнера отображаются в таблице правой панели.
4. Отметьте флажками виртуальные машины, на которых вы хотите удалить агента безопасности Bitdefender.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Удалить клиента**.
6. Появится окно конфигурации, которое позволит вам сделать следующие настройки:
   - Вы можете выбрать хранение объектов карантина на клиентской машине.
   - Для интегрированной среды vShield, вы должны выбрать необходимые учетные данные для каждой машины, в противном случае удаление не произойдет. Выберите **Используйте учетные данные для интеграции vShield**, затем ниже проверьте все соответствующие учетные данные в таблице диспетчера учетных данных.
7. 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» (p. 129).

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

Обновления

Периодически проверяйте статус управляемых виртуальных машин. Если вы заметили виртуальную машину с проблемами безопасности, нажмите на ее имя, чтобы отобразить окно **Информация**. Для получения более подробной информации, обратитесь к «Статус безопасности» (p. 87).

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

Для удаленного обновления клиента и механизмов защиты на управляемых виртуальных машинах:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все объекты из выбранного контейнера отображаются в таблице правой панели.
4. Отметьте флажками виртуальные машины, где вы хотите запустить обновление клиента.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обновить**. Появится окно настроек.
6. Вы можете обновить только продукт, только механизмы защиты или всё сразу.
7. Для ОС Linux и машин, интегрированных с vShield, также является обязательным выбрать необходимые учетные данные. Проверьте опцию **Используйте учетные данные для интеграции Linux и vShieldn**, затем выберите соответствующие учетные данные из таблицы диспетчера учетных данных, которые отображаются ниже.
8. 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» (p. 129).

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.

Чтобы изменить параметры установки для одной или нескольких виртуальных машин:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все объекты из выбранного контейнера отображаются в таблице правой панели.
4. Отметьте флажками виртуальные машины, для которых вы хотите изменить параметры установки.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Перенастроить клиента**.
6. В разделе **Общие**, настройте время выполнения задачи:
   - **Сейчас**, чтобы немедленно начать задачу.
   - **Запланировано**, чтобы настроить интервал повторяемости задачи. В этом случае, выберите желаемый интервал времени (ежечасно, ежедневно или еженедельно) и настройте его в соответствии с вашими потребностями.

     Примечание
     Например, когда другие важные процессы также должны работать на выбранной машине, вы можете запланировать запуск задачи через каждые 2 часа. Задача будет запускаться на каждой выбранной машине через каждые 2 часа, пока не будет завершена.

7. Настройте необходимые модули, роли и режимы сканирования для выбранной конечной точки. Для получения более подробной информации, обратитесь к руководству по установке GravityZone.

   Предупреждение
   - Будут установлены только поддерживаемые модули для каждой операционной системы.

Пожалуйста, обратите внимание, что модуль брандмауэр доступен только для поддерживаемых рабочих станций Windows.

- Bitdefender Tools (стандартный клиент) поддерживает только централизованное сканирование.

8. 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» (p. 129).

Сетевое Обнаружение

Сетевое обнаружение происходит автоматически только агентами безопасности с Роль ретранслятора. Если у вас в сети нет агента ретрансляции, вам придется вручную запускать задачу сетевого обнаружения из защищенной конечной точки.

Чтобы запустить задачу сетевого обнаружения в вашей сети:

Важно
Если вы используете ретранслятор Linux для обнаружения других конечных точек Linux или Mac, вы должны либо установить Samba на целевые конечные точки, либо присоединиться к ним в Active Directory и использовать DHCP. Таким образом, NetBIOS будет автоматически настроен на них.

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все объекты из выбранного контейнера отображаются в таблице правой панели.
4. Отметьте флажком машину, на которой вы хотите выполнить задачу сетевого обнаружения.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Обнаружение сети**.
6. 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» (p. 129).

Перезагрузка машины

Вы можете удаленно перезагрузить управляемые виртуальные машины.

Примечание
Проверьте страницу **Сеть > Задачи** перед перезапуском определенных виртуальных машин. Ранее созданные задачи еще могут быть в процессе выполнения на выбранных виртуальных машинах.

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все объекты из выбранного контейнера отображаются в таблице правой панели.
4. Установите флажки на виртуальных машинах, которые вы хотите перезагрузить.
5. Нажмите кнопку **Задачи** в верхней части таблицы и выберите **Перезагрузить машину**.
6. Выберите опции перезагрузки по расписанию:
   - Выберите **Перезапустить сейчас**, чтобы немедленно перезагрузить виртуальные машины.
   - Выберите **Включить перезагрузку** и используйте поля ниже, чтобы запланировать перезагрузку в определенную дату и время.
7. 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.

6.3.6. Формирование быстрых отчетов

Вы можете выбрать создание быстрых отчетов на управляемых виртуальных машинах, используя страницу **Сеть**:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все виртуальные машины, из выбранного контейнера, отобразятся в таблице правой панели.

4. Фильтр содержимого выбранной группы доступен только для управляемых виртуальных машин.
5. Установите флажки на соответствующих виртуальных машинах, которые будут включены в отчет.
6. Нажмите кнопку **Отчет** в верхней части таблицы и выберите из меню тип отчета. Для получения более подробной информации, обратитесь к «Типы отчетов» (p. 261).
7. Настройте параметры отчета. Для получения более подробной информации, обратитесь к«Создание отчетов» (p. 264)
8. Нажмите **Создать**. Отчет отобразится немедленно. Время, необходимое для создания отчетов, может изменяться в зависимости от количества выбранных виртуальных машин.

6.3.7. Назначение политик

Вы можете управлять настройками безопасности на виртуальных машинах с помощью политик.

В разделе **Сеть** вы можете просматривать, изменять и назначать политики для каждой виртуальной машины или группы виртуальных машин.

Примечание
Настройки безопасности доступны только для управляемых виртуальных машин. Для облегчения просмотра и управления настройками безопасности, вы можете отфильтровать сетевое содержимое только для управляемых виртуальных машин.

Для просмотра параметров безопасности, назначенных виртуальной машине:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все виртуальные машины, из выбранного контейнера, отобразятся в таблице правой панели.
4. Нажмите на имя виртуальной машины, которая вас интересует. Появится информационное окно.
5. На вкладке **Общее**, в разделе **Политика**, нажмите на название текущей политики, чтобы просмотреть ее настройки.

6. 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, влияет на все виртуальные машины, которым назначена данная политика.

   Для получения более подробной информации о настройках политик виртуальных машин, обратитесь к«Политики безопасности (Security Policies)» (p. 141)

Чтобы назначить политику виртуальной машине или группе виртуальных машин:

1. Перейдите в раздел **Сеть**.
2. Выберите **Виртуальные машины** из меню видов сетей.
3. Выберите желаемый контейнер в левой панели. Все виртуальные машины, из выбранного контейнера, отобразятся в таблице правой панели.
4. Отметьте флажок на желаемом объекте. Вы можете выбрать один или несколько объектов одного типа, только одного уровня.
5. Нажмите кнопку **Назначить политику** в верхней части таблицы.
6. Сделайте необходимые настройки в окне **Назначение политики**.

   Для получения более подробной информации, обратитесь к «Назначение политик» (p. 143).

6.3.8. 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 виртуальных машинах 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. 251).

6.4. 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**:

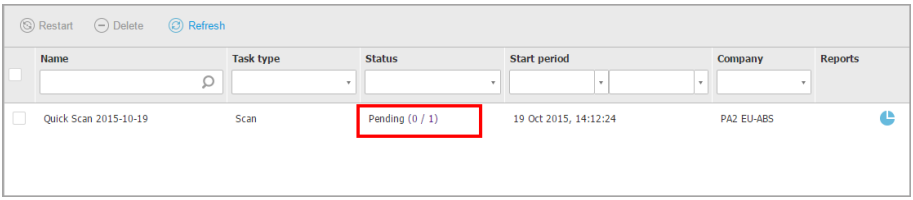
- Проверить статус задачи
- Просмотреть отчеты задач

- Перезапустить задачи
- Удалить задачи

6.4.1. 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:
  - **В стадии ожидания**, когда ни одна из подзадач еще не началась или когда лимит количества одновременных развертываний превышен. Максимальное количество одновременных развертываний можно установить в меню **Настройки**. Для получения более подробной информации, обратитесь к руководству по установке GravityZone.
  - **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.

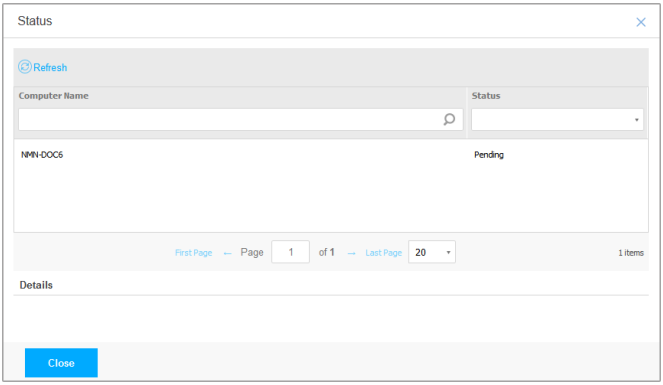
  – **Завершена**, если подзадача успешно завершена.

  – **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.

  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.

6.4.2. Просмотр отчетов задач

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

1. Перейдите на страницу **Сеть > Задачи**.
2. Выберите нужный сетевой объект из меню видов сетей.
3. Установите флажок на интересующей вас задаче сканирования.
4. Нажмите соответствующую кнопку в колонке **Отчеты**. Дождитесь отображения отчета. Для получения более подробной информации, обратитесь к «Использование отчетов» (p. 261).

6.4.3. 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. Выберите нужный сетевой объект из меню видов сетей.
3. Установите флажки на требуемых незавершенных задачах.
4. 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.

6.4.4. 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. Выберите нужный сетевой объект из меню видов сетей.
3. Установите флажок на соответствующей задаче, которую вы хотите удалить.
4. 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.

6.5. 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 папке **Пользовательские группы** :
  - 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, сервер vCenter, сервер Xen 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. Выберите требуемый вид сети из меню видов сетей.
3. 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 **Custom Groups**, которые были обнаружены за пределами любой интегрированной сетевой инфраструктуры.

4. Установите в правой панели флажок напротив конечной точки, которую хотите удалить.
5. 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 папки **Удаленные** в **Пользовательские группы** , используя перетаскивание.

6.6. 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

6.6.1. 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:

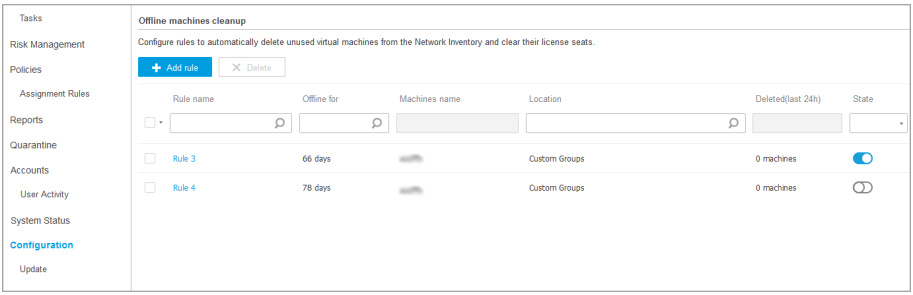
  - **Применяется к клонированным физическим конечным точкам, объединенным в Active Directory**. Эта опция разрешает проблемы с клонированными жесткими дисками из машин эксплуатации.
  - **Применяется к клонированным виртупльным конечным точкам, объединенным в Active Directory**. Этот параметр разрешает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

6.6.2. 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**.

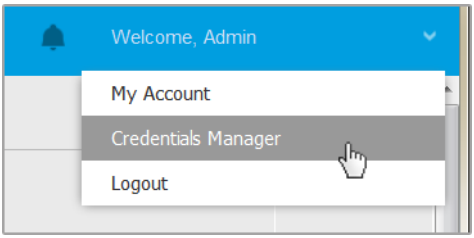
Чтобы удалить одно или несколько правил:

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

6.7. Диспетчер учетных данных (Credentials Manager)

Диспетчер учетных данных поможет вам определить учетные данные, необходимые для доступа к имеющимся ресурсам vCenter Server, а также для удаленной аутентификации в различных операционных системах 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

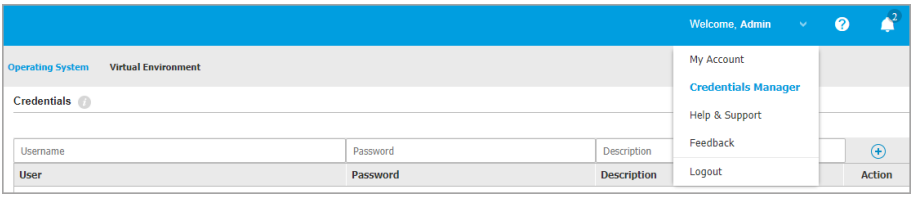
Окно **Диспетчер учетных данных** содержит две вкладки:

- Операционная система
- Виртуальная среда

6.7.1. Операционная система

На вкладке **Operating System**, вы можете управлять учетными данными администратора, необходимыми для удаленной аутентификации во время установки, отправки задач для компьютеров и виртуальных машин 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.

6.7.2. Виртуальная среда

На вкладке Virtual Environment вы можете управлять учетными данными для доступных виртуальных серверных систем.

Для доступа к виртуальной инфраструктуре, интегрированной с Control Center, вы должны указать свои учетные данные для каждой доступной серверной системы. Control Center использует ваши учетные данные для подключения к виртуальной инфраструктуре, отображая только те ресурсы, к которым у вас есть доступ (задается на виртуальном сервере).

Чтобы задать учетные данные, необходимые для подключения к виртуальному серверу:

1. Выберите сервер из соответствующего меню.

   Примечание
   Если меню недоступно, значит интеграция еще не была выполнена или все необходимые учетные данные уже настроены.

2. Введите имя пользователя, пароль и подходящее описание.
3. Нажмите кнопку ⊕ **Добавить**. Новый набор учетных данных будет добавлен в таблицу.

   Примечание
   Если вы не настроили учетные данные в диспетчере учетных данных, вам будет необходимо ввести их, когда вы будете пытаться просмотреть ресурсы любой виртуализованной серверной системы. Единожды введя ваши учетные данные, они будут сохранены в вашем менеджере учетных данных и вам не придется вводить их повторно в дельнейшем.

   Важно
   Всякий раз, когда вы изменяете свой пароль пользователя виртуального сервера, не забудьте также обновить его в диспетчере учетных данных.

6.7.3. 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)

После установки, защита Bitdefender может быть настроена и управляться из Control Center с помощью политик безопасности. Политика определяет параметры безопасности, которые должны применяться к выбранным объектам сетевого содержимого (компьютеры и виртуальные машины).

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.

Вы можете создать столько политик, сколько вам нужно, на основе требований безопасности для каждого типа управляемого объекта сети.

Вот то, что вам нужно знать о политиках:

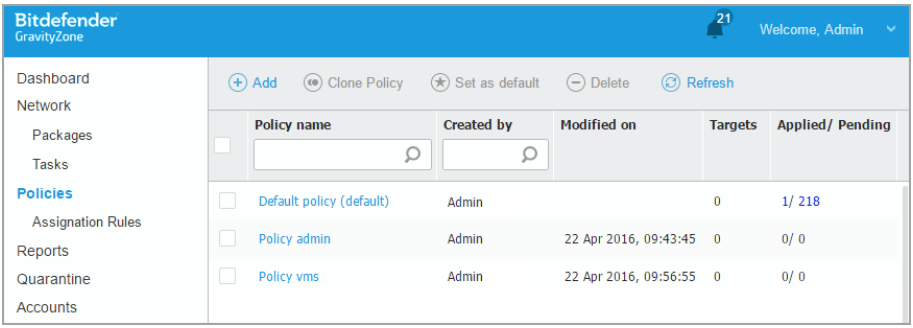
- Политики создаются на странице **Политики** и назначаются сетевым объектам в разделе **Сеть**.
- Политики могут наследовать некоторые настройки модулей из других политик.
- Вы можете настроить назначение политик для конечных точек таким образом, что политика сможет применяться только при определенных условиях - на основании местоположения или зашедшего пользователя. 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. 154).
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:

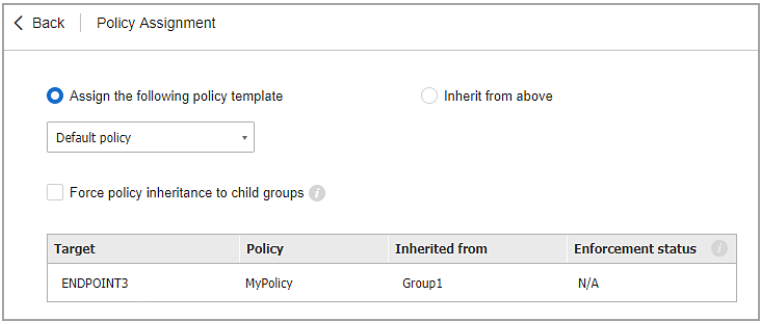
- Назначить политику непосредственно на цель.
- Назначить политику родительской группы через наследование.
- Принудительное наследование политики.

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:

1. Перейдите на страницу **Политики**.
2. Найдите политику, которую вы назначили.

   В столбце **Активна/Применена/Ожидает** вы можете просмотреть количество конечных точек для каждого из трех статусов.
3. Нажмите на любую цифру, чтобы просмотреть список конечных точек с соответствующим статусом на странице **Сеть**.

Назначение политик на основе правил

Страница **Политики > правила назначения** позволяет вам задать политику по пользователю и местоположению. Например, вы можете применять более строгие правила файрволла, когда пользователи подключаются к сети Интернет из-за пределов компании или вы можете включить Управление веб-доступом для пользователей, которые не входят в группу администраторов.

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
   - Правило тегов
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`

Тип	Значение
Конечная точка может разрешать имена хостов	Имя хоста. Например: `fileserv.company.biz`
Конечная точка может подключиться к GravityZone	Да/Нет
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.

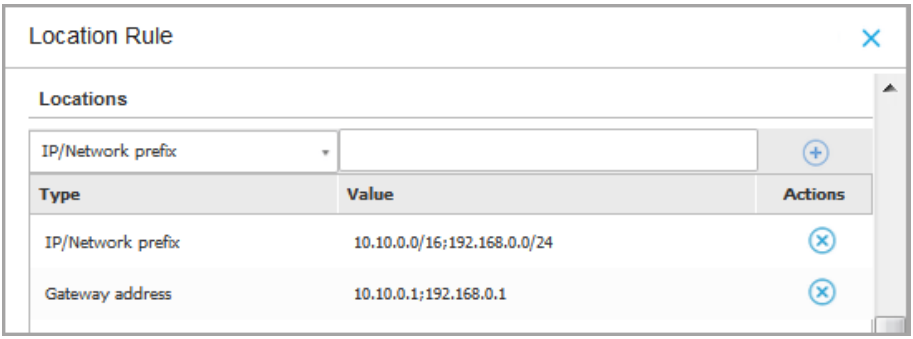
Имя хоста	Имя хоста
	For example: `cmp.bitdefender.com`
	Важно
	Вы также можете использовать подстановочные символы. Звездочка (*) заменяет ноль или более символов, а знак вопроса (?) заменяет ровно один символ. Примеры:
	`*.bitdefender.com`
	`cmp.bitdefend??.com`

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. 148).

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.

Настройка правил тегов

Важно
Вы можете создавать правила тегов, только если доступна интеграция с Amazon EC2 или Microsoft Azure.

Вы можете использовать теги, определенные в облачных инфраструктурах, чтобы назначить конкретную политику GravityZone для ваших виртуальных машин, размещенных в облаке. Все виртуальные машины, имеющие теги, указанные в правиле тега, будут применяться с политикой, установленной правилом.

Примечание
В соответствии с облачной инфраструктурой вы можете определить теги виртуальной машины следующим образом:

- Для Amazon EC2: на вкладке **Теги** экземпляра EC2.
- Для Microsoft Azure: в разделе **Обзор** виртуальной машины.

Правило тега может содержать один или несколько тегов. Чтобы создать правило тега:

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 тега.
4. В таблицу **Тег** добавьте один или несколько тегов.

   Тег состоит из чувствительной к регистру пары ключ-значение. Убедитесь, что вводите теги, которые определены в вашей облачной инфраструктуре. Будут задействованы только действительные пары ключ-значение.

Чтобы добавить тег:

a. В поле **Ключ тега** введите имя ключа.

b. В поле **Значение тега** введите имя значения.

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

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. 154).
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. Выберите **компьютеры и виртуальные машины** из меню видов сетей.

3. Нажмите на имя политики. Откроется страница настройки политики.
4. Настройте необходимые параметры политики. Настройки расположены в следующих разделах:
   - Основные
   - Защита от вредоносного ПО
   - Sandbox Analyzer
   - Защита сети
   - Ретранслятор

   Для перемещения по разделам используйте меню в левой части страницы.
5. 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. 142).

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.

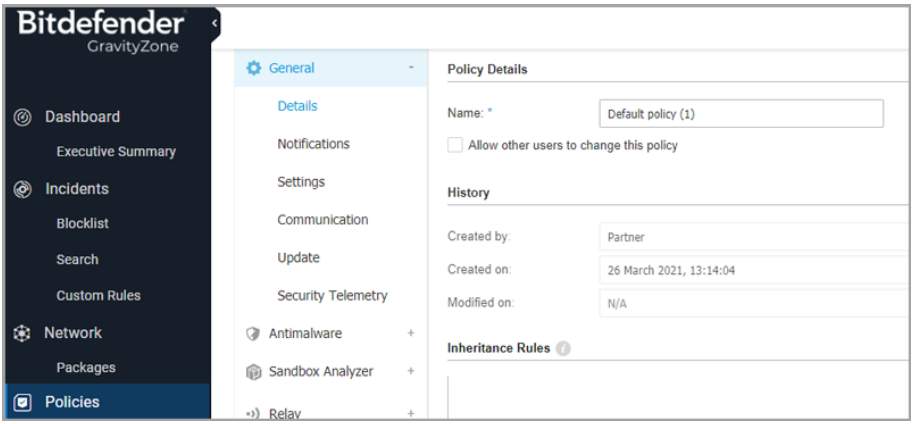
Настройки объединены в следующие разделы:

- Подробная информация
- Настройки
- Коммуникации
- Обновления

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

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, унаследственные точки и настройки разделов вернутся к дочерним настройкам.

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**.

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.

- **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.

  – **Отправьте подозрительные исполняемые файлы для анализа.** Выберите этот параметр, чтобы отправить файлы, которые кажутся ненадежными или имеют подозрительное поведение, в Bitdefender Labs для анализа.

Примечание
Для получения информации о том, как эти настройки нарушают правила HIPAA, обратитесь к разделу "GravityZone и HIPAA" в Руководстве по установке.

Коммуникации

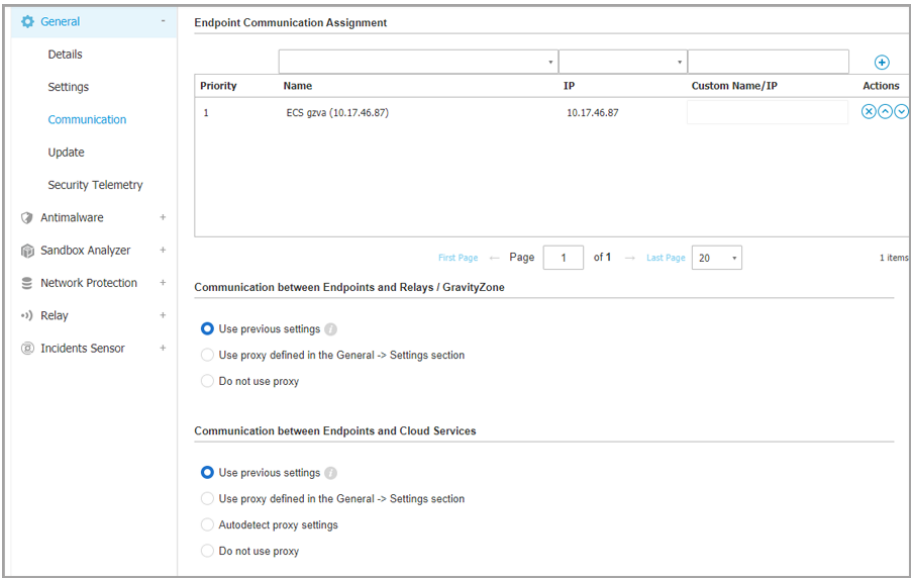
В этом разделе вы можете назначить одну или несколько машин-ретрансляторов для требуемых конечных точек, а затем настроить прокси-сервер для связи между этими конечными точками и GravityZone.

Назначение коммуникационных параметров конечной точке

Когда несколько коммуникационных серверов устанавливается на устройство GravityZone, вы можете назначить выбранным компьютерам один или несколько коммуникационных серверов с помощью политики. Доступные конечные точки-ретрансляторы, которые выступают в качестве коммуникационных серверов, также будут учтены.

Чтобы назначить коммуникационные серверы выбранным компьютерам:

1. В окне **Назначение связи конечной точки**, нажмите на поле **Имя**. Появится список обнаруженных коммуникационных серверов.
2. Выберите объект.



Политики - Настройки связи

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

   Коммуникационный сервер добавится к списку. Все выбранные компьютеры будут общаться с Control Center через указанный коммуникационный сервер.
4. Выполните те же действия, чтобы добавить несколько коммуникационных серверов, при их наличии.
5. Вы можете настроить приоритет использования коммуникационных серверов, с помощью стрелок вверх и вниз, доступных 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 прокси-сервер для связи между желаемыми конечными точками и назначенными машинами-ретрансляторами или между требуемыми конечными точками и устройством GravityZone (если ретранслятор не был 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

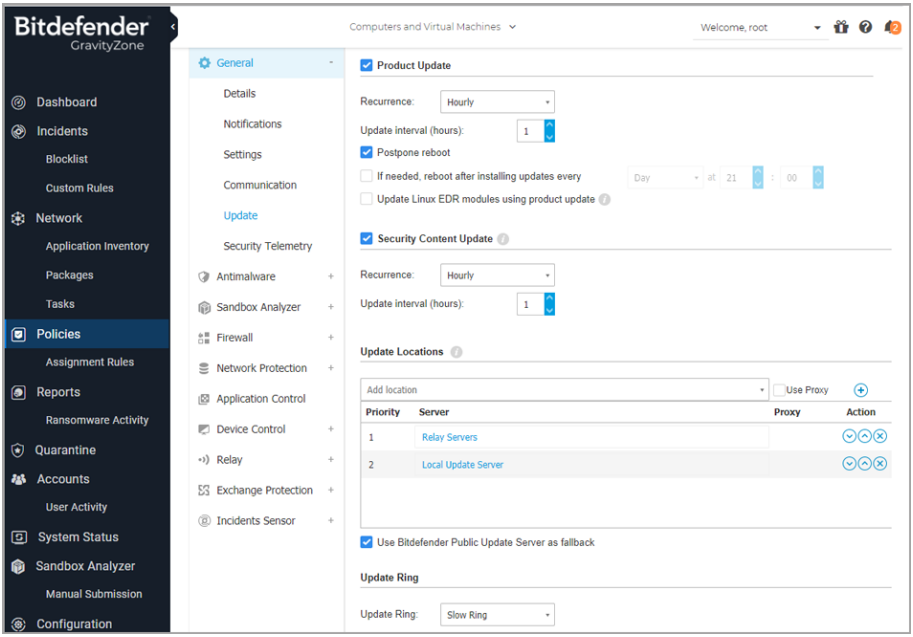
В этом разделе вы можете настроить прокси-сервер для связи между нужными конечными точками и Bitdefender Cloud Services (требуется подключение к Интернету):

- **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).

- **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**. По умолчанию, агенты безопасности Bitdefender обновляются с локального сервера обновлений GravityZone. 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

     - **Локальный сервер обновлений**
   - 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.

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.
- 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.

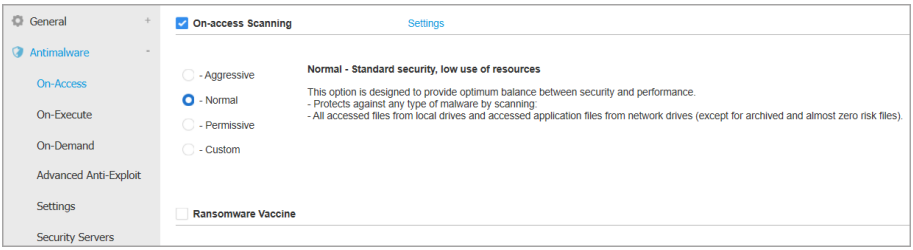
Настройки объединены в следующие разделы:

- Сканирование при доступе (On-Access)
- При выполнении
- Сканирование по запросу (On-Demand)
- Advanced Anti-Exploit
- Настройки

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. 318).

  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 модуль Advanced Threat Control

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.

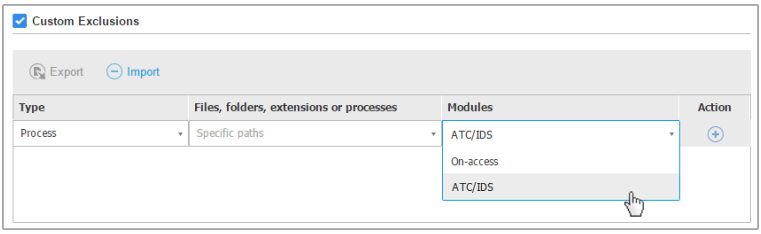
Для настройки Advanced Threat Control:

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

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. 287).

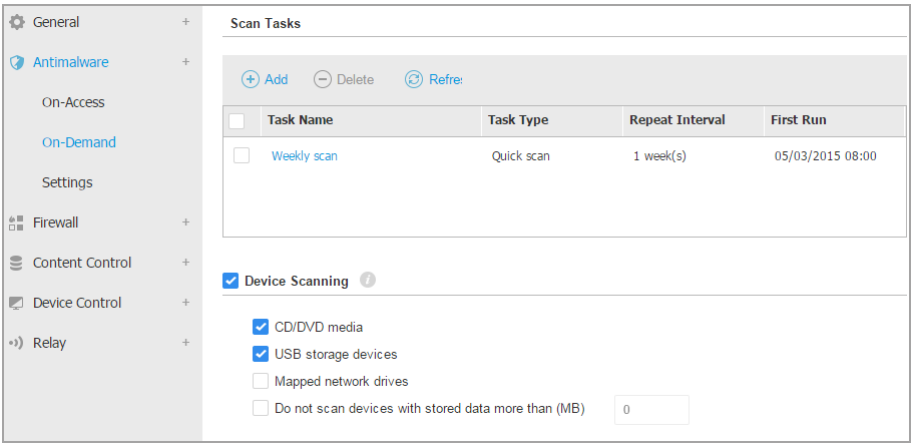
- Проверьте **Security Audit** отчет.
- Проверьте страницу **Деятельность вымогателей**.

  Далее, на этой странице Вы можете запустить задачи восстановления, если это необходимо. Для получения более подробной информации, обратитесь к ???.

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. 196).

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 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».

  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.

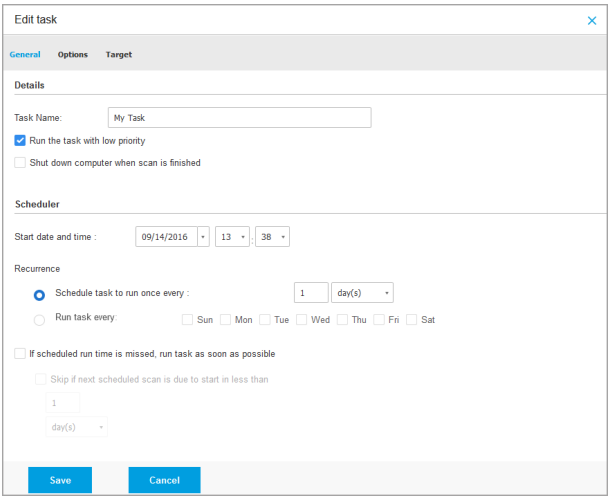
Чтобы удалить задачу из списка, выберите задачу и нажмите кнопку ⊖ **Удалить** в правой части таблицы.

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).

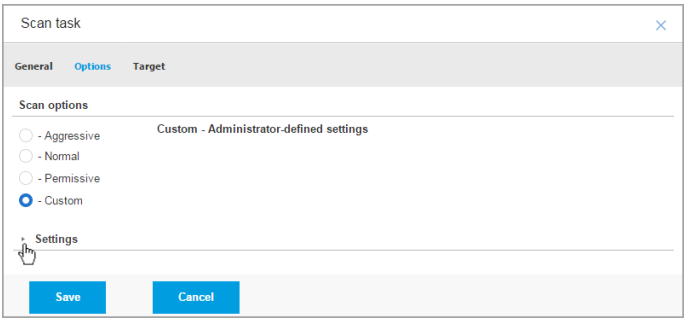
  При желании вы можете указать, что происходит, когда задача проверки не может быть запущена в запланированное время (конечная точка была отключена или отключена). Используйте параметр **Если запланированное время выполнения пропущено, запустите задачу как можно скорее** в соответствии с вашими потребностями:

  – 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**.



Задачи сканирования компьютеров - 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. 318).

  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. 196).

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.

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. 188).

- **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. 189).

- **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. 189).

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

Метод	Описание
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
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

Метод	Описание
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
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

Метод	Описание
	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.

Централизованный карантин

Если файлы, помещенные на карантин из конечных точек, необходимо сохранить для дальнейшего анализа, используйте параметр **Централизованный карантин**, который отправляет архивированную копию каждого локального файла, помещенного на карантин, в общий сетевой ресурс.

После включения этого параметра каждый файл, помещенный на карантин из управляемых конечных точек, копируется и упаковывается в защищенный паролем ZIP-архив на указанное расположение в сети. Именем архива является хэш файла, помещенного в карантин.

Важно
Максимальный размер архива составляет 100 МБ. Если архив превышает 100 МБ, он не будет сохранен в общей сетевой папке.

Чтобы настроить параметры централизованного карантина, заполните следующие поля:

- **Пароль архива**: введите пароль для архива файлов, помещенных в карантин. Пароль должен содержать, по крайней мере, один символ верхнего регистра, по крайней мере, одну строчную букву и, по крайней

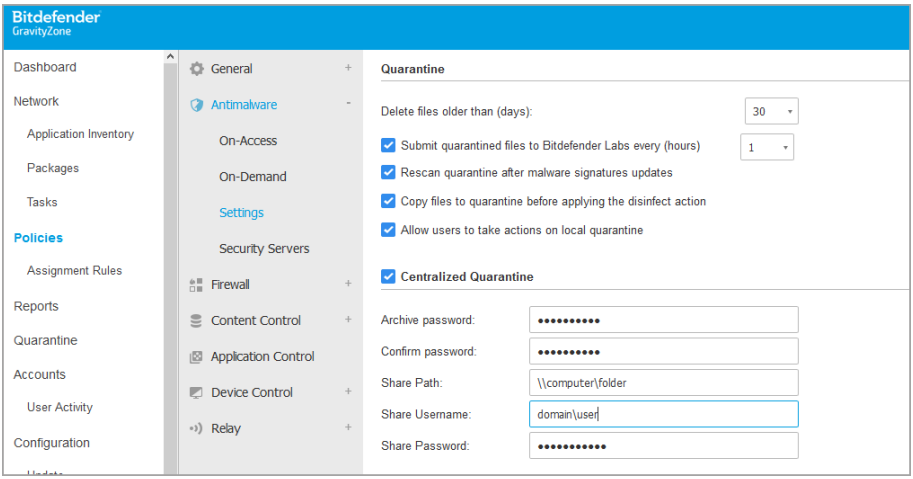
мере, одну цифру или специальный символ. Подтвердите пароль в следующем поле.

- **Общий путь**: введите сетевой путь, в котором будут храниться архивы (например, `\\computer\folder`).
- Имя пользователя и пароль, необходимые для подключения к сетевой папке. Поддерживаемые форматы для имени пользователя:
  - `username@domain`
  - `domain\username`
  - `Имя пользователя.`

Для корректной работы централизованного карантина убедитесь, что выполнены следующие условия:

- Общее расположение доступно в сети.
- Конечные точки имеют подключение к сетевому ресурсу.
- Учетные данные для выполнения входа являются действительными и предоставляют доступ к записи на сетевом ресурсе.
- На сетевом ресурсе достаточно места на диске.

Примечание
Централизованный карантин не применяется к карантину почтовых серверов.



Централизованный карантин

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.

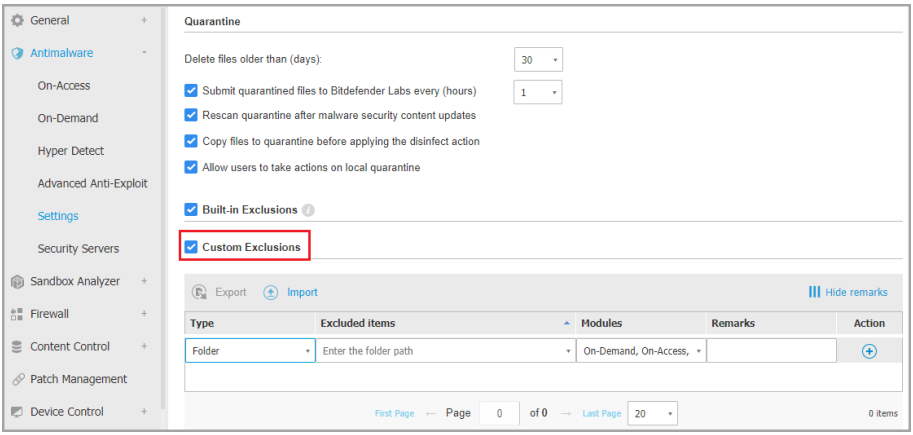
  Пользовательские исключения сканирования применяются к одному или нескольким следующим методам:

- 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 - Пользовательские исключения

Чтобы добавить пользовательское правило исключений:

1. Выберите тип исключения из меню:

- **Папка**: только указанная папка, без всех файлов и процессов внутри нее или из всех ее вложенных папок
- **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.

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 следующее:

- Подача через датчик конечной точки
- Подача через датчик сети
- Подача через датчик ICAP
- Настройки Sandbox Manager

В настройках политики вы также можете настроить автоматическую отправку из централизованного карантина. Дополнительные сведения см. в разделе «Централизованный карантин» (p. 194).

Подробнее о ручной подаче см. «Manual Submission» (p. 278). Подробнее о передаче через API см. В главах **Sandbox** и **Sandbox Portal** в GravityZone API Guide (On-Premises) .

Примечание
Для получения информации о том, как Sandbox Analyzer нарушает правила HIPAA, обратитесь к разделу "GravityZone и HIPAA" в Руководстве по установке.

Сетевой датчик

В этом разделе вы можете настроить автоматическую отправку образцов сетевого трафика в Sandbox Analyzer через датчик сети. Этот модуль требует развертывания и настройки виртуального устройства сетевой безопасности с помощью Sandbox Analyzer On-Premises

Для настройки автоматической отправки через датчик сети:

1. Установите флажок **Automatic samples submission from network sensor** , чтобы включить автоматическую отправку подозрительных файлов в Sandbox Analyzer.
2. В разделе **Предварительная фильтрация контента** настройте уровень защиты от потенциальных угроз. В датчик сети встроен механизм фильтрации содержимого, который определяет необходимость детонирования 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. 320).

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 сети автоматически отправляет Sandbox Analyzer только объекты, которые с наибольшей вероятностью могут быть вредоносными и игнорирует остальные объекты.
- **Обычный**. Датчик сети находит баланс между отправленными и проигнорированными объектами и отправляет в Sandbox Analyzer те, которые могу быть вредоносными в большей или в меньшей степени.
- **Агрессивный**. Датчик сети 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.

3. В разделе **Настройки подключения** выберите предпочтительный экземпляр Sandbox Analyzer для отправки сетевого содержимого.

   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.

4. 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**.

Датчик ICAP

В этом разделе вы можете настроить автоматическую отправку в Sandbox Analyzer через датчик ICAP.

Примечание
Для Sandbox Analyzer требуется Security Server, настроенный для сканирования устройств сетевого хранилища (NAS), использующих протокол ICAP. Подробности см. в???

1. Установите флажок **Automatic samples submissions from ICAP sensor**, чтобы включить автоматическую отправку подозрительных файлов в Sandbox Analyzer.
2. В разделе **Предварительная фильтрация контента** настройте уровень защиты от потенциальных угроз. В датчик сети встроен механизм фильтрации содержимого, который определяет необходимость детонирования 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. 320).

   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 ICAP автоматически отправляет Sandbox Analyzer только объекты, которые с наибольшей вероятностью могут быть злонамеренными и игнорирует остальные объекты.
   - **Обычный**. Датчик ICAP находит баланс между отправленными и проигнорированными объектами и отправляет в Sandbox Analyzer оба объекта, которые с большей и с меньшей вероятностью могут быть вредоносным.

- **Агрессивный**. Датчик ICAP 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.

3. В разделе **Настройки подключения** выберите предпочтительный экземпляр Sandbox Analyzer для отправки сетевого содержимого.

   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.

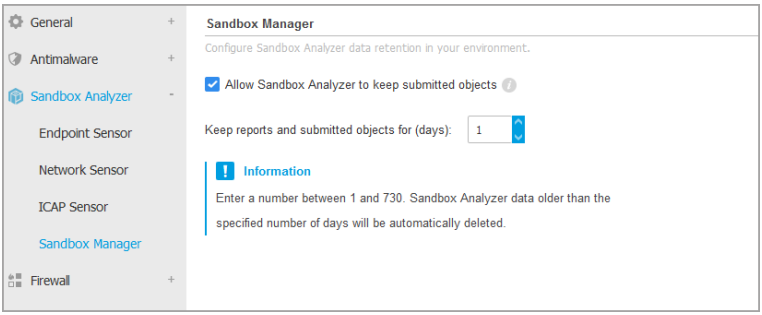
4. В разделе **Профиль детонации** настройте уровень сложности поведенческого анализа, влияя на пропускную способность Sandbox Analyzer. Например, если установлено значение **Высокое**, Sandbox Analyzer будет выполнять более точный анализ на меньшем количестве образцов за тот же интервал, чем на **Среднее** или **Низкое**.

Sandbox Manager

В этом разделе вы настраиваете хранение данных для ваших экземпляров Sandbox Analyzer:

- Установите флажок **Разрешить Sandbox Analyzer, чтобы сохранить отправленные объекты** . Этот параметр позволяет использовать параметр **Повторно отправить на анализ** в области карточек отправки интерфейса отчетности Sandbox Analyzer.
- Укажите, какое количество дней вы хотите, чтобы Sandbox Analyzer сохранял отчеты и отправленные объекты в хранилище данных.

Максимальное количество данных, которое вы можете ввести, составляет 730. По истечении заданного периода все данные будут удалены.



Политики > Sandbox Analyzer > Sandbox Manager

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. 210).

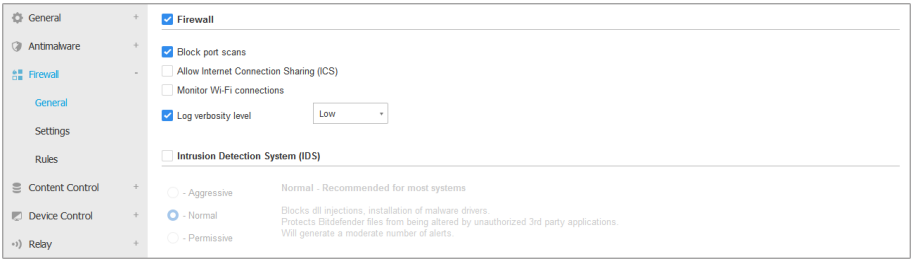
Важно
Модуль файрвола доступен только для поддерживаемых рабочих станций Windows.

Настройки объединены в следующие разделы:

- Основные
- Настройки
- Правила

Основные

В этом разделе можно включить или отключить файрвол Bitdefender и настроить общие параметры.



Политики - Общие настройки файрволла

- **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** .

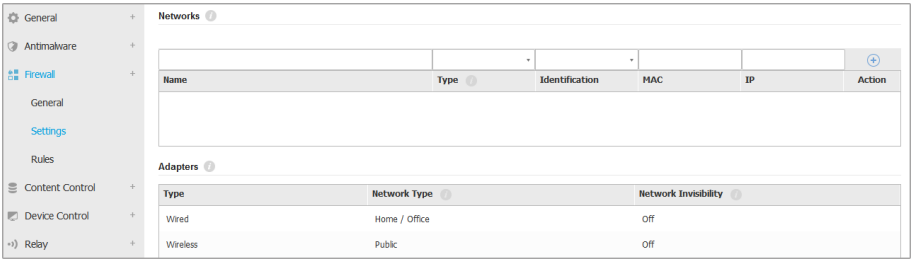
Важно
Система обнаружения вторжений доступна только для клиентов Endpoint Security.

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 **Сети**. 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**, **Шлюх** и **Сеть**.
  - **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**.

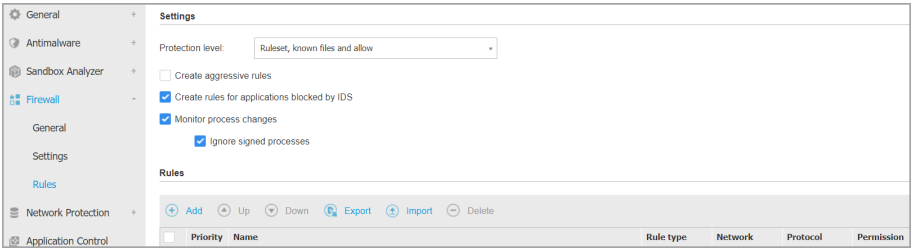
  Если обнаружение, основанное на управлении сетями Windows, даст сбой, будет применена попытка основного обнаружения. Общий профиль используется, когда назначен сетевой профиль **Общественный** и настройки видимости установлены в состояние **Включен**.

  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)
`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**

Поле	Имя и значение
`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
`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

Поле	Имя и значение
`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

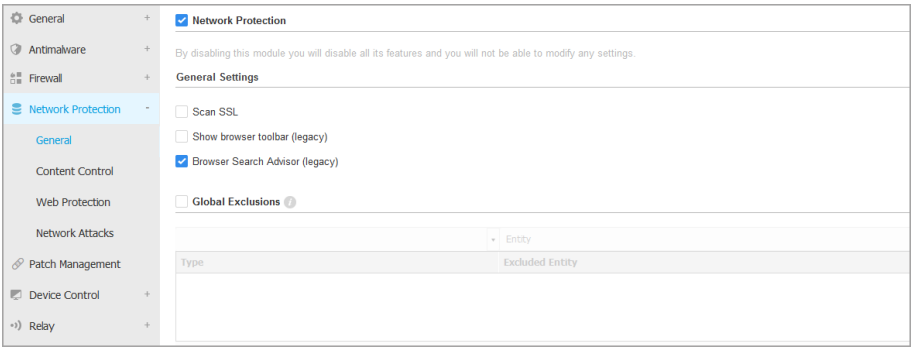
На macOS Контроль устройств использует расширение ядра или системы. Установка расширения ядра требует подтверждения пользователя на macOS High Sierra (10.13.x). Система уведомляет пользователя о том, что расширение системы от Bitdefender было заблокировано. Пользователь может разрешить это в настройках **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 просмотрают. 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: `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".

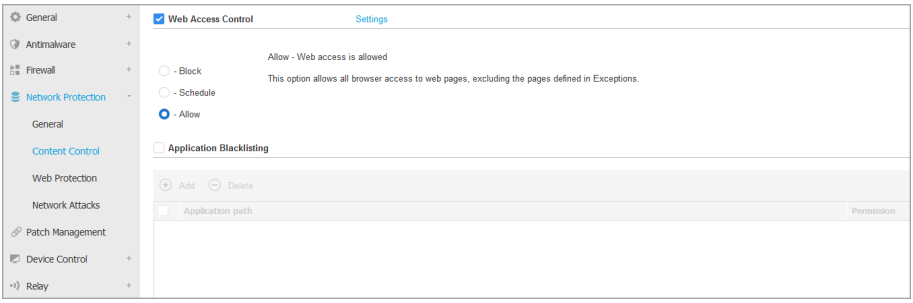
3. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы.

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.

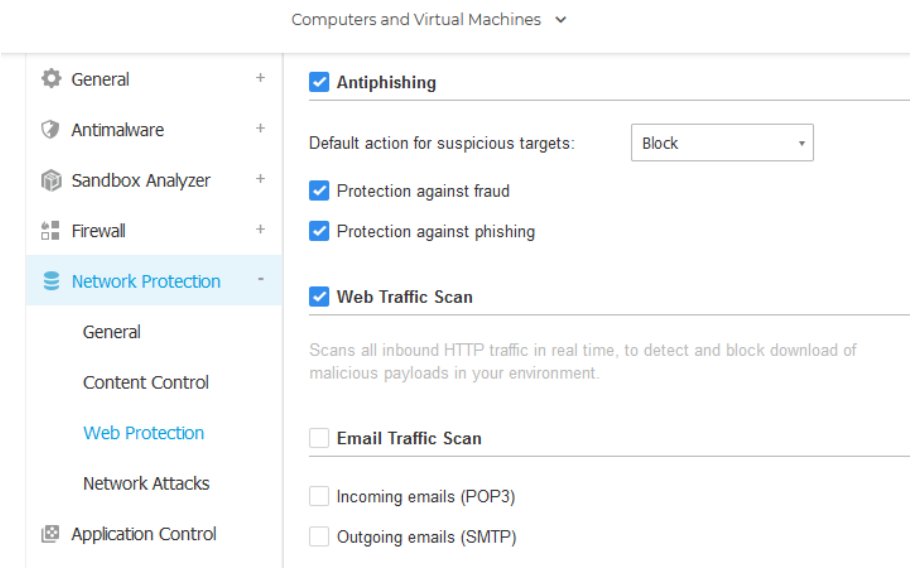
Примечание
Если письмо, содержащее блокируемые данные, адресовано нескольким получателям, для которых были определены исключения, они его получат.

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.

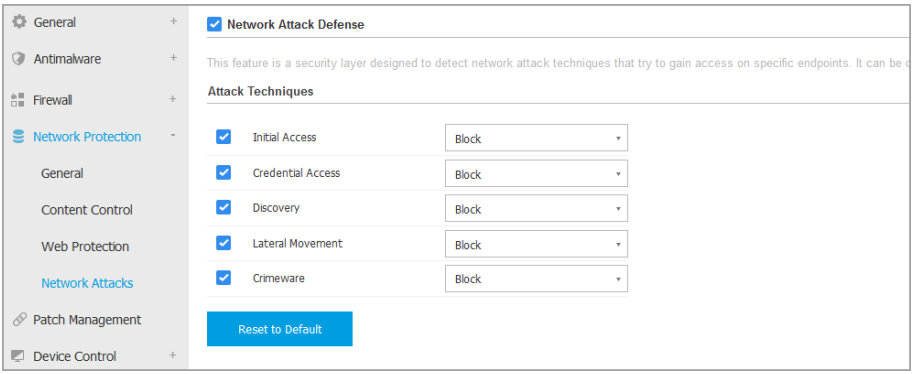
При обнаружении зараженной электронной почты, она автоматически заменяется стандартным письмом, информирующим получателя оригинального зараженного письма.

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.

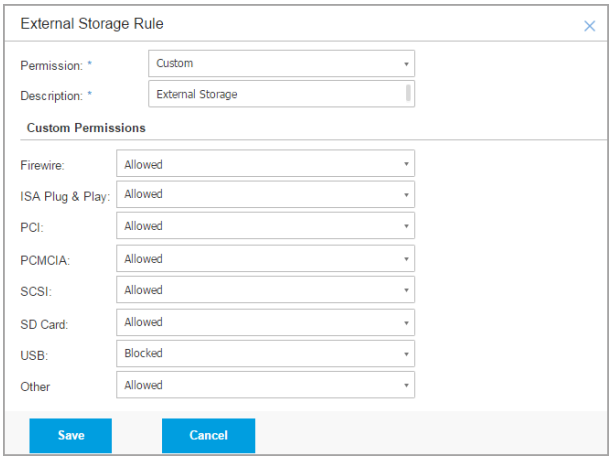
Чтобы задать разрешения определенным типам устройств:

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**.

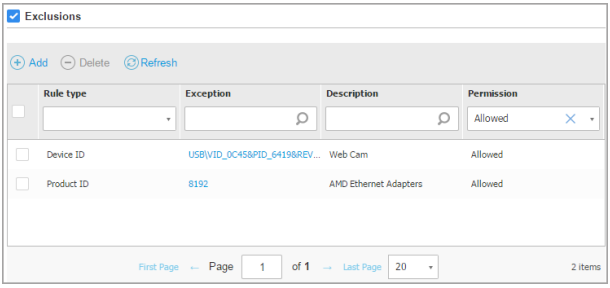
Важно

- 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

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.

- **Определить пользовательское место обновления**. По умолчанию, обновления для агентов-ретрансляторов располагаются на локальном сервере обновлений GravityZone. Вы можете указать другие источники обновлений, указав IP-адрес или имя одного или нескольких серверов обновлений в сети, а затем настроить приоритеты их использования кнопками 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. 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.

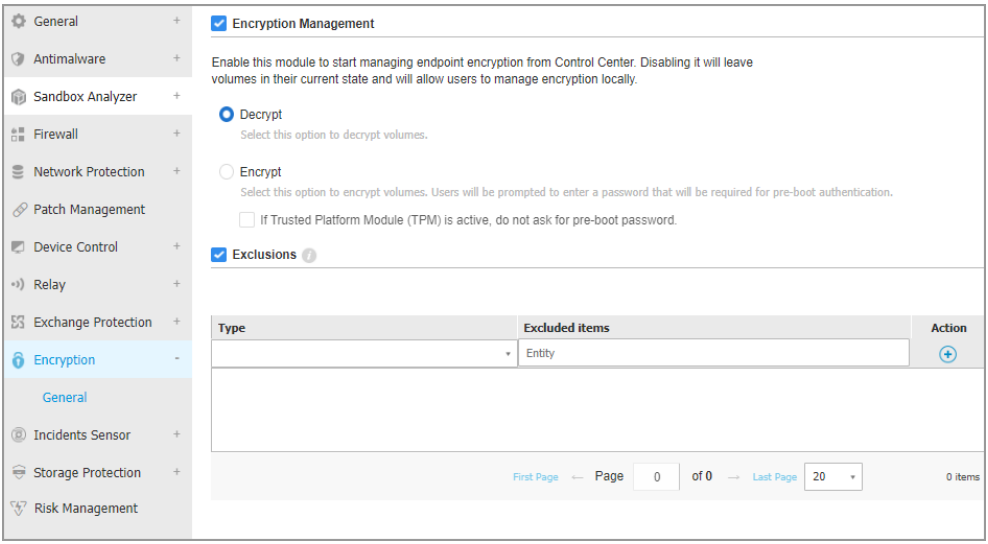
При таком подходе GravityZone может обеспечить некоторые постоянные преимущества:

- 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. 254).

- **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. ???.

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** ⊗.

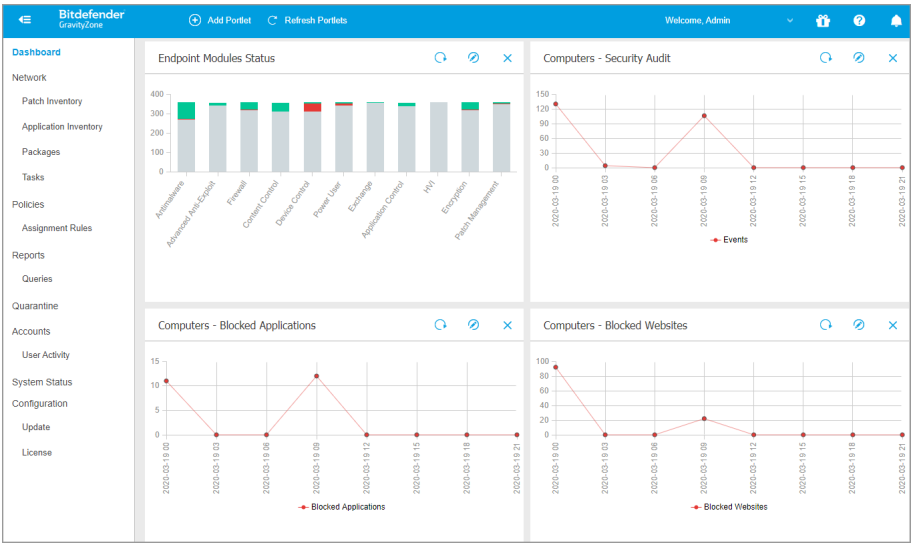
8. ИНФОРМАЦИОННАЯ ПАНЕЛЬ МОНИТОРИНГА

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.

8.1. Панель управления

Панель Control Center - настраиваемый визуальный дисплей, обеспечивающий быстрый обзор всех конечных точек и статуса сети.

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 конечной точки (**Компьютеры** или **Виртуальные машины**)
   - 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. 261).
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.

9. 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).

9.1. Типы отчетов

Следующие типы отчетов доступны для физических и виртуальных машин:

Антифишинговая активность

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.

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

При нажатии кнопки **Добавить исключения** для выбранного обнаружения автоматически создается запись в **Глобальных исключениях** из раздела **Защита сети**.

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.

Аудит безопасности

Предоставляет информацию о событиях безопасности, произошедших на выбранном объекте. Информация относится к следующим событиям:

- Обнаружение вредоносного ПО
-
-
-
-
- Network Attack Defense события
- Обнаружение программы-вымогателя

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.

Состояние обновления

Показывает состояние обновления агента безопасности, установленного для выбранных целей. 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.

9.2. Создание отчетов

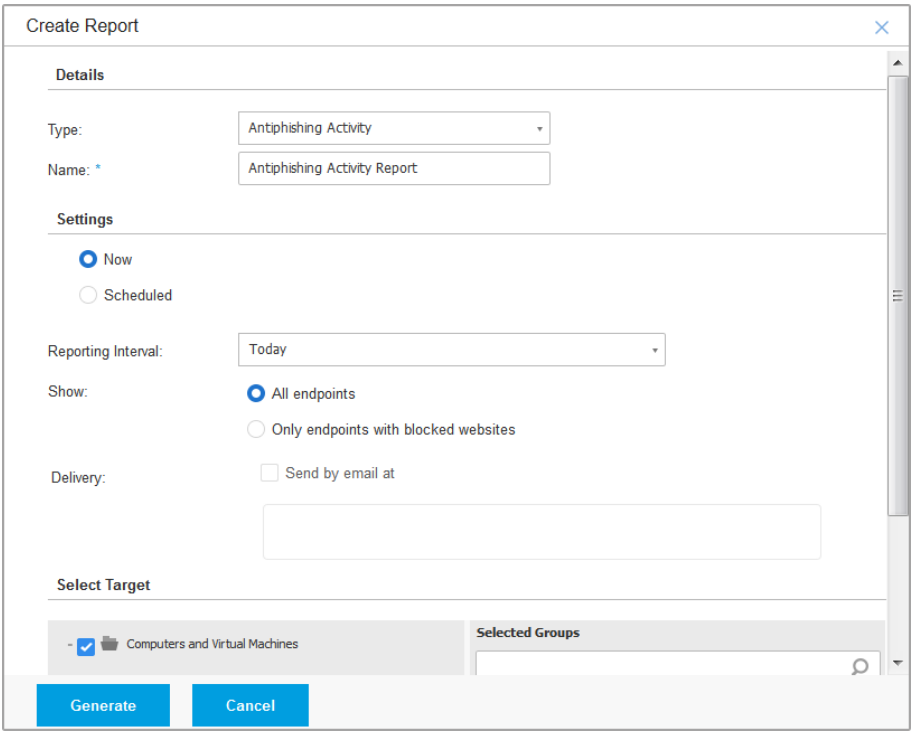
Вы можете создать две категории отчетов:

- **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. Выберите тип объектов сети из меню видов сетей.
3. Нажмите кнопку ⊕ **Добавить** в верхней части таблицы. Появится окно конфигурации.



Настройки отчета

4. Выберите нужный тип отчета из меню. Для получения более подробной информации, обратитесь к «Типы отчетов» (p. 261).
5. Введите подходящее имя для отчета. При выборе имени учитывайте тип отчета, его назначение и возможности параметров отчета.
6. 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).

7. Для большинства типов отчетов вам необходимо указать интервал времени, к которому относятся обрабатываемые данные. В отчете будут отображаться данные только за выбранный период времени.

8. 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.

9. **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.

10. **Выберите цель**. Прокрутите вниз, чтобы выбрать объекты отчета. Выберите одну или несколько групп конечных точек, которые вы хотите включить в отчет.

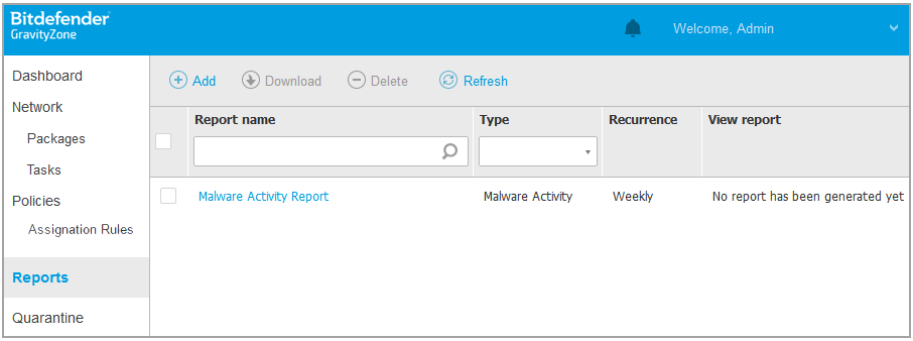
11. В зависимости от выбранной переодичности, нажмите **Создать**, чтобы создать мгновенный отчет или **Сохранить**, чтобы создать отчет по расписанию.

    - 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**.

9.3. 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.

9.3.1. 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. 271)

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.

9.3.2. 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.

9.3.3. 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.

9.4. 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.

9.5. 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

9.5.1. 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.

9.5.2. 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.

9.6. 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.

9.7. Печать отчетов

Control Center в настоящее время не поддерживает функцию печати. Чтобы напечатать отчет, необходимо сначала сохранить его на свой компьютер.

10. 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:

1. **Область фильтрации** позволяет вам искать и фильтровать материалы по различным критериям: имя, хэш, дата, результат анализа, статус, среда детонации и техники MITRE's 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

10.1. 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 **OK** , 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. 320).
- **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 сетевого трафика** . Датчик сети отправил образец в локальный экземпляр Sandbox Analyzer на основе параметров политики.
  - **Централизованный карантин** . GravityZone отправил образец в локальный экземпляр Sandbox Analyzer на основе параметров политики.
  - **API**. Образец был передан в локальный экземпляр Sandbox Analyzer с помощью методов API.
  - **Датчик ICAP**. Security Server отправил образец в локальный экземпляр Sandbox Analyzer после сканирования сервера ICAP.

- **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.

10.2. 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
- Конечная точка, отправившая образец в Sandbox Analyzer
- 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.

10.3. Повторное представление образца

Из области карточек отправки вы можете повторно отправить детонированные образцы в локальный экземпляр Sandbox Analyzer, не загружая их снова. Вы можете сделать это для образцов, ранее переданных в локальный экземпляр Sandbox Analyzer любым датчиком или методом, автоматически, вручную или через API.

Чтобы повторно отправить образец:

1. Нажмите **Повторно отправить для анализа** в карточке отправки.
2. В окне конфигурации сохраните настройки из предыдущей отправки или измените их следующим образом:
   a. В разделе **Управление изображениями** выберите образ виртуальной машины, который вы хотите использовать для детонации.
   b. В разделе **Конфигурации детонации** настройте следующие параметры:
      i. **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.
      ii. **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.
      iii. **Предфильтрация** . Выберите этот параметр, чтобы исключить из детонации уже проанализированные образцы.
      iv. **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.

c. 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**.

3. Нажмите **Отправить повторно**.

После повторной отправки на странице **Sandbox Analyzer** отображается новая карта, и срок хранения данных для этого образца соответственно увеличивается.

Примечание
Параметр **Повторно отправить для анализа** доступен для образцов, которые все еще присутствуют в хранилище данных Sandbox Analyzer. Убедитесь, что хранение данных настроено на странице параметров политики **Sandbox Analyzer > Sandbox Manager** .

10.4. 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.

10.5. 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. 14).
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:
   - Sandbox Analyzer экземпляр, который вы хотите использовать. Вы можете выбрать несколько виртуальных машин, куда можно отправить образец сразу.
   - **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**

10.6. Инфраструктура управления Sandbox Analyzer

В разделе **Sandbox Analyzer > Инфраструктура**, вы можете выполнить следующие действия, связанные с Sandbox Analyzer экземпляр установлен локально:

- Проверьте статус экземпляра Sandbox Analyzer
- Настроить количество одновременных детонаций
- Проверить статус образов виртуальных машин
- Настроить и управлять образами виртуальных машин

10.6.1. Проверка статуса Sandbox Analyzer

После развертывания и настройки Sandbox Analyzer виртуального устройства на гипервизоре ESXi, вы можете получить информацию о локальных примерах Sandbox Analyzer в разделе **Статус** .

В таблице приведены следующие данные:

- **Sandbox Analyzer имя экземпляра**. Каждое имя соответствует экземпляру Sandbox Analyzer установленному на один гипервизор ESXi. Вы можете установить анализатор песочницы на нескольких ESXi гипервизорах.
- **Сдетонировавшие образцы**. Значение указывает количество образцов, проанализированных с момента как экземпляр Sandbox Analyzer был лицензирован в первый раз.
- **Использование диска**. Процентаж указывает объем дискового пространства, используемого Sandbox Analyzer на хранилище данных.
- **Статус**. В этой колонке вы видите информацию о том, что данный Sandbox Analyzer экземпляр онлайн, оффлайн, не установлен, установка продолжается или установка не удалась.

- **Максимальное количество одновременных детонаций**. Значение показывает максимальное число виртуальных машин, которые Sandbox Analyzer может создать, чтобы взорвать образцы. В данный момент времени, одна виртуальная машина может выполнять одну детонации. Количество виртуальных машин определяется количеством аппаратных ресурсов на ESXi.
- **настройка одновременных детонаций**. Это фактическое количество виртуальных машин, созданных на основе имеющейся лицензий.
- **Использовать прокси-сервер**. Нажмите кнопку Вкл/Выкл, чтобы включить или отключить связь между экземплярами GravityZone Control Center и Sandbox Analyzer через прокси-сервер. Чтобы настроить прокси-сервер, перейдите в раздел **Configuration > Proxy** в главном меню Control Center. Если ни один прокси-сервер не установлен, Control Center не поддерживает данную функцию.

  Дополнительные сведения о конфигурации прокси-сервера см. в разделе **Установка защиты > установка и настройка GravityZone > Настройка параметров Control Center > прокси-сервер** в руководстве по установке GravityZone.

  Примечание
  Прокси-серверы, настроенные в GravityZone, имеют разные роли:
  - Control Center использует прокси-сервер, указанный в **Конфигурации > Прокси-сервер** для связи с локальными экземплярами Sandbox Analyzer и Облачным порталом Sandbox Analyzer.
  - Агенты безопасности, установленные на конечных точках, используют для отправки прокси-сервер, указанный на странице **Sandbox Analyzer** в настройках политики.
  - Прокси - сервер, указанный на странице **Общие настройки** в настройках политики, обеспечивает связь между агентами безопасности и другими компонентами GravityZone.

  Важно
  Для отправки вручную на облачный портал Sandbox Analyzer требуется прокси-сервер HTTPS.

Вы можете искать и фильтровать столбцы по имени и статусу экземпляра Sandbox Analyzer. Используйте кнопки в правом верхнем углу таблицы для

обновления страницы, а также для отображения и скрытия фильтров и столбцов.

10.6.2. Настройка одновременных детонаций

В разделе **Status**, вы можете настроить количество одновременных детонаций, представляющее количество виртуальных машин, которые могут одновременно работать и детонировать образцы на Sandbox Analyzer. Количество одновременных детонаций зависят от аппаратных ресурсов и лицензий на распространение слотов между несколькими Sandbox Analyzer экземпляров.

Чтобы настроить количество одновременных детонаций:

1. Нажмите на номер или значок **Edit** в столбце **Configured Concurrent Detonations**.
2. В новом окне укажите в соответствующем поле количество одновременных детонаций, которое вы хотите выделить в Sandbox Analyzer.
3. Нажмите **Сохранить**.

10.6.3. Проверка состояния VM.

Sandbox Analyzer использует образы виртуальных машин в средах детонации для выполнения поведенческого анализа представленных образцов. Вы можете проверить состояние виртуальной машины в **Image Management page**.

В таблице приведены следующие данные:

- **Имя** для существующих образов виртуальных машин, как указано в консоли Sandbox Analyzer. Несколько образов виртуальных машин сгруппированы в одной песочнице анализаторе.
- **Операционная система** как указано в консоли Sandbox Analyzer.
- Время, когда виртуальная машина была добавлена.
- **Статус**. В этом разделе вы узнайте, является ли образ виртуальной машины новым и может быть подготовлен к детонации, готов ли к детонации или процесс подготовки не удалось.
- **Действия**. В этом разделе вы узнайте, что можно сделать с помощью образов виртуальных машин, в зависимости от их статуса: создание

изображений для детонации, установка их в качестве среды детонации по умолчанию, или их удаление.

10.6.4. Настройка и управление VM

Строение детонации виртуальных машин

Чтобы взорвать образцы с помощью локального экземпляра в песочнице анализаторе, вам нужно построить специальные виртуальные машины. В разделе **Управление изображениями** вы можете создавать детонации виртуальных машин, если вы добавили образы виртуальных машин в песочнице анализаторе.

Примечание
Чтобы узнать, как добавить VM в Sandbox Analyzer консоли прибора, обратитесь к **Установка Sandbox Analyzer Виртуальное устройство** к разделу руководство по установке в GravityZone.

яЧтобы создать детонационные виртуальные машины, в столбце **Действия** выберите параметр **Создать образ** для образов виртуальных машин, имеющих статус: **Новое-требуется сборка**. Создание виртуальной машины обычно требуется от 15 до 30 минут, в зависимости от её размера. Когда сборка будет завершена, статус виртуальной машины изменения на **Готово**.

Настройка виртуальной машине по умолчанию

В Sandbox Analyzer может иметь несколько изображений и установлен и настроен на детонация виртуальных машин. В случае автоматического регистрации, Sandbox Analyzer будет использовать первый созданный образ виртуальной машины, чтобы взорвать образцы.

Вы можете изменить это поведение, настроив изображения виртуальную машину по умолчанию. Для этого нажмите кнопку **Установить по умолчанию** для предпочтительного образа виртуальной машины.

Удаление Виртуальных Машин

Чтобы удалить образ виртуальной машины в разделе **Управление изображениями** , выберите **Удалить** в колонке**Действия**. В окне подтверждения нажмите **Удалить изображение**.

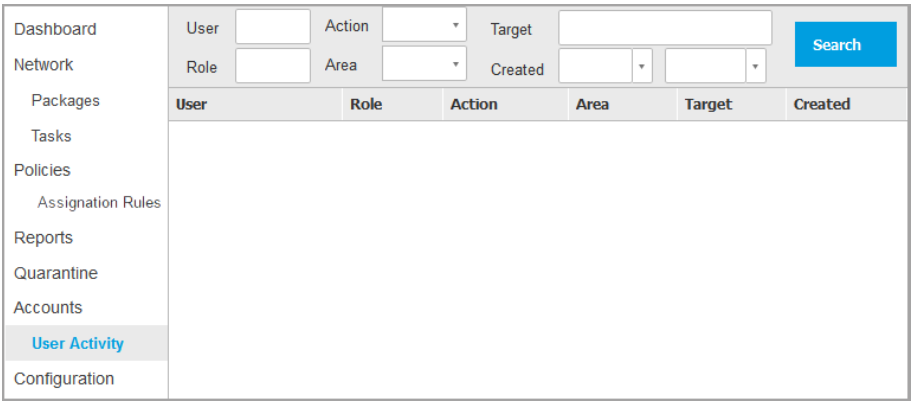
11. ЖУРНАЛ АКТИВНОСТИ ПОЛЬЗОВАТЕЛЯ

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
- Создание, редактирование и удаление учетных данных
- Создание, изменение, загрузка и удаление сетевых пакетов
- Создание сетевых задач
- Запуск, завершение, отмена и остановка процессов устранения неполадок на зараженных компьютерах
- Создание, редактирование, переименование и удаление учетных записей пользователей
- Удаление или перемещение конечных точек между группами
- Создание, перемещение, переименование и удаление групп
- Удаление и восстановление файлов из карантина
- Создание, редактирование и удаление учетных записей пользователей
- Создание, редактирование и удаление правил доступа.
- Создание, редактирование, переименование, назначение и удаление политик
- Редактирование параметров аутентификации для учетных записей GravityZone.
- Создание, редактирование, синхронизация и удаление интеграции с Amazon EC2
- Создание, редактирование, синхронизация и удаление интеграций Microsoft Azure
- Обновление устройства GravityZone.

Чтобы изучить записи действий пользователей, перейдите на страницу **Аккаунты > Действия пользователя** и выберите требуемый вид сети из меню видов сетей.

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:

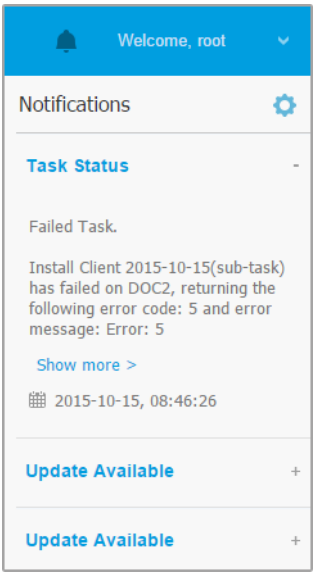
- Имя пользователя, который совершил действие.
- Роль пользователя.
- Действие, которое вызвало событие.
- Тип объекта консоли, затронутый действием.
- Конкретный объект консоли, затронутый действием.
- Время, когда произошло событие.

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.

12. 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.

12.1. 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. 295).

Доступные форматы системного журнала: JSON, CEF

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** .

Доступные форматы системного журнала: JSON, CEF

Лимит использования лицензии достигнут

Это уведомление отправляется, когда все доступные лицензии использованы.

Доступные форматы системного журнала: JSON, CEF

Срок действия лицензии подходит к концу

Это уведомление отправляется, когда использовано 90% имеющихся лицензий.

Для просмотра этого уведомления необходимо иметь права **Управление компанией** .

Доступные форматы системного журнала: JSON, CEF

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** .

Доступные форматы системного журнала: JSON, CEF

Лимит лицензирования серверов почти достигнут.

Это уведомление отправляется, когда использовано 90% имеющихся серверных лицензий.

Для просмотра этого уведомления необходимо иметь права **Управление компанией** .

Доступные форматы системного журнала: JSON, CEF

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** .

Доступные форматы системного журнала: JSON, CEF

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.

Доступные форматы системного журнала: JSON, CEF

Состояние обновления версии продуктов

Это уведомление запускается еженедельно, если в сети обнаружены старые версии продукта.

Доступные форматы системного журнала: JSON, CEF

Доступно обновление

Это уведомление информирует вас о наличии новой версии GravityZone - нового пакета обновления или нового продукта.

Доступные форматы системного журнала: JSON, CEF

Подключение к сети Интернет

Это уведомление срабатывает, когда обнаружено изменение в подключении к сети Интернет следующими процессами:

- Проверка лицензии
- Доступ к аккаунту MyBitdefender

Доступные форматы системного журнала: JSON, CEF

Соединение SMTP

Это уведомление отправляется каждый раз, когда Bitdefender GravityZone обнаруживает изменения, касающиеся подключения почтового сервера.

Доступные форматы системного журнала: JSON, CEF

Резервное копирование базы данных

Это уведомление информирует вас о состоянии запланированного резервного копирования базы данных - успешное или неудачное. Если резервное копирование базы данных не удалось, уведомление также отобразит причину сбоя.

Для получения подробной информации о настройках резервного копирования базы данных GravityZone, обратитесь к руководству по установке GravityZone.

Доступные форматы системного журнала: JSON, CEF

Автоматическое обновление интеграции XenServer

Данное уведомление появляется, когда происходит автоматическое обновление параметров интеграции, после чего хозяин Xenserver получает новый IP.

Доступные форматы системного журнала: JSON

Событие о вредоносном ПО

Это уведомление предупредит вас при обнаружении вредоносного ПО на конечном устройстве в вашей сети. Данное уведомление создано для обнаружения зловредных программ и обеспечивает сведениями о поврежденных конечных точках (имя, IP), распознанных угрозах, версии подписи, времени обнаружения и типе сканирующего двигателя.

Доступные форматы системного журнала: JSON, CEF

Вне интеграции синхронизации

Это уведомление отправляется, когда существующая интеграция с виртуальной платформой не может синхронизироваться с GravityZone. В настройках уведомлений вы можете выбрать интеграцию, для которой желаете получать уведомления при возникновении ошибки синхронизации. Вы можете получить больше информации о статусе синхронизации в деталях уведомления.

Доступные форматы системного журнала: JSON, CEF

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.

Доступные форматы системного журнала: JSON, CEF

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.

Доступные форматы системного журнала: JSON, CEF

События защиты данных

Это уведомление формируется каждый раз, когда трафик блокируется на конечном устройстве в соответствии с правилами защиты данных.

Доступные форматы системного журнала: JSON, CEF

События модуля приложений

Это уведомление направляется каждый раз, когда модуль безопасности в установленном агенте отключается или включается.

Доступные форматы системного журнала: JSON, CEF

События регистрации продуктов

Это уведомление информирует вас, когда статус регистрации агента, установленного в вашей сети, изменяется.

Доступные форматы системного журнала: JSON, CEF

Аудит аутентификации

Это уведомление информирует вас, когда другая учетная записьGravityZone, исключая вашу собственную, была использована, чтобы войти в Control Center с нераспознанного устройства.

Доступные форматы системного журнала: JSON, CEF

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.

Доступные форматы системного журнала: JSON, CEF

Сертификат Истекает

Это уведомление информирует вас о том, что сертификат безопасности истекает. Уведомление направляется за 30, семь и один день до истечения срока действия.

Доступные форматы системного журнала: JSON, CEF

GravityZone Обновлен

Это уведомление отправляется, когда обновление GravityZone завершено. Если произошла ошибка, то обновление будет запущено снова в течение 24 часов.

Доступные форматы системного журнала: JSON, CEF

Статус задачи

Данное уведомление предупредит вас, когда статус задания изменен или только при завершении задания, в соответствии с вашими настройками.

Доступные форматы системного журнала: JSON, CEF

Сервер обновлений устарел

Это уведомление отправляется, когда сервер обновлений в вашей сети имеет устаревшие механизмы защиты.

Доступные форматы системного журнала: JSON, CEF

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.

Доступные форматы системного журнала: JSON, CEF

Вне интеграции синхронизации

Это уведомление информирует вас о проблемах интеграции и невозможности синхронизации. Это может произойти из-за различных факторов, таких как измененные параметры интеграции или временной недоступности сервера.

Доступные форматы системного журнала: JSON, CEF

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.

Доступные форматы системного журнала: JSON, CEF

Заблокированные устройства

Это уведомление инициируется, когда к конечной точке подключается заблокированное устройство или устройство с разрешением только для чтения. Если одно и то же устройство подключается несколько раз в течение одного часа, в течение этого интервала отправляется только одно уведомление. Если устройство снова подключается через час, выдается новое уведомление.

Доступные форматы системного журнала: JSON, CEF

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.

Доступные форматы системного журнала: JSON, CEF

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

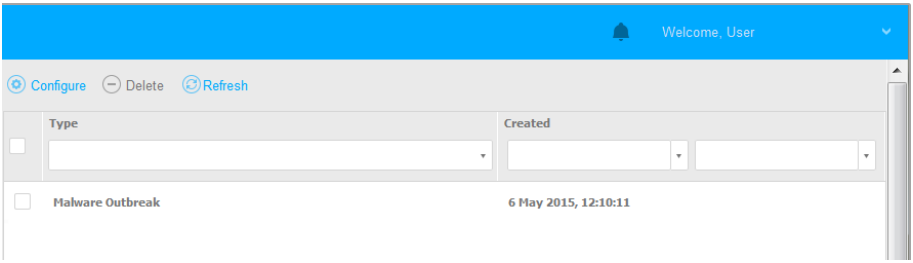
Это уведомление сообщает Вам о включении политики блокировки учетной записи для Вашего аккаунта.

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.

12.2. 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.

12.3. 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.

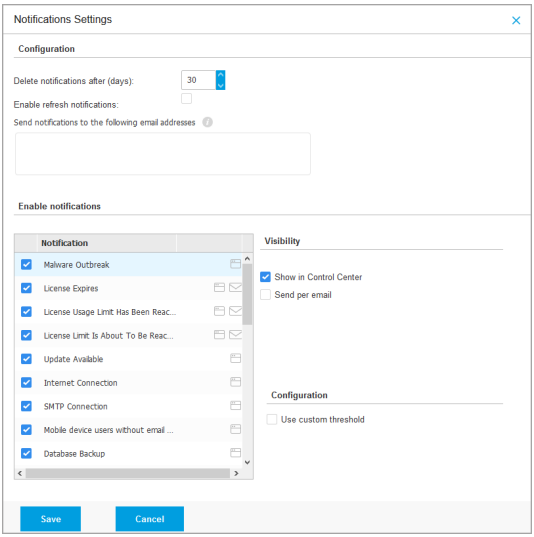
Вы также можете настроить уведомления для автоматического удаления после определенного количества дней. Для получения более подробной информации, обратитесь к «Настройка параметров уведомлений» (p. 295).

12.4. 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 0 до 365 в поле **Удалить уведомления через (дней)** .
   - Отметьте флажок **Включите уведомления об обновлениях**, если вы хотите, чтобы область уведомлений автоматически обновлялась каждые 60 секунд.
   - 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. 287). 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 журнал на сервер** обозначает, что данный тип событий также отправляется в файл `syslog`, в случае если syslog-сервер сконфигурирован.

  Чтобы узнать о том, как настроить syslog-серверы, обратитесь к Руководству по установке GravityZone.
- **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.

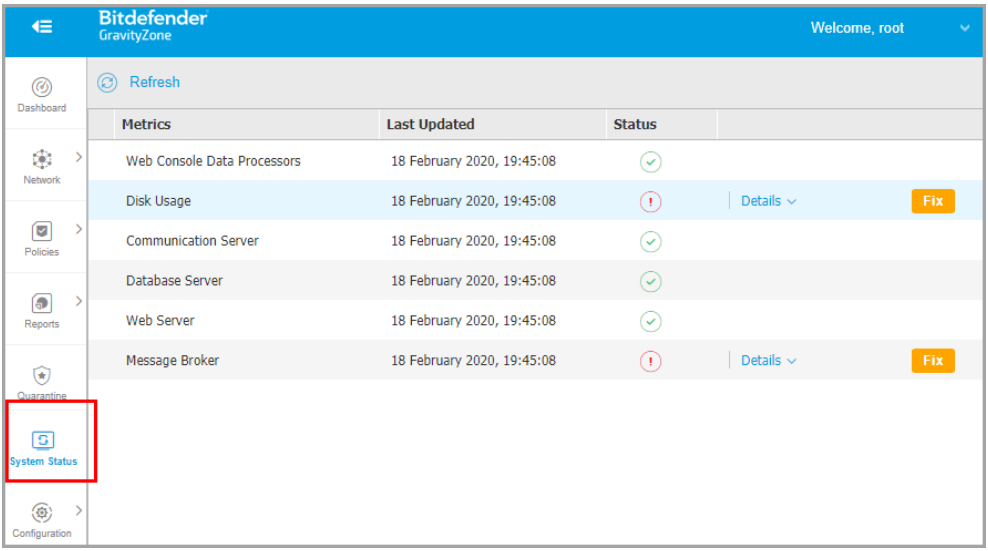
  Например, уведомление о вспышках заражения вредоносным ПО отправляется по умолчанию пользователям, если не менее 5% всех управляемых объектов сети заражены одним и тем же вредоносным ПО. Чтобы изменить порог срабатывания о вспышках заражения, разрешите опцию **Использовать пользовательский порог**, затем введите желаемое значение в поле **Порог вспышки вредоносного ПО**.
- Для уведомления **Database Backup** вы можете выбрать только получение уведомлений о сбое резервного копирования. Оставьте эту опцию неотмеченной, если хотите получать уведомления о всех событиях, связанных с резервным копированием.

- 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**.

13. СТАТУС СИСТЕМЫ

На странице **Статус системы** отображается информация о состоянии работоспособности развертывания GravityZone, что упрощает просмотр при возникновении неполадок. На странице представлены системные показатели, их статус и когда они были обновлены в последний раз, все отображаются в виде сетки.



Страница статуса системы

В столбце **Показатели** отображаются все индикаторы, отслеживаемые GravityZone Control Center. Подробнее о каждой показатели и статусе сообщений см. В разделе «Процессоры данных» (p. 322).

В столбце **Последнее обновление** отображаются дата и время последней проверки состояния метрики.

В столбце **Статус** отображается состояние каждой метрики: **OK** или **Внимание**. **Статус** показателя обновляется каждые 15 минут или каждый раз, когда вы нажимаете кнопку **Обновить**

13.1. Состояние OK

Статус OK указывает на то, что показатель ведет себя нормально. Никаких дополнительных подробностей в этом случае не отображается.

13.2. Статус учетной записи

Статус учетной записи отображает метрику, которую невозможно запустить при нормальных параметрах

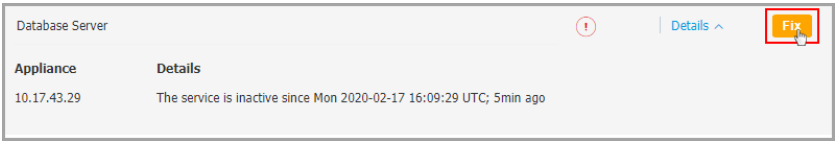
В данном случае Вам следует понять, что произошло и выбрать текущие действия:

1. Нажмите кнопку **Подробности** чтобы развернуть дополнительную информацию, связанную с рассматриваемым параметром.

Детали параметров

- В разделе **Устройство** вы можете найти IP-адреса зараженных компьютеров.
- В разделе **Подробности** вы можете просмотреть информацию, относящуюся к каждому параметру.

2. Нажмите **Fix** для восстановления метрики и GravityZone сделает все за Вас.



Детали параметров

Статус метрики будет отвернут от **OK** до тех пор, пока он не будет исправлен.

Примечание
Для другой метрики, относящейся к делу, свяжитесь с Командой по поддержке предприятия.

13.3. Параметры

Страница **System Status** содержит сведения о следующих показателях:

- Процессоры данных веб-консоли
- Использование диска
- Коммуникационный Сервер
- Сервер базы данных
- Веб-сервис
- Брокер сообщений

Процессоры данных веб-консоли

Этот показатель отслеживает состояние процессоров данных, которые используются для компиляции данных, отображаемых в Control Center.

Сообщение о возможной проблеме статуса	Подробная информация
`Процессоры, которые вышли из строя на этом устройстве: <массив процессоров данных> .`	Один или несколько процессоров данных остановлены.
`Виртуальное устройство не работает`	Виртуальное устройство, использующее службы веб-консоли, остановлено.

Полный список процессоров, используемых Control Center, см. в «Процессоры данных» (p. 322).

Использование диска

Этот показатель отслеживает объем дискового пространства, используемого на каждом виртуальном устройстве, объем оставшегося свободного места, а также общее пространство на диске. Если какой-либо из дисков используется выше 80%, параметр отображает статус **Внимание**

Сообщение о возможной проблеме статуса	Подробная информация
`Используемое место на диске (имя диска)`	Один или несколько дисков используются свыше 80% их максимальной емкости.
`Виртуальное устройство не работает`	Указанное виртуальное устройство отключено.

Коммуникационный Сервер

Этот показатель отслеживает связь между агентами безопасности, установленными на ваших конечных точках, и сервером базы данных.

Сообщение о возможной проблеме статуса	Подробная информация
`Служба неактивна <timestamp>`	Данный сервис остановлен.

Сервер базы данных

Этот показатель отслеживает состояние базы данных GravityZone.

Сообщение о возможной проблеме статуса	Подробная информация
`Служба неактивна <timestamp>`	Сервис перестал работать на одном из устройств.
`Виртуальное устройство не работает`	Виртуальное устройство, использующее сервер базы данных, выключено.

Веб-сервис

Этот показатель отслеживает состояние веб-сервера, на котором размещается GravityZone Control Center.

Сообщение о возможной проблеме статуса	Подробная информация
Служба неактивна <timestamp>	Сервер перестал работать на одном из устройств.
Виртуальное устройство не работает	Виртуальное устройство, использующее этот сервер, выключено.

Брокер сообщений

Этот показатель отслеживает состояние службы брокера сообщений на устройствах с ролями веб-консоли и сервера связи.

Сообщение о возможной проблеме статуса	Подробная информация
Служба брокера сообщений не работает на этом устройстве	Сервис перестал работать на одном из устройств.
Не удалось установить сетевое соединение между устройствами	Связь между двумя приборами прервана.
Виртуальное устройство не работает	Виртуальное устройство, использующее этот сервис, отключено.

14. 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.

14.1. 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.

Вы также можете проверить и загрузить документацию в разделе Центр поддержки во вкладке **Документация** , доступной на каждой странице поддержки продукта.

14.2. Обращение за помощью

Вы можете обратиться за помощью в наш онлайн Центр поддержки. Заполните контактная форма и примите.

14.3. 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.

14.3.1. 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.

14.3.2. 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

14.3.3. 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.

14.4. 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.

14.4.1. 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

14.4.2. 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.

14.4.3. 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
Веб-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
Веб-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
Веб-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
Веб-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
Веб-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
	Виртуальная машина
	Виртуальная машина ретранслятора
	Золотой образ
	Инвентаризация Nutanix
	Nutanix Prism
	кластер Nutanix
	Содержимое VMware
	VMware vCenter
	VMware дата-центр
	Пул ресурсов VMware
	Кластер VMware
	Содержимое Citrix
	XenServer
	Пул серверов Xen
	Инвентаризация Amazon EC2

Значок	Тип
	Интеграция Amazon EC2
	Amazon EC2 / Регион Microsoft Azure
	Amazon EC2 / Зона доступности Microsoft Azure
	Инвентаризация Microsoft Azure
	Инвентаризация Microsoft Azure
	VMware vApp

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
	Хост без сервера безопасности, отключен
	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. 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.5. Объекты Sandbox Analyzer

A.5.1. 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.5.2. 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.5.3. Исключения По Умолчанию в Автоматической Отправке

`asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt.`

A.5.4. Рекомендуемые приложения для детонации виртуальных машин

Sandbox Analyzer On-Premises требует, чтобы определенные приложения были установлены на виртуальных машинах детонации, чтобы они открывали отправленные образцы.

Приложения	Типы файлов.
Пакет Microsoft Office	xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx
Adobe Flash Player	swf
Программа Adobe Acrobat Reader	pdf
Windows по умолчанию	bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif
7zip WinZip WinRAR	7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue
Google Chrome Internet Explorer	html, url
Python	py, pyc, pyp
Mozilla Thunderbird Microsoft Outlook	eml

A.6. Процессоры данных

Имя	Подробная информация
Процессор пересылки запросов	Пересылает запросы процессора в различных средах
Аппаратный гипервизор VMware	Синхронизирует ресурсы VMware и другую информацию с GravityZone
Аппаратный гипервизор Citrix	Синхронизирует ресурсы Xen и другую информацию с GravityZone
Универсальный интегратор виртуализации	Синхронизирует ресурсы Nutanix, Amazon EC2 и Azure с GravityZone
Интегратор NTSA	Синхронизирует состояние интеграции Network Traffic Security Analytics (NTSA)и отправляет обновления лицензии на устройство (NTSA)
Синхронизация инвентаризации компьютеров Active Directory	Синхронизирует инвентаризацию компьютеров Active Directory с GravityZone
Синхронизация инвентаризации групп Active Directory	Синхронизирует инвентаризацию групп Active Directory с GravityZone
Синхронизация импорта пользователей Active Directory	Синхронизирует учетные записи пользователей Active Directory с GravityZone (используется для связывания учетных записей AD с учетными записями GravityZone)
Синхронизация инвентаризации пользователей Active Directory	Синхронизирует инвентаризацию пользователей Active Directory с GravityZone
Процессор электронной почты	Выстраивает в очередном порядке электронные письма для отправки от GravityZone
Процессор отчетов	Обрабатывает отчеты и портлеты

Имя	Подробная информация
Развертывание агента безопасности Windows	Задействование Bitdefenderагента безопасности для устройств Windows
Развертывание сервера безопасности	Развертывает виртуальные устройства безопасности
Использование лицензии	Управляет лицензиями установленных конечных точек
Процессор мобильных push-уведомлений	Отправляет push-уведомления на защищенные мобильные устройства
Развертывание агента безопасности Linux и macOS	Использует Bitdefender GravityZone безопасность предприятия для агента SVE на устройствах Linux и macOS
Комплекты конечных точек и средство обновления продукта	Загружает и публикует наборы конечных точек Bitdefender и обновления продуктов
GravityZone Обновлен	Автоматически обновляет GravityZone при настройке. Обновляет версию для виртуальных устройств GravityZone
Package Cleaner	Удаляет неиспользуемые файлы
Процессор вопросов безопасности	Обрабатывает проблемы безопасности для элементов в разделе Сеть
Резервный процессор	Выполняет резервное копирование базы данных GravityZone
Процессор уведомлений	Отправляет уведомления пользователям
Процессор системных событий	Обрабатывает события из инфраструктуры (Application Control, Sandbox Analyzer, Serenity, SVA) или интеграций (Exchange, Nutanix, NSX)
Задача Дополнительного пакета HVI	Управляет установкой, обновлением и удалением дополнительного пакета HVI для хостов XEN
HVI Reboot Task Processor	Управляет задачами перезагрузки на хостах HVI

Имя	Подробная информация
Состояние питания и состояние процессора	Вычисляет состояние питания и состояние подключения компьютеров и виртуальных машин
Процессор очистки автономных машин	Удаляет офлайн машины из сети
Выполнение* фоновых задач	Обрабатывает и запускает фоновые задачи

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 .

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.

Вирус

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.

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.

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.

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.