Bitdefender

GravityZone

GUIDA PER GLI AMMINISTRATORI

Bitdefender GravityZone
Guida per gli amministratori

Data di pubblicazione 2021.01.12

Diritto d'autore© 2021 Bitdefender

Avvertenze legali

Tutti i diritti riservati. Nessuna parte di questo manuale può essere riprodotta o trasmessa in alcuna forma o tramite qualsiasi strumento, elettronico o meccanico, incluse fotocopie, registrazioni, o attraverso qualsiasi informazione di archivio o sistema di recupero dati, senza il consenso scritto di un rappresentante autorizzato di Bitdefender. L'inserimento di brevi citazioni nelle recensioni è possibile solo indicando la fonte citata. Il contenuto non può essere modificato in alcun modo.

Avvertenze e Limiti. Questo prodotto e la sua documentazione sono protetti dal diritto d'autore. Le informazioni su questo documento sono fornite «così come sono» senza alcuna garanzia. Sebbene sia stata adottata ogni precauzione nella preparazione di questo documento, gli autori non hanno alcun obbligo nei confronti di alcuna persona o entità rispetto a qualsiasi perdita o danno causati o che si presume essere stati causati, direttamente o indirettamente, dalle informazioni contenute in questo prodotto.

Questo manuale contiene collegamenti a siti Internet di terze parti, che non sono sotto il controllo di Bitdefender, conseguentemente Bitdefender non è responsabile per il contenuto di qualsiasi sito collegato. Se accedi a siti Internet di terze parti, menzionati in questo manuale, lo farai assumendotene tutti i rischi. Bitdefender fornisce tali collegamenti solo come risorsa, e l'inclusione dei collegamenti non implica che Bitdefender approvi o accetti alcuna responsabilità per il contenuto dei siti di terze parti.

Marchi registrati. In questo manuale potrebbero essere citati nomi e marchi registrati. Tutti i marchi registrati e non in questo documento appartengono ai rispettivi proprietari e vengono rispettosamente riconosciuti.

Bitdefender

Indice

Prefazione

Questa guida è intesa per gli amministratori di rete che si occupano di gestire la protezione GravityZone per i loro clienti.

Questo documento intende illustrare come applicare e visualizzare le impostazioni di sicurezza sugli endpoint della rete con il tuo account, utilizzando GravityZone Control Center. Scoprire come visualizzare il tuo inventario di rete nella Control Center, come creare e applicare le policy sugli endpoint gestiti, come creare rapporti, come gestire gli elementi in quarantena e come usare la dashboard.

1. Convenzioni usate in questo manuale

Convenzioni tipografiche

Questa guida utilizza diversi stili di testo per migliorare la leggibilità. Scopri maggiori dettagli sul loro aspetto e significato nella tabella sottostante.

Aspetto	Descrizione
`campione`	I nomi dei comandi e le sintassi, i percorsi e i nomi dei file, i percorsi dei file di configurazione e i testi inseriti vengono stampati con caratteri a `spaziatura fissa`.
http://www.bitdefender.com	I link URL portano a ubicazioni esterne, su server http o ftp.
gravityzone-docs@bitdefender.com	Gli indirizzi e-mail vengono inseriti nel testo come informazioni di contatto.
«Prefazione» (p. viii)	Questo è un link interno, verso una qualche posizione nel documento.
opzione	Tutte le opzioni del prodotto sono indicate in **grassetto**.
parola chiave	Le opzioni dell'interfaccia, le parole chiave o le scorciatoie sono evidenziate usando caratteri **in grassetto**.

Avvertenze

Gli avvisi appaiono sotto forma di note di testo, segnalate graficamente, portando alla tua attenzione informazioni aggiuntive relative al paragrafo attuale.

Nota
La nota è una breve osservazione. Anche se la puoi omettere, la nota può fornire informazioni di valore come una caratteristica specifica o un link verso temi collegati.

Importante
Questa richiede attenzione, è sconsigliato saltarla. Solitamente contempla informazioni non critiche ma importanti.

Avvertimento
Questa è un'informazione critica che deve essere trattata con estrema cautela. Seguendone le indicazioni si eviteranno eventualità negative. Dovrebbe essere letta e compresa in quanto è la descrizione di qualcosa di estremamente rischioso.

1. INFORMAZIONI SU GRAVITYZONE

GravityZone è un prodotto con una console di gestione unificata disponibile nel cloud, ospitata da Bitdefender o come appliance virtuale da installare nelle strutture dell'azienda, fornendo un unico punto per la distribuzione, l'applicazione e la gestione delle policy di sicurezza per qualunque numero e tipo di endpoint, in qualsiasi posizione.

GravityZone offre più livelli di sicurezza per gli endpoint e per i mail server di Microsoft Exchange: antimalware con monitoraggio comportamentale, protezione da minacce zero-day, blacklist delle applicazioni e sandboxing, firewall, controllo dei dispositivi, controllo dei contenuti, anti-phishing e antispam.

2. LIVELLI DI PROTEZIONE DI GRAVITYZONE

GravityZone ti offre i seguenti livelli di protezione:

- Antimalware
- Advanced Threat Control
- HyperDetect
- Anti-exploit avanzato
- Firewall
- Controllo contenuti
- Patch Management
- Controllo dispositivi
- Full Disk Encryption
- Security for Exchange
- Sandbox Analyzer
- Endpoint Detection and Response (EDR)
- Endpoint Risk Analytics (ERA)
- Email Security

2.1. Antimalware

Il livello di protezione antimalware è basato su scansione delle firme e analisi euristica (B-HAVE, ATC) contro virus, worm, Trojan, spyware, adware, keylogger, rootkit e altri tipi di software dannoso.

La tecnologia di scansione di Bitdefender si basa sulle seguenti tecnologie:

- Per iniziare, viene impiegato un metodo di scansione tradizionale, dove i contenuti esaminati vengono confrontati con il database delle firme. Il database delle firme include schemi di byte specifici per le minacce conosciute e viene regolarmente aggiornato da Bitdefender. Questo metodo di scansione è efficace contro le minacce confermate che sono state individuate e documentate. Tuttavia, non importa quanto il database delle firme venga aggiornato prontamente, c'è sempre una finestra di vulnerabilità tra il momento in cui la minaccia viene scoperta e quello in cui viene rilasciata una soluzione.
- Contro le nuove minacce non ancora documentate, un secondo livello di protezione viene offerto da **B-HAVE**, il motore euristico di Bitdefender. Gli algoritmi euristici rilevano i malware basati sulle caratteristiche comportamentali. B-HAVE esegue i file sospetti in un ambiente virtuale per

testarne l'impatto sul sistema e assicurarsi che non siano una minaccia. Se viene rilevata una minaccia, viene bloccata l'esecuzione del programma.

Motori di scansione

Bitdefender GravityZone è in grado di impostare automaticamente i motori di scansione quando si creano i pacchetti dell'agente di sicurezza, in base alla configurazione dell'endpoint.

L'amministratore può anche personalizzare i motori di scansione, potendo scegliere tra diverse tecnologie di scansione:

1. **Scansione locale**, quando la scansione è eseguita su un endpoint in locale. La modalità di scansione locale è adatta per macchine potenti, con il contenuto di sicurezza memorizzato localmente.
2. **Scansione ibrida con motori leggeri (cloud pubblico)**, con un'impronta media, utilizzando la scansione in-the-cloud e, in parte, il contenuto di sicurezza in locale. Questa modalità di scansione ha il vantaggio di un miglior consumo delle risorse, mentre coinvolge la scansione off-premise.
3. **Scansione centrale in cloud pubblico o privato**, con una piccola impronta che richiede un Security Server per la scansione. In questo caso, nessun contenuto di sicurezza viene memorizzato localmente e la scansione viene scaricata sul Security Server.

   Nota
   C'è un minimo set di motori che viene memorizzato localmente, necessario per scompattare i file compressi.

4. **Scansione centrale (scansione tramite cloud pubblico o privato con Security Server) con riserva* nella scansione locale (motori completi)**
5. **Scansione centrale (scansione tramite cloud pubblico o privato con Security Server) con riserva* nella scansione ibrida (cloud pubblico con motori leggeri)**

* Quando si usa un doppio motore di scansione, se il primo motore non è disponibile, sarà utilizzato quello di riserva. Il consumo di risorse e l'utilizzo della rete dipenderanno dai motori utilizzati.

2.2. Advanced Threat Control

Per le minacce in grado di eludere persino il motore euristico, c'è un altro livello di protezione costituito da Advanced Threat Control (ATC).

Advanced Threat Control monitora costantemente i processi in esecuzione e classifica i comportamenti sospetti come un tentativo di: mascherare il tipo di processo, eseguire il codice nello spazio di un altro processo (disattivando la memoria del processo per l'escalation dei privilegi), replicare, rilasciare file, nascondere applicazioni dall'enumerazione dei processi, ecc. Ogni comportamento sospetto aumenta la valutazione del processo. Quando viene raggiunta una determinata soglia, viene attivato un allarme.

2.3. HyperDetect

Bitdefender HyperDetect è un livello di sicurezza aggiuntivo appositamente progettato per rilevare attacchi avanzati e attività sospette in fase di pre-esecuzione. HyperDetect contiene modelli di apprendimento automatico e tecnologie di rilevamento di attacchi furtivi contro minacce come attacchi zero-day, minacce persistenti avanzate (APT), malware oscurati, attacchi privi di file (uso improprio di PowerShell, Windows Management Instrumentation, ecc.), furto di credenziali, attacchi mirati, malware personalizzati, attacchi basati su script, exploit, strumenti di hacking, traffico di rete sospetto, applicazioni potenzialmente indesiderate (PUA) e ransomware.

Nota
Questo modulo è un add-on disponibile con un codice di licenza separato.

2.4. Anti-exploit avanzato

Dotato di apprendimento automatico, l'Anti-Exploit avanzato è una nuova tecnologia proattiva che blocca gli attacchi zero-day portati da exploit evasivi. L'Anti-exploit avanzato rileva gli exploit più recenti in tempo reale e attenua le vulnerabilità in grado di danneggiare la memoria, che potrebbero altre soluzioni di sicurezza. Protegge le applicazioni più comunemente utilizzate, come i browser, Microsoft Office o Adobe Reader, e non solo. Monitora i processi del sistema e protegge da violazioni di sicurezza e dall'hijack dei processi esistenti.

2.5. Firewall

Il Firewall controlla l'accesso delle applicazioni alla rete e a Internet. L'accesso viene consentito automaticamente per un vasto database di applicazioni note e legittime. Inoltre, il firewall può proteggere il sistema da port scan, limitare ICS e avvisare quando nuovi nodi si uniscono a una connessione Wi-Fi.

2.6. Controllo contenuti

Il modulo Controllo contenuti ti aiuta a rafforzare le politiche aziendali relative a traffico consentito, accesso web, protezione dati e controllo applicazioni. Gli amministratori possono definire le opzioni e le eccezioni di scansione del traffico, programmare l'accesso al web bloccando o consentendo eventuali URL o categorie web, configurare le regole della protezione dati e definire le autorizzazioni per l'uso di determinate applicazioni.

2.7. Network Attack Defense

Il modulo Network Attack Defense si affida a una tecnologia di Bitdefender focalizzata sul rilevamento di attacchi di rete progettati per ottenere accesso agli endpoint attraverso tecniche specifiche, come attacchi di forza bruta, exploit di rete, furti di password, vettori di infezione drive-by-download, bot e Trojan.

2.8. Patch Management

Pienamente integrato in GravityZone, Gestione patch mantiene i sistemi operativi e le applicazioni software sempre aggiornati, fornendo una visione completa sullo stato delle patch per i tuoi endpoint Windows gestiti.

Il modulo Gestione patch di GravityZone include diverse funzionalità, come scansione patch a richiesta / programmata, applicazione di patch automatica / manuale o segnalazione di patch mancanti.

Puoi anche trovare maggiori informazioni su fornitori e prodotti supportati da Gestione patch di GravityZone in questo articolo della KB.

Nota
Gestione patch è un add-on disponibile con un codice di licenza separato per tutti i pacchetti GravityZone disponibili.

2.9. Controllo dispositivi

Il modulo Controllo dispositivi consente di prevenire la sottrazione di dati sensibili e le infezioni di malware tramite dispositivi esterni collegati agli endpoint, applicando regole ed eccezioni di blocco tramite una policy a una vasta gamma di tipi di dispositivi (come unità flash USB, dispositivi Bluetooth, lettori CD/DVD, dispositivi di archiviazione, ecc.).

2.10. Full Disk Encryption

Questo livello di protezione ti consente di fornire una cifratura completa del disco sugli endpoint, gestendo BitLocker su Windows e FileVault e diskutil su macOS. È possibile cifrare e decifrare i volumi di avvio con pochi clic, mentre GravityZone gestisce l'intero processo con un intervento minimo da parte degli utenti. Inoltre, GravityZone memorizza i codici di ripristino necessari per sbloccare i volumi quando gli utenti dimenticano le proprie password.

Nota
Full Disk Encryption è un add-on disponibile con un codice di licenza separato per tutti i pacchetti GravityZone disponibili.

2.11. Security for Exchange

Bitdefender Security for Exchange offre funzioni antimalware, antispam, antiphishing e di filtraggio contenuti e allegati, integrate perfettamente con Microsoft Exchange Server per assicurare un ambiente di messaggistica e collaborazione protetto e aumentare la produttività. Utilizzando tecnologie antimalware e antispam pluripremiate, protegge gli utenti di Exchange dai malware più recenti e sofisticati, e da ogni tentativo di sottrarre dati sensibili e preziosi degli utenti.

Importante
Security for Exchange è stato progettato per proteggere l'intera organizzazione di Exchange a cui appartiene il server Exchange protetto. Ciò significa che protegge tutte le caselle di posta attive, incluso le caselle di posta di utente/stanza/equipaggiamento/condivise.

Nota
Questo modulo è un add-on disponibile con un codice di licenza separato.

2.12. Sandbox Analyzer

Bitdefender Sandbox Analyzer fornisce un potente livello di protezione dalle minacce avanzate, eseguendo un'analisi automatica e approfondita dei file sospetti non ancora firmati dai motori antimalware di Bitdefender. Il sandbox utilizza una vasta gamma di tecnologie Bitdefender per eseguire i payload in un ambiente virtuale contenuto, ospitato da Bitdefender, analizzare il loro comportamento e segnalare anche il minimo cambiamento del sistema, in genere un chiaro segnale di intenzioni dannose.

Sandbox Analyzer invia automaticamente i file sospetti presenti sugli endpoint gestiti, ma comunque nascosti ai servizi antimalware basati sulle firme. L'euristica dedicata inclusa nel modulo antimalware all'accesso di Bitdefender Endpoint Security Tools innesca il processo di invio.

Il servizio Sandbox Analyzer è in grado di impedire l'esecuzione di minacce sconosciute nell'endpoint. Funziona in modalità monitoraggio o blocco, consentendo o negando l'accesso al file sospetto fino al ricevimento di un verdetto. Sandbox Analyzer consente di risolvere automaticamente le minacce scoperte in base alle azioni di risanamento definite nella policy di sicurezza dei sistemi interessati.

Inoltre, Sandbox Analyzer ti consente di inviare manualmente eventuali campioni direttamente da Control Center, permettendoti di decidere che cosa farne.

Importante
L'invio manuale è disponibile per gli utenti di GravityZone con diritto di **Gestione delle reti**.

Nota
Questo modulo è un add-on disponibile con un codice di licenza separato.

2.13. Endpoint Detection and Response (EDR)

Endpoint Detection and Response è un componente di correlazione degli eventi, in grado di identificare minacce avanzate o attacchi in corso. Come parte della nostra Endpoint Protection Platform completa e integrata, EDR riunisce le informazioni sul dispositivo in tutta la rete aziendale. Questa soluzione contribuisce a supportare lo sforzo dei team di risposta degli incidenti per indagare e rispondere a minacce avanzate.

Tramite Bitdefender Endpoint Security Tools, puoi attivare un modulo di protezione chiamato Sensore EDR sui tuoi endpoint gestiti, per raccogliere i dati sull'hardware

e i sistemi operativi. Seguendo un framework client-server, i metadati vengono ottenuti ed elaborati in entrambi i lati.

Questo componente fornisce informazioni dettagliate sugli incidenti rilevati, una mappa dell'incidente interattiva, azioni di risanamento e integrazione con Sandbox Analyzer e HyperDetect.

Nota
Questo modulo è un add-on disponibile con un codice di licenza separato.

2.14. Endpoint Risk Analytics (ERA)

Endpoint Risk Analytics (ERA) identifica, valuta e corregge le vulnerabilità degli endpoint attraverso scansioni dei rischi (a richiesta o programmate), prendendo in considerazione un gran numero di indicatori di rischio. Dopo aver scansionato la tua rete con determinati indicatori di rischio, avrai accesso a una panoramica dello stato di rischio della rete tramite la dashboard di **Gestione rischi**, disponibile dal menu principale. Potrai risolvere alcuni rischi di sicurezza automaticamente da GravityZone Control Center e visualizzare suggerimenti per la mitigazione dell'esposizione degli endpoint.

2.15. Email Security

Tramite Email Security puoi controllare la consegna delle e-mail, filtrare i messaggi e applicare policy a livello aziendale, per bloccare minacce mirate e sofisticate per le e-mail, tra cui Business Email Compromise (BEC) e frodi del CEO.Email Security richiede la fornitura di un account per accedere alla console. Per maggiori informazioni, fai riferimento alla Guida per l'utente di Bitdefender Email Security.

2.16. Disponibilità dei livelli di protezione di GravityZone

La disponibilità dei livelli di protezione di GravityZone varia a seconda del sistema operativo dell'endpoint. Per maggiori informazioni, fai riferimento all'articolo della KB disponibilità dei livelli di protezione di GravityZone.

3. ARCHITETTURA DI GRAVITYZONE

La soluzione di GravityZone include i seguenti componenti:

- Console web (Control Center)
- Security Server
- Agenti di sicurezza

3.1. Console web (GravityZone Control Center)

Control Center, un'interfaccia basata sul web, si integra con i sistemi di gestione e monitoraggio esistenti per semplificare l'applicazione della protezione a workstation e server non gestiti.

3.2. Security Server

Il Security Server è una macchina virtuale dedicata che deduplica e centralizza la maggior parte delle funzionalità antimalware dei relativi agenti, comportandosi come un server di scansione.

Nota
La licenza del tuo prodotto potrebbe non includere questa funzionalità.

Il Security Server deve essere installato su uno o più host in modo da accogliere il numero di macchine virtuali protette.

3.3. Agenti di sicurezza

Per proteggere la tua rete con Bitdefender, devi installare gli appropriati agenti di sicurezza di GravityZone sugli endpoint della rete.

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac

3.3.1. Bitdefender Endpoint Security Tools

GravityZone assicura la protezione di macchine Windows e Linux fisiche e virtuali con Bitdefender Endpoint Security Tools, un agente di sicurezza intelligente e consapevole, che si adatta al tipo di endpoint. Bitdefender Endpoint Security Tools può essere impiegato su qualsiasi macchina, virtuale o fisica, fornendo un sistema

di scansione flessibile e diventando una scelta ideale per ambienti misti (fisici, virtuali e cloud).

Oltre a proteggere il file system, Bitdefender Endpoint Security Tools include anche una protezione del server mail per Microsoft Exchange Server.

Bitdefender Endpoint Security Tools utilizza un unico modello di policy per macchine fisiche e virtuali e una fonte per i kit di installazione per qualsiasi ambiente (fisico o virtuale) con Windows.

Livelli di protezione

Con Bitdefender Endpoint Security Tools sono disponibili i seguenti livelli di protezione:

- Antimalware
- Advanced Threat Control
- HyperDetect
- Firewall
- Controllo contenuti
- Network Attack Defense
- Patch Management
- Controllo dispositivi
- Full Disk Encryption
- Security for Exchange
- Sandbox Analyzer
- Endpoint Detection and Response (EDR)
- Endpoint Risk Analytics (ERA)

Ruoli degli endpoint

- Utente esperto
- Relay
- Server caching patch
- Exchange Protection

Utente esperto

Gli amministratori del Control Center possono garantire diritti di Utente esperto agli utenti degli endpoint tramite le impostazioni della policy. Il modulo Utente esperto consente di garantire diritti di amministrazione a livello di utente, permettendo all'utente dell'endpoint di accedere e modificare le impostazioni di

sicurezza tramite una console in locale. Control Center riceve una notifica ogni volta che un endpoint passa in modalità Utente esperto e l'amministratore di Control Center può sempre sovrascrivere le impostazioni di sicurezza locali.

Importante
Questo modulo è disponibile solo per i sistemi operativi Windows desktop e server supportati. Per maggiori informazioni, fai riferimento alla Guida di installazione di GravityZone.

Relay

Gli agenti endpoint con ruolo Bitdefender Endpoint Security Tools Relay agiscono da proxy di comunicazione e server di aggiornamento per gli altri endpoint nella rete. Gli agenti endpoint con ruolo di relay sono particolarmente richiesti in organizzazioni con reti isolate, in cui tutto il traffico passa da un singolo punto di accesso.

In aziende con grandi reti distribuite, gli agenti relay aiutano a ridurre il consumo di banda, prevenendo agli endpoint protetti e ai server di sicurezza di connettersi direttamente alla appliance di GravityZone.

Una volta che un agente Bitdefender Endpoint Security Tools Relay viene installato nella rete, altri endpoint possono essere configurati tramite la policy per comunicare con Control Center tramite l'agente relay.

Gli agenti Bitdefender Endpoint Security Tools Relay servono per i seguenti scopi:

- Scoprire tutti gli endpoint non protetti nella rete.

  Questa funzionalità è essenziale per l'impiego dell'agente di sicurezza in un ambiente cloud di GravityZone.
- Impiegare l'agente dell'endpoint nella rete locale.
- Aggiornare gli endpoint protetti nella rete.
- Assicurare la comunicazione tra Control Center e gli endpoint connessi.
- Agire come server proxy per gli endpoint protetti.
- Ottimizzare il traffico di rete durante gli aggiornamenti, gli impieghi, la scansione e le altre attività che richiedono risorse.

Server caching patch

Gli endpoint con ruolo Relay possono agire anche come Server di cache patch. Con questa regola attivata, i Relay servono per memorizzare le patch software scaricate dai siti web del fornitore e distribuirle agli endpoint di destinazione nella propria rete. Ogni volta che un endpoint connesso ha software mancante di patch,

le scarica dal server e non dal sito web del fornitore, ottimizzando così il traffico generato e il carico sulla banda della rete.

Importante
Questo ruolo aggiuntivo è disponibile con un add-on di Gestione patch registrato.

Exchange Protection

Bitdefender Endpoint Security Tools con ruolo Exchange può essere installato su Microsoft Exchange Server allo scopo di proteggere gli utenti di Exchange da minacce derivanti da e-mail.

Bitdefender Endpoint Security Tools con ruolo di Exchange protegge sia la macchina server che la soluzione Microsoft Exchange.

3.3.2. Endpoint Security for Mac

Endpoint Security for Mac è un agente di sicurezza progettato per proteggere workstation e portatili Macintosh basati su Intel. La tecnologia di scansione disponibile è la **Scansione locale**, con il contenuto di sicurezza memorizzato a livello locale.

Livelli di protezione

Con Endpoint Security for Mac sono disponibili i seguenti livelli di protezione:

- Antimalware
- Advanced Threat Control
- Controllo contenuti
- Controllo dispositivi
- Full Disk Encryption

3.4. Architettura di Sandbox Analyzer

Bitdefender Sandbox Analyzer fornisce un potente livello di protezione dalle minacce avanzate, eseguendo un'analisi automatica e approfondita dei file sospetti non ancora firmati dai motori antimalware di Bitdefender.

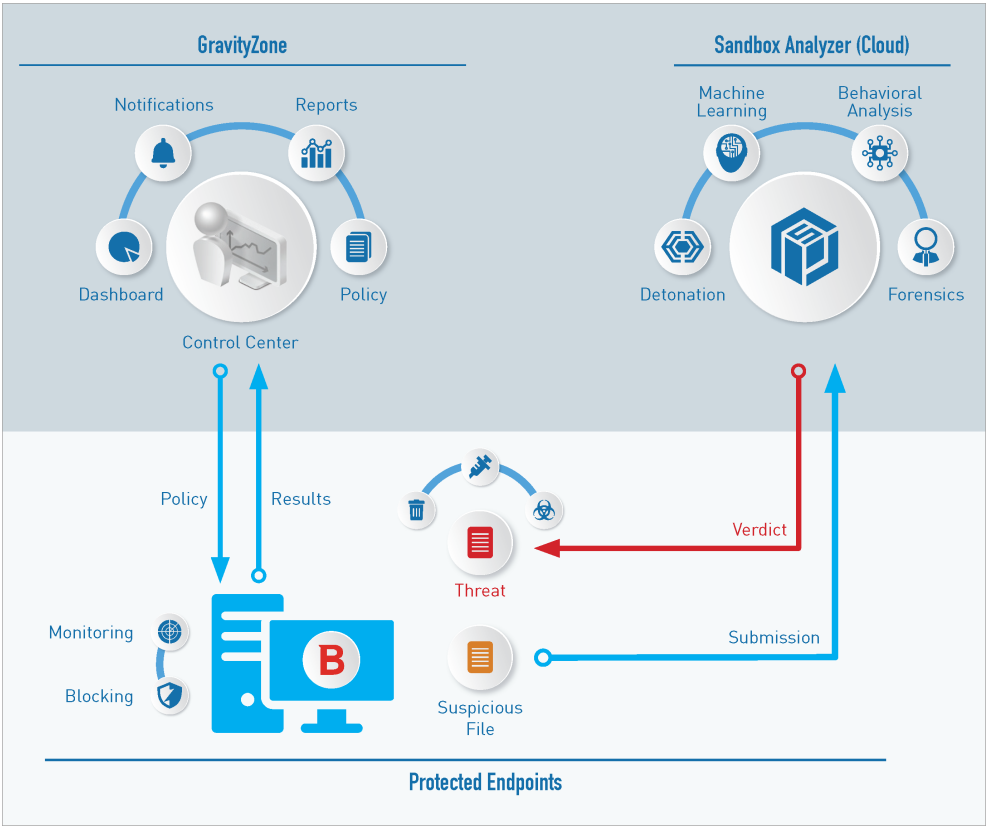
Sandbox Analyzer include i seguenti componenti:

- **Portale di Sandbox Analyzer**. Questo componente è un server di comunicazione usato per la gestione delle richieste tra gli endpoint e il cluster di Bitdefender Sandbox.

- **Cluster di Sandbox Analyzer**. Questo componente è l'infrastruttura sandbox ospitata, in cui si verifica l'analisi comportamentale dei campioni. A questo livello, i file inviati vengono attivati su virtual machine con Windows 7.

GravityZone Control Center funziona come una console di gestione e reportistica, dove puoi configurare le policy di sicurezza, oltre a visualizzare notifiche e rapporti di analisi.

Bitdefender Endpoint Security Tools, l'agente di sicurezza installato sugli endpoint, che agisce come sensore di feeding per Sandbox Analyzer.



Architettura di Sandbox Analyzer

Una volta che il servizio Sandbox Analyzer è stato attivato da Control Center sugli endpoint:

1. L'agente di sicurezza di Bitdefender inizia a inviare i file sospetti che corrispondono alle regole di protezione impostate nella policy.
2. Una volta analizzati i file, viene inviata una risposta al Portale e all'endpoint.
3. Se un file viene rilevato come pericoloso, l'utente viene avvisato e viene intrapresa un'azione di rimedio.

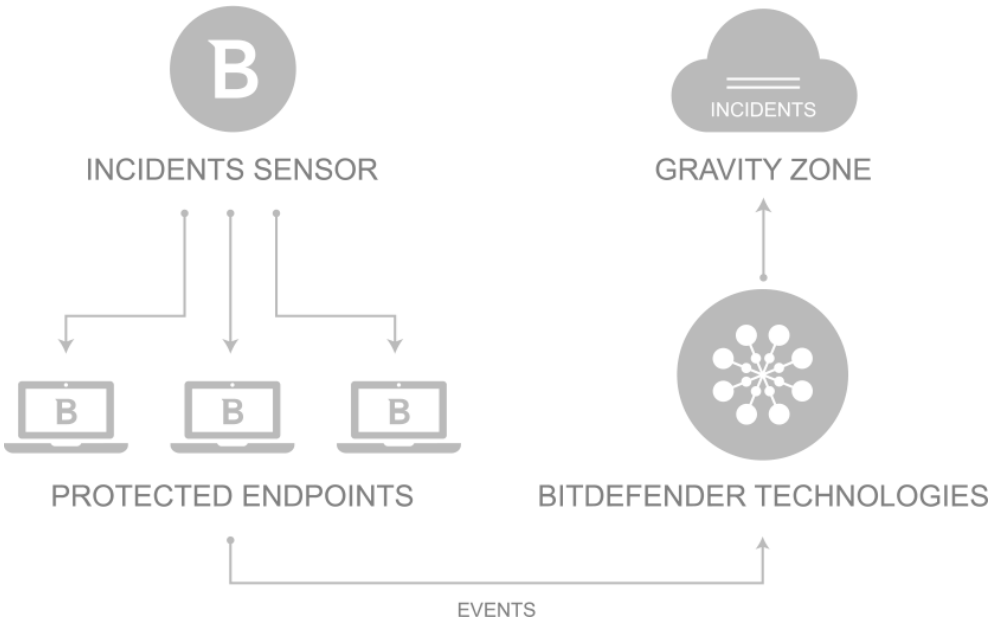
I risultati delle analisi sono conservati tramite un valore di hash del file nel database di Sandbox Analyzer. Quando un file analizzato in precedenza viene inviato da un altro endpoint, si ottiene una risposta immediata, perché i risultati sono già disponibili nel database.

3.5. Architettura EDR

Per identificare le minacce avanzate e gli attacchi in corso, l'EDR richiede dati dell'hardware e del sistema operativo. Alcuni dei dati grezzi vengono elaborati a livello locale, mentre gli algoritmi di apprendimento automatico in Security Analytics, eseguendo attività più complesse.

L'EDR include due componenti principali:

- Il Sensore incidenti, che raccoglie i dati dei processi, e segnala i dati comportamentali di endpoint e applicazioni.
- Security Analytics, una componente back-end della suite di tecnologie di Bitdefender utilizzata per interpretare i metadati raccolti dal Sensore incidenti.



Flusso dell'EDR dall'endpoint al Control Center

4. COME INIZIARE

Le funzionalità di GravityZone possono essere configurate e gestite tramite una piattaforma di gestione centralizzata chiamata Control Center. Control Center ha un'interfaccia web a cui è possibile accedere tramite nome utente e password.

4.1. Connessione a Control Center

L'accesso a Control Center viene eseguito tramite account utente. Riceverai le tue credenziali di accesso via e-mail, una volta creato il tuo account.

Prerequisiti:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Risoluzione dello schermo consigliata: 1280x800 o superiore

Avvertimento
Control Center non funzionerà / apparirà correttamente in Internet Explorer 9+ con la funzione Visualizzazione compatibilità attivata, che equivale a utilizzare una versione del browser non supportata.

Per connetterti a Control Center:

1. Apri il tuo browser web.
2. Vai al seguente indirizzo: https://gravityzone.bitdefender.com
3. Se usi le **credenziali di GravityZone**:
   a. Inserisci l'indirizzo e-mail del tuo account e clicca su **Avanti**.
   b. Inserisci la password del tuo account e clicca su **Avanti**.
   c. Inserisci il codice di sei cifre della app di autenticazione come parte dell'autenticazione a due fattori.
   d. Clicca su **Continua** per accedere.

   Se usi l'**autenticazione singola**:
   a. Quando accedi la prima volta, inserisci l'indirizzo e-mail del tuo account e clicca su **Avanti**.

      GravityZone ti reindirizzerà alla pagina di autenticazione del tuo fornitore di identità.

b. Autenticati con il fornitore di identità.

c. Il fornitore di identità ti reindirizzerà nuovamente a GravityZone e accederai automaticamente alla Control Center.

   La prossima volta, accederai alla Control Center solo con il tuo indirizzo e-mail.

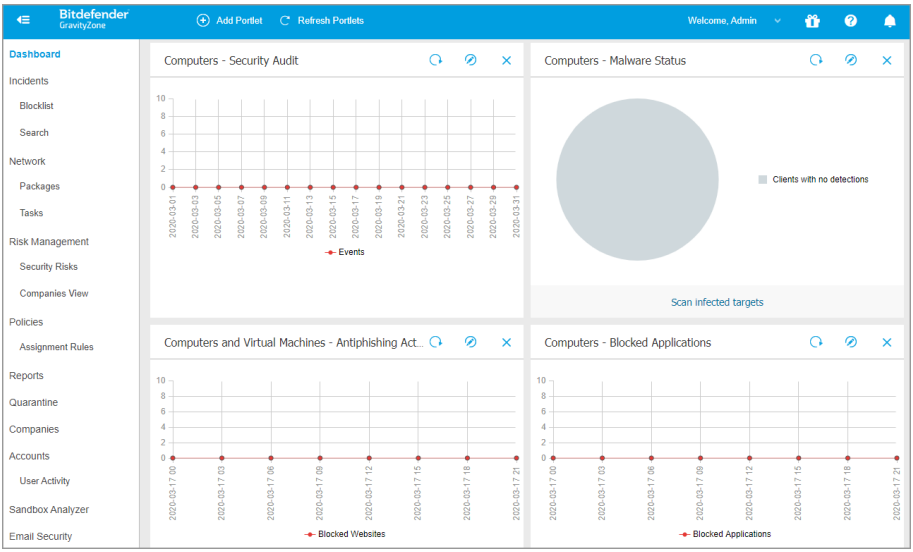
Al primo accesso, devi accettare le Condizioni d'uso di Bitdefender. Clicca su **Continua** per iniziare a usare GravityZone.

Nota

- Se hai dimenticato la tua password, usa il link di recupero della password per riceverne una nuova. Devi inserire l'indirizzo e-mail del tuo account.
- Se il tuo account usa l'autenticazione singola, ma GravityZone ti chiede una password, contatta il tuo amministratore per ricevere assistenza. Nel frattempo, accedi con la password precedente o usa il link di recupero della password per riceverne una nuova.

4.2. Control Center a prima vista

Control Center consente un accesso immediato a tutte le funzionalità. Usa la barra del menu sul lato destro per muoverti nella console. Le funzionalità disponibili dipendono dal tipo di utente che accede alla console.



L'interfaccia

4.2.1. Panoramica della Control Center

Usa il pulsante **Visualizza menu** nell'angolo in alto a sinistra per comprimere l'icona e nascondere o espandere le opzioni del menu. Clicca sul pulsante per scorrere le opzioni o clicca due volte per saltare.

In base al tuo ruolo, puoi accedere alle seguenti opzioni del menu:

Dashboard
Visualizza grafici di facile lettura che forniscono informazioni chiave sulla sicurezza della tua rete.

Incidenti
Vedi e gestisci gli incidenti di sicurezza nella rete aziendale.

Rete
Installa la protezione, applica le policy per gestire le impostazioni, esegui attività in remoto e crea rapporti veloci.

Politiche
Crea e gestisci le policy di sicurezza.

Rapporti
Ottieni rapporti di sicurezza relativi alle aziende e ai computer gestiti.

Quarantena
Gestisci in remoto i file in quarantena.

Account
Crea e gestisci gli account utente per le tue aziende partner e clienti a cui fornisci i servizi.

In questo menu, puoi anche trovare la pagina **Attività utente**, che consente di accedere a un registro delle attività dell'utente.

Nell'angolo in basso a sinistra della Control Center, la sezione **Strumenti** ti consente di utilizzare altre risorse di GravityZone, come l'invio manuale dei file a Sandbox Analyzer.

Cliccando sul tuo nome utente nell'angolo in alto a destra della console, sono disponibili le seguenti opzioni:

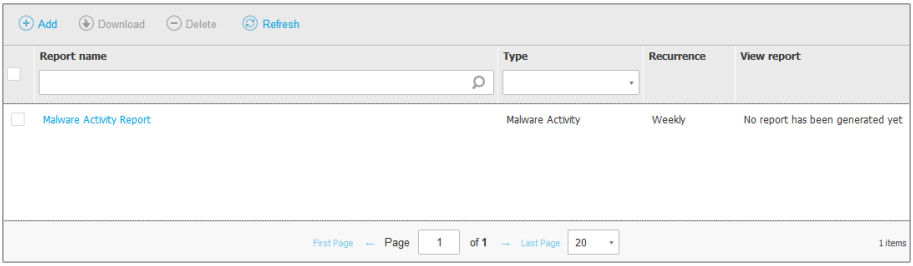
- **Il mio Account**. Clicca su questa opzione per gestire i dettagli e le preferenze del tuo account utente.
- **La mia azienda**. Clicca su questa opzione per gestire i dettagli e le preferenze della tua azienda.
- **Integrazioni**. Clicca su questa opzione per gestire l'integrazione di GravityZone con altre piattaforme di gestione.
- **Credentials Manager**. Clicca su questa opzione per aggiungere e gestire le credenziali di autenticazione richieste per le attività di installazione in remoto.
- **Aiuto e Supporto**. Clicca su questa opzione per trovare informazioni di aiuto e supporto.
- **Feedback**. Clicca su questa opzione per mostrare un modulo che ti consente di modificare e inviare eventuali messaggi di feedback relativi alla tua esperienza con GravityZone.
- **Uscita**. Clicca su questa opzione per uscire dal tuo account.

Inoltre, nell'angolo in alto a destra della console, puoi trovare:

- L'icona della **modalità Aiuto**, che consente di espandere alcune caselle di aiuto posizionate nei vari elementi della Control Center. Puoi trovare facilmente molte informazioni utili relative alle caratteristiche della Control Center.
- L'icona **Notifiche**, che fornisce un accesso rapido ai messaggi di notifica e anche alla pagina **Notifiche**.

4.2.2. Tabella dati

Le tabelle vengono usate spesso nella console per organizzare i dati in un formato facilmente utilizzabile.



La pagina dei rapporti

Muoversi tra le pagine

Le tabelle con più di 20 voci sono suddivise in più pagine. Normalmente, vengono visualizzate solo 20 voci per pagina. Per muoversi tra le pagine, usa i pulsanti di navigazione nella parte inferiore della tabella. Puoi cambiare il numero di valori mostrati in una pagina selezionando un'altra opzione nel menu accanto ai pulsanti di navigazione.

Cercare determinate voci

Per trovare facilmente determinate voci, usa le caselle di ricerca disponibili sotto le intestazioni della colonna.

Inserire il termine da cercare nel campo corrispondente. Gli elementi che corrispondono vengono mostrati nella tabella mentre digiti. Per azzerare i contenuti di una tabella, libera i campi di ricerca.

Ordinare i dati

Per ordinare i dati di una determinata colonna, clicca sulla sua intestazione. Clicca nuovamente sull'intestazione della colonna per invertire l'ordine selezionato.

Aggiornare i dati della tabella

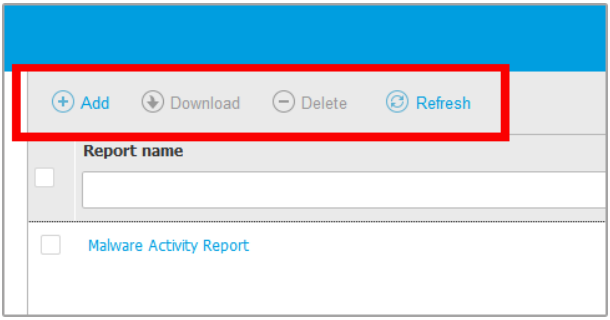
Per assicurarsi che la console mostri i dati più aggiornati, clicca sul pulsante **Aggiorna** nel lato superiore della tabella.

Potrebbe essere necessario se si trascorre molto tempo nella pagina.

4.2.3. Barre degli strumenti

In Control Center, le barre degli strumenti ti consentono di eseguire determinate operazioni inerenti alla sezione in cui ti trovi. Ogni barra degli strumenti consiste in un set di icone che in genere vengono posizionate nel lato superiore della tabella. Per esempio, la barra degli strumenti nella sezione **Rapporti**, ti consente di eseguire le seguenti azioni:

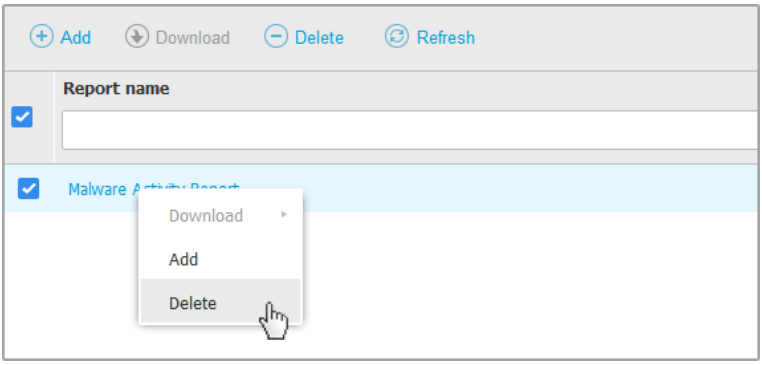
- Crea un nuovo rapporto.
- Scarica un rapporto programmato.
- Elimina un rapporto programmato.



La pagina Rapporti - Barra degli strumenti

4.2.4. Menu contestuale

I comandi della barra degli strumenti sono anche accessibili dal menu contestuale. Clicca con il pulsante destro sulla sezione Control Center che stai utilizzando attualmente e seleziona il comando che ti serve dall'elenco disponibile.

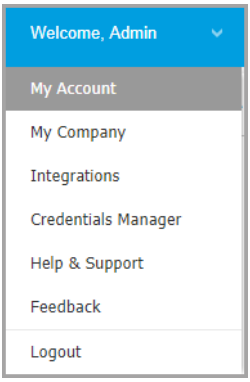


La pagina dei Rapporti - Menu contestuale

4.3. Gestire il tuo account

Per verificare o cambiare le informazioni e le impostazioni dell'account:

1. Clicca sul tuo nome utente nell'angolo in alto a destra della console e seleziona **Il mio account**.



Il menu Account utente

2. In **Dettagli account**, correggi o aggiorna i dettagli del tuo account.
   - **Nome completo.** Inserisci il tuo nome completo.
   - **E-mail.** Questo è il tuo indirizzo e-mail di accesso e contatto. A questo indirizzo vengono inviati i rapporti e le notifiche inerenti la sicurezza. Le

e-mail di notifica vengono inviate automaticamente ogni volta che nella rete vengono rilevate importanti condizioni di rischio.
- Un link **Modifica password** ti consente di modificare la tua password di accesso.

3. In **Impostazioni**, configura le impostazioni dell'account in base alle tue preferenze.
   - **Fuso orario.** Seleziona il fuso orario del tuo account dal menu. La console mostrerà le informazioni orarie in base al fuso orario selezionato.
   - **Lingua.** Seleziona la lingua utilizzata dalla console nel menu.
   - **Scadenza sessione.** Seleziona l'intervallo di tempo di inattività prima della scadenza della sessione dell'utente.
4. In **Sicurezza accesso**, configura l'autenticazione a due fattori e verifica lo stato delle policy disponibili per proteggere il tuo account di GravityZone. Le policy stabilite a livello aziendale sono di sola lettura.

   Per attivare l'autenticazione a due fattori:

   a. **Autenticazione a due fattori.** L'autenticazione a due fattori aggiunge un ulteriore livello di sicurezza al tuo account GravityZone, richiedendo un codice di autenticazione oltre alle tue credenziali di Control Center.

      Quando accedi per la prima volta al tuo account di GravityZone ti sarà chiesto di scaricare e installare Google Authenticator, Microsoft Authenticator o un altro autenticatore a due fattori compatibile TOTP (Time-Based One-Time Password Algorithm) con lo standard RFC6238 su un dispositivo mobile, collegarlo al tuo account di GravityZone e utilizzarlo in ogni accesso a Control Center. Google Authenticator genera un codice di sei cifre ogni 30 secondi. Per completare l'accesso a Control Center, dopo aver inserito la password, dovrai fornire il codice di sei cifre di Google Authenticator.

      Nota
      Puoi saltare tale processo per tre volte, dopo le quali non potrai più accedere senza l'autenticazione a due fattori.

      Per attivare l'autenticazione a due fattori:

      i. Clicca sul pulsante **Attiva** sotto il messaggio dell'**autenticazione a due fattori**.

      ii. Nella finestra di dialogo, clicca sul link appropriato per scaricare e installare Google Authenticator sul tuo dispositivo mobile.

iii. Sul tuo dispositivo mobile, apri Google Authenticator.

iv. Nella schermata **Aggiungi un account**, esamina il codice QR per collegare la tua app al tuo account di GravityZone.

Puoi anche inserire il codice segreto manualmente.

Questa azione è necessaria una sola volta, per attivare la funzionalità in GravityZone.

Importante
Assicurati di copiare e salvare il codice segreto in un posto sicuro. Clicca su **Stampa una copia di backup** per creare un file PDF con il codice QR e il codice segreto. Se il dispositivo mobile usato per attivare l'autenticazione a due fattori viene perso o sostituito, dovrai installare Google Authenticator su un nuovo dispositivo e inserire il codice segreto per collegarlo al tuo account GravityZone.

v. Inserisci il codice di sei cifre nel campo **codice di Google Authenticator**.

vi. Clicca su **Attiva** per completare l'attivazione della funzionalità.

Nota
Il tuo amministratore aziendale può rendere obbligatoria l'autenticazione a due fattori per tutti gli account di GravityZone. In questo caso, all'accesso ti sarà chiesto di configurare la tua 2FA. Allo stesso tempo, non potrai disattivare la 2FA per il tuo account, finché questa funzionalità viene applicata dal tuo amministratore aziendale.
Tieni presente che, se la 2FA attualmente configurata viene disattivata per il tuo account, il codice segreto non sarà più valido.

b. **Policy di scadenza della password**. Modificare regolarmente la tua password fornisce un ulteriore livello di protezione dall'uso non autorizzato delle password o ne limita la durata dell'uso non autorizzato. Quando attivata, GravityZone richiede di cambiare la password al massimo ogni 90 giorni.

c. **Policy di blocco dell'account**. Questa policy previene l'accesso al tuo account dopo cinque tentativi di accesso falliti consecutivi. Questa misura serve per proteggersi dagli attacchi di forza bruta.

Per sbloccare il tuo account, devi resettare la tua password dalla pagina di accesso o contattare un altro amministratore di GravityZone.

5. Clicca su **Salva** per applicare le modifiche.

Nota
Non puoi eliminare il tuo account personale.

4.4. Modificare la password di accesso

Una volta creato il tuo account, riceverai un'e-mail con le credenziali di accesso.

Si consigliare di eseguire le seguenti operazioni:

- Modifica la password di accesso predefinita la prima volta che visiti Control Center.
- Modifica regolarmente la tua password di accesso.

Per modificare la password di accesso:

1. Clicca sul tuo nome utente nell'angolo in alto a destra della console e seleziona **Il mio account**.
2. In **Dettagli account**, clicca su **Modifica password**.
3. Inserisci la tua password ideale e la nuova password nei campi corrispondenti.
4. Clicca su **Salva** per applicare le modifiche.

4.5. Gestire la tua azienda

Come utente con il diritto di **Gestione azienda**, puoi controllare o modificare le informazioni e le impostazioni della licenza aziendali, oltre a gestire le impostazioni di autenticazione, come l'autenticazione singola e quella a due fattori.

4.5.1. Dettagli e impostazioni della licenza

Per verificare o modificare le informazioni dell'azienda e le impostazioni della licenza:

1. Clicca sul tuo nome utente nell'angolo in alto a destra della console e seleziona **La mia azienda**.
2. In **Dettagli azienda**, inserisci le tue informazioni aziendali, come nome dell'azienda, indirizzo e telefono.

   Puoi modificare il logo mostrato nella Control Center e anche nei rapporti e nelle notifiche e-mail dell'azienda, come segue:

   - Clicca su **Cambia** per cercare l'immagine da usare come logo sul tuo computer. L'immagine dev'essere in formato .png o .jpg, mentre la dimensione deve essere di 200x30 pixel.

- Clicca su **Predefinita** per eliminare l'immagine e passare all'immagine fornita da Bitdefender.

3. Di norma, la tua azienda può essere gestita da account partner di altre aziende che possono avere la tua azienda indicata nella loro Bitdefender Control Center. Puoi bloccare l'accesso di queste aziende alla tua rete disattivando l'opzione **Consenti al tuo partner di assisterti con la gestione della sicurezza di questa azienda**. Di conseguenza, la tua rete non sarà visibile nella Control Center delle altre aziende, ma potranno gestire il tuo abbonamento.
4. Nella sezione **Licenza**, puoi visualizzare e modificare i dettagli della tua licenza e puoi anche inserire un codice di un add-on.
   - Per aggiungere un nuovo codice di licenza:
     a. Dal **menu Tipo**, seleziona un tipo di **Licenza** in abbonamento.
     b. Inserisci il codice nel campo **Codice di licenza**.
     c. Clicca sul pulsante **Controlla** e attendi che la Control Center recuperi le informazioni sul codice di licenza inserito.
   - Per maggiori dettagli sul tuo codice di licenza, consulta le informazioni indicate sotto il codice di licenza:
     – **Data di scadenza**: la data fino a quando è possibile utilizzare il codice di licenza.
     – **Utilizzati**: il numero di posti utilizzati sull'ammontare totale incluse nel codice di licenza. Un posto della licenza viene usato quando il client di Bitdefender viene installato su un endpoint della rete che gestisci.
     – **Totale**: il numero totale di posti disponibili nel tuo codice di licenza o abbonamento.

     Inoltre, se usi un abbonamento mensile, puoi generare il rapporto **Utilizzo licenza mensile** per il mese attuale. Per maggiori informazioni, fai riferimento a **Utilizzo licenza mensile** .
   - Per inserire un codice add-on:
     – Inserisci il codice nel campo **Codice add-on**.
     – Clicca sul pulsante **Aggiungi** e attendi che GravityZone controlli il codice add-on. Se valido, la Control Center recupera le seguenti informazioni sull'add-on: il tipo, il codice e l'opzione per rimuoverlo.

Nota
Il campo **Codice add-on** non compare se hai una licenza mensile o di prova.

5. In **Bitdefender Partner**, puoi trovare informazioni sulla tua azienda di fornitura di servizi.

   Per modificare il tuo fornitore del servizio gestito:

   a. Clicca sul pulsante **Modifica**.

   b. Inserisci il codice ID dell'azienda nel campo **ID partner**.

   Nota
   Ogni azienda può trovare il suo ID nella pagina **La mia azienda**. Una volta siglato un accordo con un'azienda partner, il suo rappresentante deve fornirti l'ID del suo Control Center.

   c. Clicca su **Salva**.

   Di conseguenza, la tua azienda viene spostata automaticamente dalla Control Center del partner precedente a quella del nuovo partner.

6. In alternativa, puoi collegare la tua azienda con il tuo account MyBitdefender utilizzando i campi disponibili.
7. Clicca su **Salva** per applicare le modifiche.

4.5.2. Impostazioni autenticazione

GravityZone offre alcune opzioni aggiuntive per proteggere l'autenticazione dell'utente al Control Center, come:

- Autenticazione a due fattori
- Scadenza password
- Blocco account
- Autenticazione singola

Come amministratore dell'azienda, puoi facilmente attivare queste misure di sicurezza di accesso aggiuntive per la tua intera azienda:

1. Vai alla pagina **Configurazione > Impostazioni autenticazione**.
2. Seleziona o configura le opzioni che hai bisogno di attivare.

Scopri maggiori dettagli su ogni opzione nelle seguenti sezioni.

3. Clicca su **Salva** per applicarle.

Applica autenticazione a due fattori

L'autenticazione a due fattori (2FA) certifica che la persona che prova ad accedere a Control Center sia l'utente previsto. La 2FA richiede un codice di autenticazione oltre alle credenziali di Control Center a ogni accesso. GravityZone utilizza la app Google Authenticator per il codice di autenticazione della 2FA.

In GravityZone, l'applicazione dell'autenticazione a due fattori è attivata per impostazione predefinita in tutta l'azienda. Ciò significa che tutti gli utenti di GravityZone devono configurare e usare la 2FA con i propri account.

Deselezionare l'opzione disattiverà l'applicazione della 2FA. Dovrai confermare questa azione. Di conseguenza, gli utenti avranno ancora la 2FA attivata, ma potranno disattivarla dalle impostazioni del loro account.

Nota

- Puoi visualizzare lo stato della 2FA per un account utente nella pagina **Account**.
- Se un utente con la 2FA attivata non può accedere a GravityZone (a causa di un nuovo dispositivo o per la perdita del codice segreto per Google Authenticator), puoi reimpostare l'attivazione della sua autenticazione a due fattori dalle impostazioni del proprio account nella pagina **Account**. Per maggiori dettagli, fai riferimento a «Gestire l'autenticazione a due fattori» (p. 37).

Imposta la durata massima della password a 90 giorni

Questa opzione attiva la policy di scadenza della password. Gli utenti devono modificare le proprie password prima della durata indicata. Diversamente, non potranno più accedere a GravityZone.

Blocca gli account dopo 5 tentativi di accesso con password non valide

Questa opzione limita il numero di password non valide consecutive inserite per prevenire eventuali attacchi. Quando il contatore raggiunge tale soglia, l'account viene bloccato e l'utente deve reimpostare la propria password.

La policy si applica agli account creati in GravityZone.

Configura l'autenticazione singola usando SAML

GravityZone supporta l'autenticazione singola (SSO) avviata dal fornitore di servizi (SP) come un'alternativa semplice e sicura al classico accesso con nome utente e password.

Questo metodo richiede l'integrazione con fornitore di identità (IdP) di terze parti tramite SAML 2.0, quali AD FS, Okta e Azure AD, che autenticano gli utenti di GravityZone e forniscono loro accesso a Control Center.

Ecco come funziona l'SSO di GravityZone:

1. Gli utenti inseriscono i propri indirizzi e-mail nella pagina di accesso di GravityZone.
2. GravityZone crea una richiesta SAML, per poi inoltrare la richiesta e gli utenti ai fornitori di identità.
3. Gli utenti devono quindi autenticarsi con il fornitore di identità.
4. Dopo l'autenticazione, il fornitore di identità invia una risposta a GravityZone nella forma di un documento XML firmato con un certificato X.509. Inoltre, il fornitore di identità ridireziona gli utenti a GravityZone.
5. GravityZone recupera la risposta, la convalida con l'impronta digitale del certificato e consente agli utenti di accedere a Control Center senza più interagirvi.

Gli utenti continuano ad accedere automaticamente a Control Center finché hanno una sessione attiva con il fornitore di identità.

Per attivare l'SSO, devi fare quanto segue:

1. Configura il fornitore d'identità per usare GravityZone come fornitore del servizio. Per i fornitori di identità supportati e maggiori informazioni sulla configurazione, fai riferimento a questo articolo della KB.
2. Attiva la SSO per la tua azienda:
   a. Alla voce **Configura l'autenticazione singola usando SAML**, inserisci l'URL dei metadati del fornitore d'identità nella casella corrispondente e clicca su **Salva**.
   b. Clicca su **Salva**.

3. Configura gli utenti nella tua azienda per l'autenticazione con il loro fornitore di identità. Per maggiori dettagli, fai riferimento a «Gestire i metodi di autenticazione dell'utente» (p. 36).

Importante
Come amministratore di GravityZone, puoi configurare l'autenticazione singola per gli utenti nella tua azienda, ma non per il tuo account per via di motivi di sicurezza.

Per disattivare l'autenticazione singola per la tua azienda:

1. Elimina l'URL dei metadati del fornitore d'identità.
2. Clicca su **Salva** e conferma.

Dopo aver disattivato l'autenticazione singola per la tua azienda, gli utenti inizieranno automaticamente ad accedere con le credenziali di GravityZone. Gli utenti possono ottenere una nuova password cliccando sul link **Hai dimenticato la password?** nella pagina di accesso alla Control Center e seguendo le istruzioni.

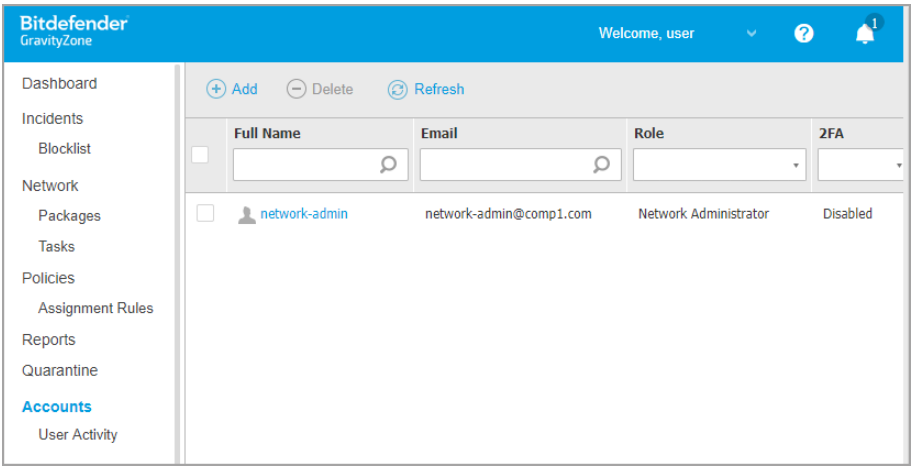
In caso di riattivazione della SSO per la tua azienda, gli utenti continueranno ad accedere a Control Center con le credenziali di GravityZone. Devi configurare manualmente ogni account per usare nuovamente la SSO.

5. ACCOUNT UTENTE

Puoi configurare e gestire GravityZone dalla Control Center, utilizzando l'account ricevuto dopo esserti abbonato al servizio.

Ecco ciò che devi sapere sugli account utente di GravityZone:

- Per ciascun account utente, puoi personalizzare l'accesso alle funzionalità di GravityZone, a determinate aziende o determinate parti della rete a cui appartiene.
- Puoi gestire solo gli account con privilegi pari o inferiori al tuo.



La pagina Account

Nella tabella vengono mostrati gli account esistenti. Per ciascun account utente, puoi visualizzare:

- Il nome utente dell'account.
- L'indirizzo e-mail dell'account (utilizzato per accedere alla Control Center). A questo indirizzo vengono inviati i rapporti e le notifiche inerenti la sicurezza. Le e-mail di notifica vengono inviate automaticamente ogni volta che nella rete vengono rilevate importanti condizioni di rischio.
- Ruolo utente (amministratore azienda / amministratore di rete / analista della sicurezza / personalizzato).

- Lo stato della 2FA (autenticazione a due fattori), che consente di verificare rapidamente se l'utente ha attivato la sua autenticazione a due fattori.
- Metodo di autenticazione, che indica se l'utente accede con le credenziali di GravityZone o con un fornitore di identità per l'autenticazione singola (SSO).

5.1. Ruoli utente

Un ruolo utente consiste in una combinazione specifica di diritti utente. Creando un account utente, puoi selezionare uno dei ruoli predefiniti oppure crearne uno personalizzato, selezionando solo determinati diritti utente.

Nota
Puoi garantire agli account utente gli stessi privilegi del tuo account, oppure inferiori.

Sono disponibili i seguenti ruoli utente:

1. **Amministratore azienda** - Adatto per direttori di aziende clienti che hanno acquistato una licenza di GravityZone da un partner. Un amministratore azienda gestisce la licenza, il profilo aziendale e l'intero impiego di GravityZone, consentendo il controllo al massimo livello su tutte le impostazioni di sicurezza (salvo che non venga superato dal suo account partner genitore in uno scenario di fornitore di servizi di sicurezza). Gli amministratori azienda possono condividere o delegare le proprie responsabilità operative ad account utente analista della sicurezza o amministratore subordinati.
2. **Amministratore di rete** - Per ogni azienda subordinata possono essere creati diversi account con il ruolo di Amministratore di rete, dotati di privilegi amministrativi su uno o più impieghi di agenti di sicurezza dell'azienda o su un determinato gruppo di endpoint, tra cui la gestione utente. Gli Amministratori di rete sono responsabili per la gestione attiva delle impostazioni di sicurezza della rete.
3. **Analista della sicurezza** - Gli account analista della sicurezza sono di sola lettura. Consentono l'accesso solo a dati, rapporti e registri correlati alla sicurezza. Tali account possono essere assegnati a dipendenti con responsabilità di monitoraggio della sicurezza o ad altri dipendenti che devono restare aggiornati sullo stato di sicurezza.
4. **Personalizzato** - Ruoli utente predefiniti che includono una determinata combinazione di diritti utente. Se un ruolo utente predefinito non soddisfa le

tue necessità, puoi creare un account personalizzato, selezionando solo i diritti di tuo interesse.

La seguente tabella riassume i rapporti tra i ruoli account e i propri diritti. Per informazioni dettagliate, fai riferimento a «Diritti utente» (p. 33).

Ruolo account	Account bambini consentiti	Diritti utente
Amministratore azienda	Amministratori azienda, Amministratori rete, Analisti della sicurezza	Gestione azienda Gestisci utenti Gestisci reti Vedi e analizza i dati
Amministratore rete	Amministratori rete, Analisti della sicurezza	Gestisci utenti Gestisci reti Vedi e analizza i dati
Analisti della sicurezza	-	Vedi e analizza i dati

5.2. Diritti utente

Puoi assegnare i seguenti diritti utente agli account utente di GravityZone:

- **Gestisci utenti**. Crea, modifica o elimina gli account utente.
- **Gestione azienda**. Gli utenti possono gestire il loro codice di licenza di GravityZone e modificare le impostazioni del proprio profilo aziendale. Questo privilegio è specifico per gli account amministratore aziendale.
- **Gestisci reti**. Fornisce privilegi amministrativi sulle impostazioni di sicurezza della rete (inventario di rete, policy, attività, pacchetti di installazione, quarantena). Questo privilegio è specifico per gli account amministratore di rete.

  Gli amministratori di rete delle aziende partner possono avere privilegi di gestione sulla sicurezza delle reti delle aziende clienti.
- **Vedi e analizza i dati**. Visualizza eventi e registri relativi alla sicurezza, gestisci i rapporti e la dashboard.

5.3. Gestire gli account aziendali

Prima di creare un account utente, assicurati di avere l'indirizzo e-mail richiesto a portata di mano. Questo indirizzo è obbligatorio per creare l'account utente di GravityZone. Gli utenti riceveranno i propri dettagli di accesso di GravityZone all'indirizzo e-mail indicato.

5.3.1. Gestire gli account utente individualmente

In Control Center, puoi creare, modificare ed eliminare gli account utente singolarmente.

Creare gli account utente individualmente

Per aggiungere un account utente in Control Center:

1. Vai alla pagina **Account**.
2. Clicca sul pulsante **Aggiungi** nel lato superiore della tabella. Apparirà una finestra di configurazione.
3. Nella sezione **Dettagli**, configura come indicato:
   - **Nome utente** per account locale. Disattiva **Importa da Active Directory** e inserisci un nome utente.
   - **E-mail**. Inserisci l'indirizzo e-mail dell'utente.

     L'indirizzo e-mail deve essere unico. Non è possibile creare un altro account utente con lo stesso indirizzo e-mail.

     GravityZone utilizza questo indirizzo e-mail per inviare notifiche.
   - **Nome completo**. Inserisci il nome completo dell'utente.
   - **Azienda**. Seleziona l'azienda a cui appartiene il nuovo account utente.
4. Nella sezione **Impostazioni e privilegi**, configura le seguenti impostazioni:
   - **Fuso orario**. Seleziona il fuso orario del tuo account dal menu. La console mostrerà le informazioni orarie in base al fuso orario selezionato.
   - **Lingua**. Seleziona la lingua utilizzata dalla console nel menu.
   - **Metodo di autenticazione**. Questa impostazione è disponibile per gli account di un'azienda con autenticazione singola attivata. Scegli dal menu l'account per accedere utilizzando le credenziali di GravityZone o un fornitore d'identità.

Per maggiori dettagli sui metodi di autenticazione disponibili, fai riferimento a «Gestire i metodi di autenticazione dell'utente» (p. 36).

- **Ruolo**. Seleziona il ruolo dell'utente. Per maggiori dettagli sui ruoli dell'utente, fai riferimento a «Ruoli utente» (p. 32).
- **Diritti**. Ogni ruolo dell'utente predefinito ha una determinata configurazione di diritti. Tuttavia, puoi selezionare solo i diritti che ti servono. In questo caso, il ruolo utente cambia in **Personalizzato**. Per maggiori dettagli sui diritti dell'utente, fai riferimento a «Diritti utente» (p. 33).
- **Seleziona bersagli**. Seleziona i gruppi della rete a cui l'utente dovrà accedere.

5. Clicca su **Salva** per aggiungere l'utente. Il nuovo account comparirà nell'elenco degli account utente.

> **Nota**
> La password per ciascun account utente viene generata automaticamente una volta creato l'account e inviata all'indirizzo e-mail dell'utente insieme agli altri dettagli dell'account.
> È possibile modificare la password dopo aver creato l'account. Clicca sul nome dell'account nella pagina **Accounts** per modificare la sua password. Una volta modificata la password, l'utente viene avvisato via e-mail immediatamente.
> Gli utenti possono modificare la loro password di accesso dalla Control Center, accedendo alla pagina **Il mio account**.

Modificare gli account utente individualmente

Per aggiungere un account utente in Control Center

1. Accedi al tuo account Control Center.
2. Vai alla pagina **Account**.
3. Clicca sul nome dell'utente.
4. Modifica le informazioni e le impostazioni dell'account, in base alle necessità.
5. Clicca su **Salva** per applicare le modifiche.

> **Nota**
> Tutti gli account con il diritto **Gestisci utenti** possono creare, modificare ed eliminare altri account utente. Puoi gestire solo gli account con privilegi pari o inferiori al tuo.

Eliminare gli account utente individualmente

Per eliminare un account utente in Control Center

1. Accedi al tuo account Control Center.
2. Vai alla pagina **Account**.
3. Seleziona l'account utente dall'elenco.
4. Clicca sul pulsante ⊖ **Elimina** nel lato superiore della tabella.

   Clicca su **Sì** per confermare.

5.4. Gestire i metodi di autenticazione dell'utente

Quando si crea o modifica un account utente in un'azienda con l'autenticazione singola (SSO) attivata, puoi configurarne l'accesso a Control Center.

Nella sezione **Impostazioni e privilegi**, hai le seguenti opzioni:

- **Accedi usando le credenziali di GravityZone**. Seleziona questa opzione per far accedere tale account a Control Center con nome utente e password.
- **Accedi usando il tuo fornitore d'identità**. Seleziona questa opzione per questo account per utilizzare l'autenticazione singola (SSO).

Puoi configurare il metodo di autenticazione per ogni singolo account utente di GravityZone.

GravityZone supporta diversi metodi di autenticazione per gli utenti nella stessa azienda. Inoltre, alcuni account potrebbero accedere con nome utente e password, mentre altri potrebbero autenticarsi con un fornitore di identità.

Per maggiori dettagli su come attivare la SSO per la tua azienda, fai riferimento a «Configura l'autenticazione singola usando SAML» (p. 29).

Importante

- Come amministratore di GravityZone, puoi configurare l'autenticazione singola per gli utenti nella tua azienda, ma non per il tuo account per via di motivi di sicurezza.
- Per l'SSO, gli utenti devono avere in GravityZone gli stessi indirizzi e-mail del fornitore di identità. Gli indirizzi e-mail sono sensibili alle maiuscole con l'SSO di GravityZone. Per esempio, **username@company.domain** è diverso da **UserName@company.domain** e **USERNAME@company.domain**.

- Bitdefender gestisce due istanze cloud di GravityZone. In alcuni casi, agli utenti potrebbe essere richiesto di scegliere un'istanza durante il primo accesso.

Per modificare le modifiche relative all'autenticazione singola per gli utenti di GravityZone, vai alla pagina **Account > Attività utente** e filtra i rapporti delle attività per Area e Impostazioni di autenticazione.

5.5. Modificare le password di accesso

I possessori degli account che hanno dimenticato la propria password possono modificarla utilizzando il link di recupero della password nella pagina di accesso. Puoi anche reimpostare una password di accesso dimenticata, modificando l'account corrispondente nella console.

Per modificare la password di accesso per un utente:

1. Accedi al tuo account Control Center.
2. Vai alla pagina **Account**.
3. Clicca sul nome dell'utente.
4. Digita la nuova password nei campi corrispondenti (in **Dettagli**).
5. Clicca su **Salva** per applicare le modifiche. Il possessore dell'account riceverà un'e-mail con la nuova password.

5.6. Gestire l'autenticazione a due fattori

Cliccando su un account utente, potrai visualizzare lo stato della sua 2FA (attivata o disattivata) nella sezione **Autenticazione a due fattori**. Puoi intraprendere le seguenti azioni:

- **Reimpostare o disattivare l'autenticazione a due fattori dell'utente**. Se un utente con la 2FA attivata ha cambiato o eliminato i dati sul dispositivo mobile, perdendo il suo codice segreto:
  1. Inserisci la tua password di GravityZone nel campo disponibile.
  2. Clicca su **Reimposta** (quando la 2FA è applicata) o **Disattiva** (quando la 2FA non è applicata).
  3. Un messaggio di conferma ti informerà che l'autenticazione a due fattori è stata reimpostata / disattivata per l'utente attuale.

Dopo aver reimpostato la 2FA quando questa funzionalità è applicata, all'accesso, una finestra di configurazione chiederà all'utente di configurare di nuovo l'autenticazione a due fattori con un nuovo codice segreto.

- Se l'utente ha la 2FA disattivata e vuoi attivarla, dovrai chiedere all'utente di attivare questa funzionalità dalle impostazioni del suo account.

Importante
La app di autenticazione scelta (Google Authenticator, Microsoft Authenticator o un qualsiasi autenticatore compatibile TOTP (Time-Based One-Time Password Algorithm), compatibile con lo standard RFC6238) combina il codice segreto con l'attuale time-stamp del dispositivo mobile per generare il codice a sei cifre. Assicurati che l'orario sia sul dispositivo mobile che nella appliance di GravityZone corrispondano in modo che il codice di sei cifre sia valido. Per evitare eventuali problemi di sincronizzazione con l'orario, ti consiglio di attivare l'impostazione di data e ora automatici sul dispositivo mobile.

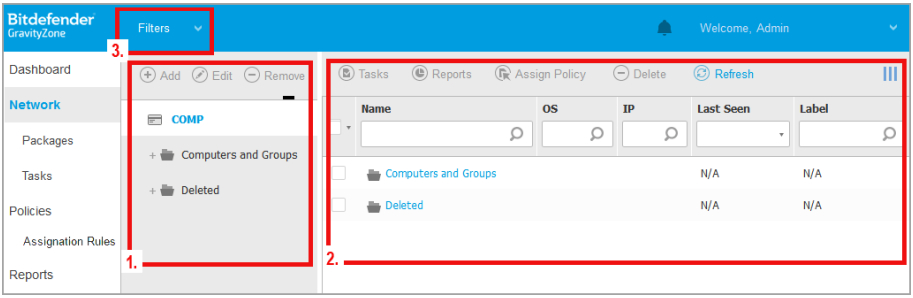
Un altro metodo per verificare le modifiche della 2FA relative all'account utente è accedere alla pagina **Account > Attività utente** e filtrare i rapporti di attività usando i seguenti filtri:

- Area > Account / Azienda
- Azione > Modificata

Per maggiori informazioni sull'attivazione della 3FA, fai riferimento a«Gestire il tuo account» (p. 22)

6. GESTIRE GLI ENDPOINT

La pagina **Rete** offre diverse funzionalità per esplorare e gestire gli endpoint disponibili. La pagina **Rete** consiste in un'interfaccia a due pannelli che mostra lo stato in tempo reale di tutti gli endpoint:



La pagina Rete

1. Il pannello a sinistra mostra la struttura della rete disponibile.

   Tutti gli endpoint eliminati vengono memorizzati nella cartella **Eliminati**. Per altre informazioni, fai riferimento a «Eliminare gli endpoint dall'inventario di rete» (p. 113).

   Nota
   Puoi visualizzare e gestire solo i gruppi su cui hai diritti di amministratore.

2. Il pannello a destra mostra i contenuti del gruppo che hai selezionato nello schema della rete. Questo pannello è formato di una griglia, in cui le righe contengono gli elementi di rete e le colonne mostrano determinate informazioni per ciascun elemento.

   Da questo pannello, è possibile:

   - Visualizzare informazioni dettagliate su ciascun elemento della rete nel tuo account. Puoi visualizzare lo stato di ciascun elemento controllando l'icona accanto al suo nome. Clicca sul nome dell'elemento per mostrare una finestra contenente maggiori dettagli.

     Ogni tipo di elemento, come computer, virtual machine o cartelle, è rappresentato da un'icona specifica. Allo stesso tempo, ogni elemento di rete può avere un determinato stato, relativo allo stato di gestione, problemi

di sicurezza, connettività e così via. Per maggiori dettagli relativi alla descrizione di ciascuna icona degli elementi della rete e gli stati disponibili, fai riferimento a «Tipi di elementi di rete e stati» (p. 457).

- Usa la Barra degli strumenti nel lato superiore della tabella per eseguire determinate operazioni per ciascun elemento di rete (come eseguire attività, creare rapporti, assegnare policy ed eliminarle) e aggiornare i dati della tabella.

3. Il menu **Filtri** disponibile nel lato superiore dei pannelli della rete ti aiuta a visualizzare facilmente ciascun elemento della rete, grazie a diversi criteri di filtro.

Nella pagina **Rete**, puoi gestire anche i pacchetti di installazione e le attività per i tuoi endpoint.

Nota
Per scoprire altre informazioni sui pacchetti di installazione, fai riferimento alla Guida di installazione di GravityZone.

Per visualizzare gli endpoint nel tuo account, vai alla pagina **Rete** e seleziona il gruppo di rete desiderato dal pannello a sinistra.

Puoi visualizzare la struttura della rete disponibile nel pannello a sinistra e maggiori dettagli su ciascun endpoint nel pannello a destra.

Inizialmente, tutte le virtual machine e i computer rilevati nella tua rete vengono mostrati come non gestiti, così puoi installare la loro protezione in remoto.

Per personalizzare i dettagli dell'endpoint mostrati nella tabella:

1. Clicca sul pulsante **Colonne** nel lato destro della Barra degli strumenti.
2. Seleziona le colonne che vuoi visualizzare.
3. Clicca sul pulsante **Reimposta** per tornare alla visuale delle colonne predefinita.

Dalla pagina **Rete**, puoi gestire gli endpoint come segue:

- Controllare lo stato dell'endpoint
- Visualizzare i dettagli dell'endpoint
- Organizzare gli endpoint in gruppi
- Ordinare, filtrare e cercare
- Gestisci le patch
- Eseguire attività
- Definire l'integrazione con Active Directory
- Creare rapporti veloci

- Assegnare policy
- Eliminare gli endpoint dall'inventario della rete

Per visualizzare le ultime informazioni nella tabella, clicca sul pulsante **Aggiorna** nell'angolo in basso a sinistra della tabella. Potrebbe essere necessario se si trascorre molto tempo nella pagina.

6.1. Controllare lo stato dell'endpoint

Ciascun endpoint viene rappresentato nella pagina della rete con una determinata icona in base al suo tipo e stato.

Fai riferimento a «Tipi di elementi di rete e stati» (p. 457) per un elenco con tutti i tipi di icone e stati disponibili.

Per informazioni dettagliate sullo stato, fai riferimento a:

- Stato gestione
- Stato connettività
- Stato sicurezza

6.1.1. Stato gestione

Gli endpoint possono avere i seguenti stati di gestione:

- **Gestiti** - Endpoint sui quali è stato installato l'agente di sicurezza.
- **Riavvio in sospeso** - Endpoint che richiedono un riavvio del sistema dopo aver installato o aggiornato la protezione di Bitdefender.
- **Non gestiti** - Endpoint rilevati su cui non è ancora stato installato l'agente di sicurezza.
- **Eliminati** - Endpoint che hai eliminato dalla Control Center. Per maggiori informazioni, fai riferimento a «Eliminare gli endpoint dall'inventario di rete» (p. 113).

6.1.2. Stato connettività

Lo stato della connettività riguarda tutte le virtual machine e solo i computer gestiti. Gli endpoint gestiti possono essere:

- **Online**. Un'icona blu indicata che l'endpoint è online.
- **Offline**. Un'icona grigia indica che l'endpoint è offline.

Un endpoint è offline se l'agente di sicurezza non è attivo per più di 5 minuti. Possibili motivi per cui gli endpoint possono apparire offline:

- L'endpoint è spento, in modalità riposo o disattivato.

  Nota
  Gli endpoint appaiono online anche quando sono bloccati o l'utente si è scollegato.

- L'agente di sicurezza non ha alcuna connettività con la Bitdefender Control Center o con il Endpoint Security Relay assegnato:
  - L'endpoint potrebbe essere stato disconnesso dalla rete.
  - Un firewall o un router della rete potrebbe bloccare la comunicazione tra l'agente di sicurezza e la Bitdefender Control Center o il Endpoint Security Relay assegnato.
  - L'endpoint si trova dietro un server proxy e le impostazioni proxy non sono state configurate correttamente nella policy applicata.

    Avvertimento
    Per gli endpoint dietro a un server proxy, le impostazioni del proxy devono essere configurate correttamente nel pacchetto di installazione dell'agente di sicurezza, altrimenti l'endpoint non comunicherà con la console di GravityZone e apparirà sempre offline, indipendentemente se dopo l'installazione viene applicata una policy con le impostazioni del proxy corrette.

- L'agente di sicurezza è stato disinstallato manualmente dall'endpoint, mentre l'endpoint non aveva alcuna connettività con la Bitdefender Control Center o con il Endpoint Security Relay assegnato. Normalmente, quando l'agente di sicurezza viene disinstallato manualmente da un endpoint, la Control Center viene notificata di questo evento e l'endpoint viene indicato come non gestito.
- L'agente di sicurezza potrebbe non funzionare correttamente.

Per scoprire per quanto tempo gli endpoint sono stati inattivi:

1. Mostra solo gli endpoint gestiti. Clicca sul menu **Filtri** nel lato superiore della tabella, seleziona tutte le opzioni "Gestito" che ti servono dalla scheda **Sicurezza**, scegli **Tutti gli elementi ricorsivamente** dalla scheda **Profondità** e clicca su **Salva**.
2. Clicca sull'intestazione della colonna **Ultima visualizzazione** per ordinare gli endpoint in base al periodo di inattività.

Puoi ignorare periodi più brevi di inattività (minuti, ore), poiché probabilmente sono dovuti a una condizione temporanea. Per esempio, l'endpoint è attualmente spento.

Periodi di inattività più lunghi (giorni, settimane), in genere, indicano un problema con l'endpoint.

Nota
Di tanto in tanto, si consiglia di aggiornare la tabella della rete, per aggiornare le informazioni degli endpoint con le ultime modifiche.

6.1.3. Stato sicurezza

Lo stato di sicurezza riguarda solo gli endpoint gestiti. Puoi identificare gli endpoint con problemi di sicurezza controllando le icone di stato che mostrano un simbolo di avvertimento:

- Computer gestito, con problemi, online.
- Computer gestito, con problemi, offline.

Un endpoint ha problemi di sicurezza se si verifica almeno una delle seguenti situazioni:

- La protezione antimalware è disattivata.
- La licenza è scaduta.
- L'agente di sicurezza è datato.
- Il contenuto di sicurezza non è aggiornato.
- Viene rilevato un malware.
- Non è stato possibile stabilire la connessione con i servizi cloud di Bitdefender, a causa dei seguenti possibili motivi:
  - Un firewall della rete sta bloccando la connessione con i servizi cloud di Bitdefender.
  - La porta 443, richiesta per la comunicazione con i servizi cloud di Bitdefender, è chiusa.

  In questo caso, la protezione antimalware si affida unicamente ai motori in locale, mentre la scansione in-the-cloud è disattivata, il che significa che l'agente di sicurezza non può fornire una protezione in tempo reale completa.

Se noti un endpoint con problemi di sicurezza, clicca sul suo nome per mostrare la finestra **Informazioni**. Puoi identificare i problemi di sicurezza dall'icona **!**. Assicurati di controllare le informazioni di sicurezza in tutte le schede della pagina

informazioni. Mostra il suggerimento dell'icona per scoprire maggiori dettagli. Potrebbero essere necessarie ulteriori indagini.

Nota
Di tanto in tanto, si consiglia di aggiornare la tabella della rete, per aggiornare le informazioni degli endpoint con le ultime modifiche.

6.2. Visualizzare i dettagli dell'endpoint

Puoi ottenere informazioni dettagliate su ciascun endpoint nella pagina **Rete**, come segue:

- Controllando la pagina **Rete**
- Controllando la finestra **Informazioni**

6.2.1. Controllare la pagina Rete

Per scoprire maggiori dettagli su un endpoint, consulta le informazioni disponibili nella tabella del pannello a destra nella pagina **Rete**.

Puoi aggiungere o rimuovere colonne con informazioni degli endpoint cliccando sul pulsante **Colonne** nel lato a destra in alto del pannello.

1. Vai alla pagina **Rete**.
2. Seleziona il gruppo desiderato dal pannello a sinistra.

   Tutti gli endpoint disponibili nel gruppo selezionato vengono mostrati nel lato destro della tabella del pannello.
3. Puoi identificare facilmente lo stato dell'endpoint controllando l'icona corrispondente. Per informazioni dettagliate, fai riferimento a «Controllare lo stato dell'endpoint» (p. 41).
4. Controlla le informazioni mostrate sulle colonne per ciascun endpoint.

   Usa la riga di intestazione mentre digiti per cercare endpoint specifici, in base ai criteri disponibili:

   - **Nome**: nome dell'endpoint.
   - **FQDN**: un nome di dominio completo che include il nome del dominio e dell'host.
   - **SO**: sistema operativo installato sull'endpoint.

- **IP**: l'indirizzo IP dell'endpoint.
- **Ultima visualizzazione**: data e ora dell'ultima visualizzazione online dell'endpoint.

  Nota
  È importante monitorare il campo **Ultima visualizzazione** in quanto i periodi di inattività potrebbero indicare un problema di comunicazione o un computer disconnesso.

- **Etichetta**: una stringa personalizzata con informazioni aggiuntive sull'endpoint. Puoi aggiungere un'etichetta nella finestra **Informazioni** e utilizzarla nelle ricerche.
- **Policy**: la policy applicata all'endpoint, con un link per visualizzare o modificare le impostazioni della policy.
- **Azienda**: l'azienda in cui si trova l'endpoint.

6.2.2. Controllare la finestra Informazioni

Nel pannello a destra della pagina **Rete**, clicca sul nome dell'endpoint a cui sei interessato per visualizzare la finestra **Informazioni**. Questa finestra mostra solo i dati disponibili per l'endpoint selezionato, raggruppati in diverse schede.

Qui di seguito trovi l'elenco completo delle informazioni che potresti trovare nella finestra **Informazioni**, in base al tipo di endpoint e le sue informazioni di sicurezza specifiche.

Scheda generale

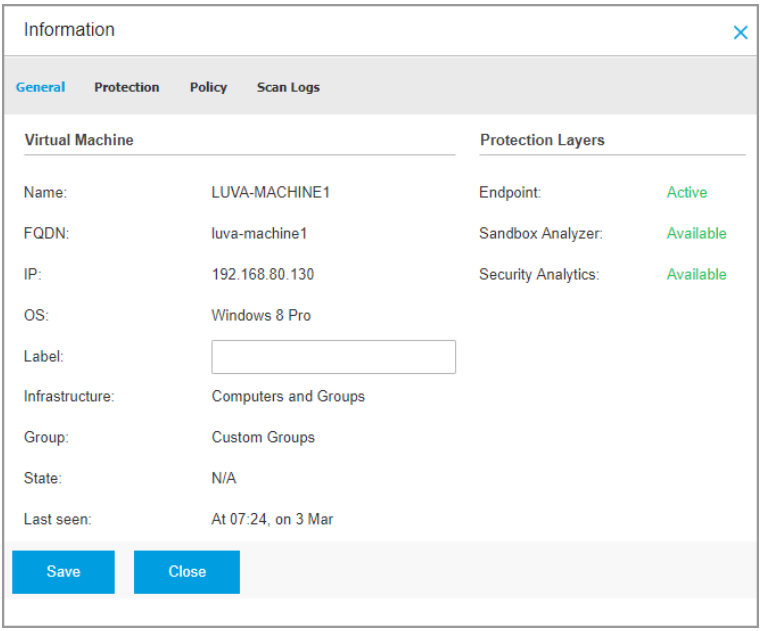
- Informazioni generali sull'endpoint, come nome, informazioni FQDN, indirizzo IP, sistema operativo, infrastruttura, gruppo parentale e stato attuale della connessione.

  In questa sezione, puoi assegnare un'etichetta all'endpoint. Potrai trovare rapidamente gli endpoint con la stessa etichetta e prendere azioni su di loro, indipendentemente dalla loro posizione nella rete. Per maggiori informazioni sul filtraggio degli endpoint, fai riferimento a «Ordinare, filtrare e cercare gli endpoint» (p. 62).

- Informazioni sui livelli di protezione, tra cui l'elenco delle tecnologie di sicurezza ottenute con la soluzione GravityZone e lo stato della loro licenza, che può essere:
  - **Senza licenza** - Il partner GravityZone non ha un codice di licenza per questo livello di protezione.
  - **Disponibile / Attivo** - Il codice di licenza per questo livello di protezione è attivo sull'endpoint.
  - **Scaduto** - Il codice di licenza per questo livello di protezione è scaduto.
  - **In sospeso** - Il codice di licenza non è ancora stato confermato.

    Nota
    Informazioni aggiuntive sui livelli di protezione sono disponibili nella scheda **Protezione**.

- **Connessione relay**: il nome, l'IP e l'etichetta del relay a cui è connesso l'endpoint, se il caso.
- Per gli endpoint con ruolo Active Directory Integrator: il nome del dominio e la data e l'ora dell'ultima sincronizzazione.



Finestra Informazioni - Scheda generali

Scheda Protezione

Questa scheda contiene dettagli sulla protezione applicata all'endpoint e fa riferimento a:

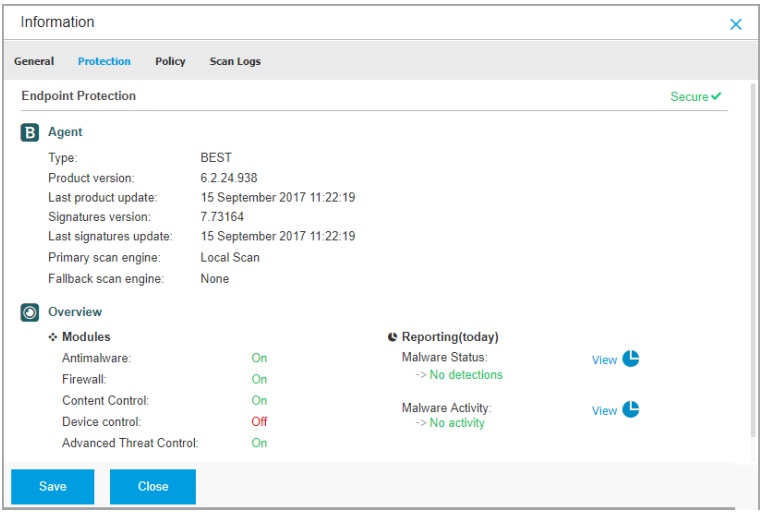
- Le informazioni dell'agente di sicurezza come nome del prodotto, versione, stato dell'aggiornamento e percorsi di aggiornamento, oltre a configurazione dei motori di scansione e versioni dei contenuti di sicurezza. Per Exchange Protection, è disponibile anche la versione del motore antispam..
- Lo stato di sicurezza per ogni livello di protezione. Questo stato compare nel lato destro del nome del livello di protezione:
  - **Sicuro**, quando non sono stati segnalati problemi di sicurezza sugli endpoint a cui è stato applicato il livello di protezione.
  - **Vulnerabile**, quando ci sono problemi di sicurezza segnalati sugli endpoint a cui è stato applicato il livello di protezione. Per maggiori dettagli, fai riferimento a «Stato sicurezza» (p. 43).

- Security Server assegnato. Ogni Security Server assegnato viene mostrato in caso di impieghi privi di agenti o quando i motori di scansione degli agenti di sicurezza vengono impostati per usare la scansione in remoto. Le informazioni del Security Server ti aiutano a identificare la virtual appliance e ottenere il suo stato di aggiornamento.
- Lo stato dei moduli di protezione. Puoi facilmente visualizzare quali moduli di protezione sono stati installati sull'endpoint e anche lo stato dei moduli disponibili (**Sì / No**) impostati tramite la policy applicata.
- Una rapida panoramica relativa all'attività dei moduli e le segnalazioni dei malware nella giornata attuale.

  Clicca sul link **Vedi** per accedere alle opzioni del rapporto e generare successivamente il rapporto stesso. Per maggiori informazioni, fai riferimento a «Creare i rapporti» (p. 406)
- Informazioni relative al livello di protezione Sandbox Analyzer:
  - Lo stato di utilizzo di Sandbox Analyzer sull'endpoint, mostrato nel lato destro della finestra:
    - **Attivo**: Sandbox Analyzer è concesso in licenza (disponibile) e attivato tramite policy sull'endpoint.
    - **Inattivo**: Sandbox Analyzer è concesso in licenza (disponibile) ma non attivato tramite policy sull'endpoint.
  - Nome dell'agente che agisce come sensore di feeding.
  - Stato del modulo sull'endpoint:
    - **Attivo** - Sandbox Analyzer viene attivato sull'endpoint tramite la policy.
    - **Inattivo** - Sandbox Analyzer non viene attivato sull'endpoint tramite la policy.
  - Rilevamenti delle minacce nell'ultima settimana cliccando sul link **Vedi** per accedere al rapporto.
- Informazioni aggiuntive relative al modulo Cifratura, come:
  - Volumi rilevati (indicando l'unità di avvio).
  - Lo stato di cifratura per ciascun volume (che può essere **Cifrato**, **Cifratura in corso**, **Decifratura in corso**, **Non cifrato**, **Bloccato** o **In pausa**).

Clicca sul link **Ripristino** per recuperare la chiave di ripristino per il volume cifrato associato. Per maggiori dettagli su come recuperare i codici di ripristino, fai riferimento a «» (p. 111).

- Informazioni su Security Analytics, come parte dell'EDR:
  - Informazioni agente specifico indica:
    - Fornitore eventi - BEST segnala il comportamento di endpoint e applicazioni al componente Security Analytics.
    - Stato comunicazione - BEST si connette a Security Analytics.
    - Ultimo stato di aggiornamento - Lo stato più recente.
  - Informazioni generali sullo stato di attivazione del Sensore incidenti.
- Lo stato della telemetria di sicurezza, che ti informa se la connessione tra l'endpoint e il server SIEM è stata stabilita e funziona, è disattivata o ha problemi.



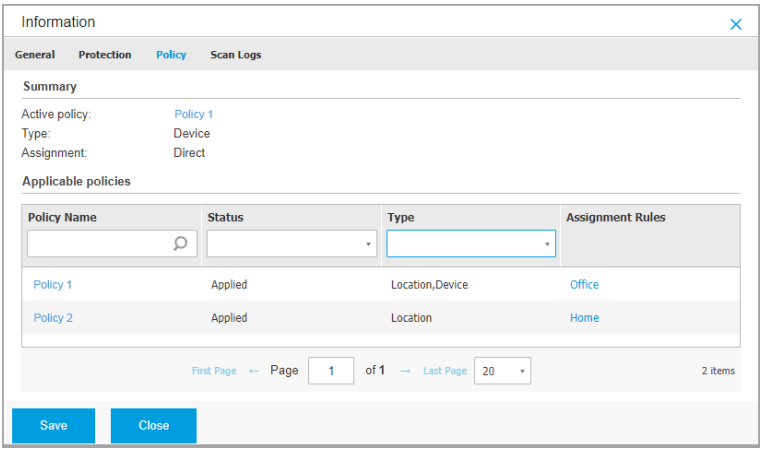
Finestra informazioni - Scheda Protezione

Scheda Policy

A un endpoint è possibile applicare una o più policy, ma può essere attivata una sola policy alla volta. La scheda **Policy** mostra informazioni su tutte le policy applicate all'endpoint.

- Il nome della policy attiva. Clicca sul nome della policy per aprire lo schema della policy e visualizzarne le impostazioni.
- Il tipo di policy attiva, che può essere:
  - **Dispositivo**: quando la policy viene assegnata manualmente all'endpoint dall'amministratore di rete.
  - **Ubicazione**: una policy basata su regola viene assegnata automaticamente all'endpoint, se le impostazioni di rete dell'endpoint corrispondono alle condizioni assegnate da una regola di assegnazione esistente.

    Per esempio, a un portatile vengono assegnate due policy in base alla posizione: una chiamata `Ufficio`, che è attiva quando si connette alla LAN aziendale, e una `Roaming`, che diventa attiva quando l'utente lavora in remoto e si connette ad altre reti.
  - **Utente**: una policy basata su regola viene assegnata automaticamente all'endpoint se corrisponde all'Active Directory bersaglio specificata in una regola di assegnazione esistente.
  - **Esterno (NSX)**: quando la policy viene definita nell'ambiente VMware NSX.
- Il tipo di assegnazione della policy attiva, che può essere:
  - **Diretta**: quando la policy viene applicata direttamente all'endpoint.
  - **Ereditata**: quando l'endpoint eredita la policy da un gruppo parentale.
- **Policy applicabili**: mostra l'elenco delle policy collegate alle regole di assegnazione esistenti. Queste policy possono essere applicate all'endpoint quando corrisponde alle condizioni assegnate delle regole di assegnazione collegate.

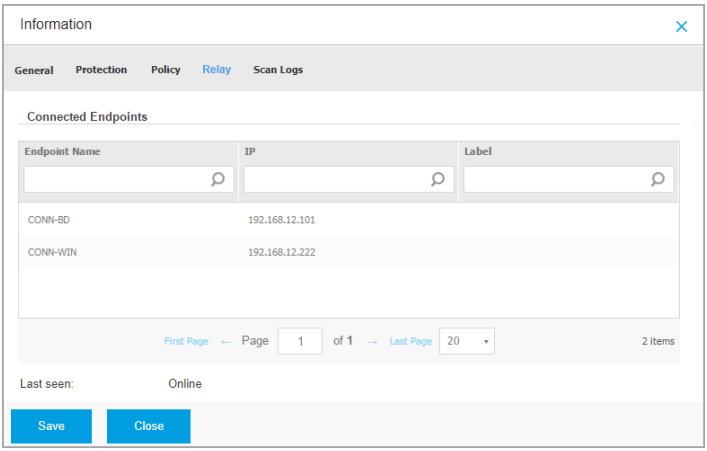


Finestra Informazioni - Scheda Policy

Per maggiori informazioni sulle policy, fai riferimento a«Modificare le impostazioni di una policy» (p. 134)

Scheda Endpoint connessi

La scheda **Endpoint connessi** è disponibile solo per gli endpoint con ruolo di relay. Questa scheda mostra informazioni sugli endpoint connessi al relay attuale, come nome, IP ed etichetta.



Finestra informazioni - Scheda Endpoint connessi

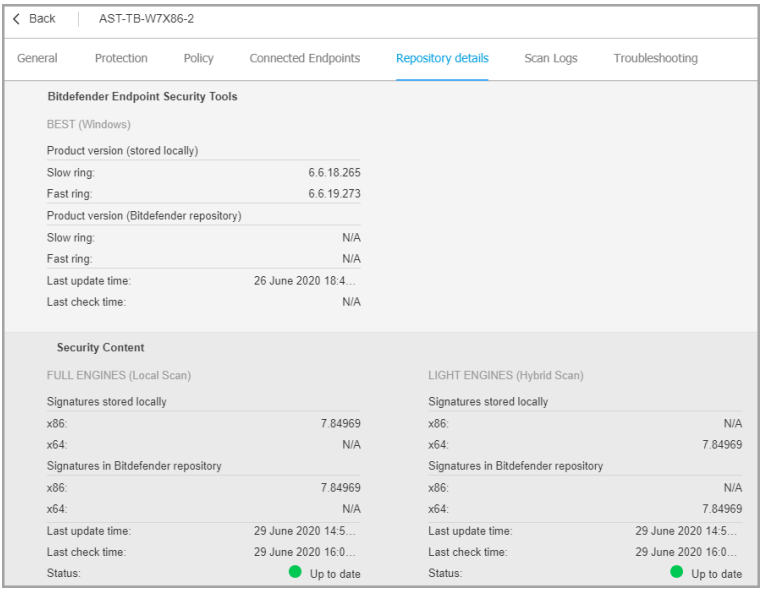
Scheda Dettagli archivio

La scheda **Dettagli archivio** è disponibile solo per gli endpoint con ruolo di relay e mostra informazioni sugli aggiornamenti dell'agente di sicurezza e i contenuti di sicurezza.

La scheda include dettagli sulle versioni del prodotto e delle firme memorizzati sul relay e su quelli disponibili nell'archivio ufficiale, ring di aggiornamento, la data e l'ora dell'aggiornamento e l'ultimo controllo delle nuove versioni.

Nota

- Le versioni dei contenuti di sicurezza sono disponibili solo per Windows Relay.
- Le versioni del prodotto non sono disponibili per i server di sicurezza.



Finestra informazioni - Scheda Dettagli archivio

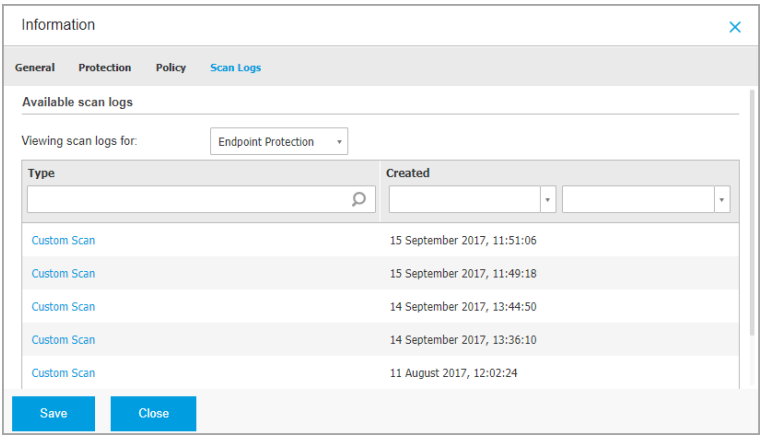
Scheda Rapporti di scansione

La scheda **Rapporti di scansione** mostra informazioni dettagliate su tutte le attività di scansione eseguite sull'endpoint.

I registri sono raggruppati per livello di protezione ed è possibile scegliere da un menu a discesa per quale livello mostrare i registri.

Clicca sull'attività di scansione che ti interessa e il registro si aprirà in una nuova pagina del browser.

Quando sono disponibili molti rapporti di scansione, possono essere utilizzate più pagine. Per muoversi tra le pagine, usa le opzioni di navigazione nella parte inferiore della tabella. Se ci sono troppi valori, puoi usare le opzioni di filtro disponibili nella parte superiore della tabella.

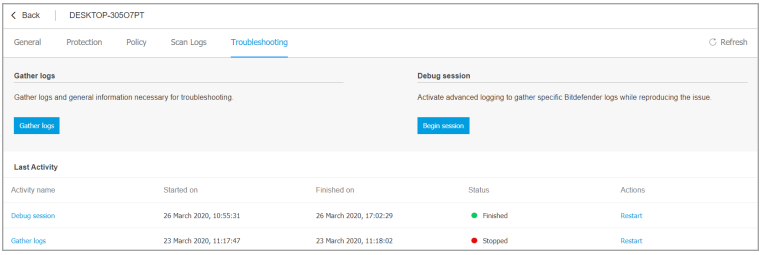


Finestra Informazioni - Tabella Rapporti di scansione

Scheda Risoluzione problemi

Questa sezione è dedicata alle attività di risoluzione dei problemi dell'agente. È possibile raccogliere rapporti generali o specifici dal controllo dell'endpoint o intraprendere azioni sugli attuali eventi di risoluzione dei problemi e visualizzare le attività precedenti.

Importante
Risoluzione problemi è disponibile per macchine con Windows, Linux, macOS e Security Server multipiattaforma.



Finestra informazioni - Scheda Risoluzione problemi

- **Raccogli rapporti**

Questa opzione ti aiuta a raccogliere un insieme di rapporti e informazioni generali necessarie per risolvere i problemi, come impostazioni, moduli attivi o policy applicate per la macchina bersaglio. Tutti i dati generati vengono salvati in un archivio.

Si consiglia di usare l'opzione quando la causa del problema non è chiara.

Per avviare il processo di risoluzione dei problemi:

1. Clicca sul pulsante **Ottieni rapporti**. Apparirà una finestra di configurazione.
2. Nella sezione **Archiviazione rapporti**, scegli una posizione di archiviazione.
   - **Macchina bersaglio**: l'archivio dei rapporti viene salvato nel percorso locale fornito. Il percorso non è configurabile per i Security Server.
   - **Condivisione di rete**: l'archivio dei rapporti viene salvato nel percorso indicato dal punto condiviso.
   - **Bitdefender Cloud**: l'archivio dei rapporti viene salvato in un punto di archiviazione di Bitdefender Cloud, dove il team di supporto aziendale può accedere ai file.

   Puoi usare l'opzione **Salva i rapporti anche sulla macchina bersaglio** per salvare una copia dell'archivio dei rapporti sulla macchina interessata come backup.
3. Inserisci le informazioni necessarie (percorso locale, credenziali per la condivisione di rete, percorso per la posizione condivisa, ID della pratica) in base alla posizione selezionata.
4. Clicca sul pulsante **Ottieni rapporti**.

Nota
Se hai scelto **Bitdefender Cloud** come opzione di archiviazione, considera quando segue:

- L'archivio dei rapporti viene salvato con nomi identici sia in **Bitdefender Cloud** che sulla macchina bersaglio. Clicca sull'evento della risoluzione problemi per visualizzare il nome dell'archivio nella finestra dei dettagli.
- Una volta che l'archivio viene aggiornato, fornisci al supporto aziendale di Bitdefender tutte le informazioni necessarie (nome della macchina bersaglio e il nome dell'archivio) nella pratica aperta. Apri una nuova pratica, se non ne esiste nessuna.

- **Sessione di debug**

Con la sessione di Debug, è possibile attivare la registrazione avanzata sulla macchina bersaglio per raccogliere rapporti specifici durante la riproduzione del problema.

Dovresti usare questa opzione una volta scoperto quale modulo sta causando i problemi o su suggerimento del supporto aziendale di Bitdefender. Tutti i dati generati vengono salvati in un archivio.

Per avviare il processo di risoluzione dei problemi:

1. Clicca sul pulsante **Inizia sessione**. Apparirà una finestra di configurazione.
2. Nella sezione **Tipo di problema**, seleziona il problema che pensi stia influenzando la macchina:

   Tipi di problema per macchine Windows e macOS:

Tipo di problema	Caso di utilizzo
Antimalware (scansione all'accesso e a richiesta)	– Rallentamento generale dell'endpoint – Un programma o una risorsa di sistema impiegano troppo tempo a rispondere – Un processo di scansione ha richiesto più tempo del solito – Nessuna connessione all'errore del servizio di sicurezza dell'host
Aggiorna errori	– I messaggi d'errore ricevuti durante gli aggiornamenti del prodotto o dei contenuti di sicurezza
Controllo contenuti (scansione del traffico e controllo utente)	– I siti web non si caricano – Gli elementi della pagina web non sono mostrati correttamente
Connettività servizi cloud	– L'endpoint non ha alcuna connettività con i servizi di Bitdefender Cloud
Problemi generali prodotto (reportistica eccessivamente prolissa)	– Riproduci un problema segnalato generico con registrazione dettagliata

   Tipi di problema per macchine Linux:

Tipo di problema	Caso di utilizzo
Antimalware e aggiornamento	– Un processo di scansione richiede più tempo del normale e consuma più risorse – I messaggi d'errore ricevuti durante gli aggiornamenti del prodotto o dei contenuti di sicurezza – L'endpoint non riesce a connettersi alla console di GravityZone.
Problemi generali prodotto (reportistica eccessivamente prolissa)	– Riproduci un problema segnalato generico con registrazione dettagliata

Tipi di problema per Security Server:

Tipo di problema	Caso di utilizzo
Antimalware (scansione all'accesso e a richiesta)	Ogni comportamento inatteso del Security Server, incluso: – Le virtual machine non sono protette correttamente – Le attività di scansione antimalware non funzionano o impiegano più tempo del previsto – Gli aggiornamenti del prodotto non sono stati installati correttamente – Generico malfunzionamento del Security Server (bd daemons non funziona)
Comunicazione con GravityZone Control Center	Ogni comportamento inatteso osservato dalla console di GravityZone: – Le virtual machine non vengono riportate correttamente nella console di GravityZone – Problemi di policy (la policy non viene applicata) – Il Security Server non può stabilire una connessione con la console di GravityZone

Tipo di problema	Caso di utilizzo
	Nota Usa questo metodo su raccomandazione del supporto aziendale di Bitdefender.

3. Per la **durata della sessione di debug**, scegli l'intervallo di tempo dopo cui la sessione di debug terminerà automaticamente.

   Nota
   Si consiglia di fermare manualmente la sessione usando l'opzione **Termina sessione**, subito dopo aver riprodotto il problema.

4. Nella sezione **Archiviazione rapporti**, scegli una posizione di archiviazione.
   - **Macchina bersaglio**: l'archivio dei rapporti viene salvato nel percorso locale fornito. Il percorso non è configurabile per i Security Server.
   - **Condivisione di rete**: l'archivio dei rapporti viene salvato nel percorso indicato dal punto condiviso.
   - **Bitdefender Cloud**: l'archivio dei rapporti viene salvato in un punto di archiviazione di Bitdefender Cloud, dove il team di supporto aziendale può accedere ai file.

   Puoi usare l'opzione **Salva i rapporti anche sulla macchina bersaglio** per salvare una copia dell'archivio dei rapporti sulla macchina interessata come backup.
5. Inserisci le informazioni necessarie (percorso locale, credenziali per la condivisione di rete, percorso per la posizione condivisa, ID della pratica) in base alla posizione selezionata.
6. Clicca sul pulsante **Inizia sessione**.

   Importante
   È possibile eseguire solo un processo di risoluzione dei problemi alla volta (**Raccogli rapporti** / **Sessione di debug** sulla macchina interessata.

- **Cronologia della Risoluzione dei problemi**

La sezione **Ultima attività** presenta le attività di risoluzione dei problemi sul computer interessato. La griglia mostra solo gli ultimi 10 eventi di risoluzione dei problemi in ordine cronologico inverso ed elimina automaticamente le attività più vecchie di 30 giorni.

La griglia mostra i dettagli per ogni processo di risoluzione dei problemi.

Il processo ha uno stato principale e uno intermedio. In base alle impostazioni personalizzate, puoi avere il seguente stato, in cui ti viene chiesto di intervenire:

- **In elaborazione (Pronto a riprodurre il problema)** - Accedi alla macchina interessata manualmente o in remoto, e riproduci il problema.

Hai diverse opzioni per fermare un processo di risoluzione dei problemi, come:

- **Termina sessione**: termina la sessione di debug e il processo di raccolta sulle macchine bersaglio, salvando tutti i dati ottenuti nella posizione di archiviazione specificata.

  Si consiglia di usare questa opzione subito dopo aver riprodotto il problema.

- **Annulla**: questa opzione annulla il processo, senza che venga ottenuto alcun rapporto.

  Usa questa opzione quando non vuoi raccogliere alcun rapporto dalla macchina bersaglio.

- **Forza blocco**: arresta forzatamente il processo di risoluzione dei problemi.

  Usa questa opzione quando l'annullamento della sessione impiega troppo tempo o la macchina bersaglio non risponde, così potrai avviare una nuova sessione in pochi minuti.

Per riavviare un processo della risoluzione problemi:

- **Riavvia**: questo pulsante, associato a ciascun evento e localizzato in **Azioni**, riavvia l'attività di risoluzione problemi mantenendo le sue impostazioni precedenti.

Importante

- Per assicurarti che la console mostri le informazioni più recenti, usa il pulsante **Aggiorna** nell'angolo in alto a destra della pagina **Risoluzione dei problemi**.
- Per maggiori dettagli su un determinato evento, clicca sul nome dell'evento nella griglia.

6.3. Organizzare gli endpoint in gruppi

Un importante beneficio di questa funzionalità è che puoi utilizzare le policy di gruppo per soddisfare requisiti di sicurezza differenti.

Puoi gestire i gruppi di endpoint nel pannello sul lato sinistro della pagina **Rete**, nella cartella **Computer e Gruppi** dall'azienda che ti interessa.

Nella cartella **Computer e Gruppi** appartenente all'azienda che vuoi gestire, puoi creare, eliminare, rinominare e spostare gruppi di computer in una struttura ad albero personalizzata.

Nota

- Un gruppo può includere sia endpoint che altri gruppi.
- Selezionando un gruppo nel pannello sul lato sinistro, puoi visualizzare tutti gli endpoint tranne quelli posizionati nei suoi sottogruppi. Per visualizzare tutti gli endpoint nel gruppo e nei suoi sottogruppi, clicca sul menu **Filtri** nel lato superiore della tabella e seleziona **Tutti gli elementi ricorsivamente** nella sezione **Profondità**.

Creare i gruppi

Prima di iniziare a creare i gruppi, pensa ai motivi per cui ti servono ed elabora uno schema di raggruppamento. Per esempio, puoi raggruppare gli endpoint in base a uno o più dei seguenti criteri:

- Struttura dell'azienda (Vendite, Marketing, Controllo qualità, Sviluppo software, Direzione, ecc.).
- Esigenze di sicurezza (desktop, portatili, server, ecc.).
- Luogo (Sede centrale, uffici locali, dipendenti in remoto, lavoro da casa, ecc.)

Per organizzare la tua rete in gruppi:

1. Seleziona la cartella **Cartella e Gruppi** nel pannello a sinistra.
2. Clicca sul pulsante **Aggiungi gruppo** nel lato superiore del pannello a sinistra.
3. Inserisci un nome specifico per il gruppo e clicca su **OK**.

Rinominare i gruppi

Per rinominare un gruppo:

1. Seleziona il gruppo nel pannello a sinistra.
2. Clicca sul pulsante **Modifica gruppo** nel lato superiore del pannello a sinistra.
3. Inserisci il nuovo nome nel campo corrispondente.

4. Clicca su **OK** per confermare.

Spostare i gruppi e gli endpoint

Puoi spostare eventuali entità in **Computer e Gruppi** in qualsiasi punto della gerarchia del gruppo. Per spostare un'entità, trascinala e rilasciala dal pannello a destra al gruppo in cui desideri nel panello a sinistra.

Nota

L'entità spostata erediterà le impostazioni della policy del nuovo gruppo parentale, a meno che non gli sia già stata assegnata direttamente una policy. Per maggiori informazioni sull'eredità delle policy, fai riferimento a «Policy di sicurezza» (p. 124).

Spostare gli endpoint tra le aziende

Puoi selezionare più endpoint e spostarli tra aziende che sono a un livello superiore o inferiore nella gerarchia dell'Inventario di rete. Per spostare gli endpoint in un'altra azienda:

1. Seleziona gli endpoint che intendi spostare nel lato destro della pagina **Rete**.
2. Trascina e rilasciane una in una cartella nell'azienda di destinazione. Comparirà una finestra di conferma con i dettagli dell'operazione di spostamento ed eventuali problemi che potrebbero verificarsi.

   Nota

   Se rilasci gli endpoint scelti direttamente sotto l'azienda, si verificherà un errore.

3. Conferma l'attività.

Per maggiori informazioni sullo spostamento degli endpoint tra aziende, fai riferimento a questo articolo della KB.

Eliminare i gruppi

Eliminare un gruppo è l'ultima azione. Di conseguenza, l'agente di sicurezza installato sull'endpoint considerato sarà rimosso.

Per eliminare un gruppo:

1. Clicca sul gruppo vuoto nel pannello a sinistra della **pagina Rete**.
2. Clicca sul pulsante ⊖ **Rimuovi gruppo** nel lato superiore del pannello a sinistra. Dovrai confermare la tua azione cliccando su **Sì**.

6.4. Ordinare, filtrare e cercare gli endpoint

In base al numero di endpoint, il pannello a destra può essere formato da diverse pagine (di norma, per ogni pagina sono presenti solo 20 voci). Per muoversi tra le pagine, usa i pulsanti di navigazione nella parte inferiore della tabella. Per cambiare il numero di valori mostrati in una pagina, seleziona un'opzione nel menu accanto ai pulsanti di navigazione.

Nel caso ci fossero troppi valori, puoi usare le caselle di ricerca sotto le intestazioni delle colonne o il menu **Filtri** nel lato superiore della pagina per mostrare solo le entità che ti interessano. Per esempio, puoi cercare un endpoint specifico o scegliere di visualizzare solo gli endpoint gestiti.

6.4.1. Ordinare gli endpoint

Per ordinare i dati di una determinata colonna, clicca sulla sua intestazione. Per esempio, se vuoi ordinare gli endpoint per nome, clicca sull'intestazione **Nome**. Se clicchi ancora sull'intestazione, gli endpoint saranno indicati in ordine inverso.

Ordinare i computer

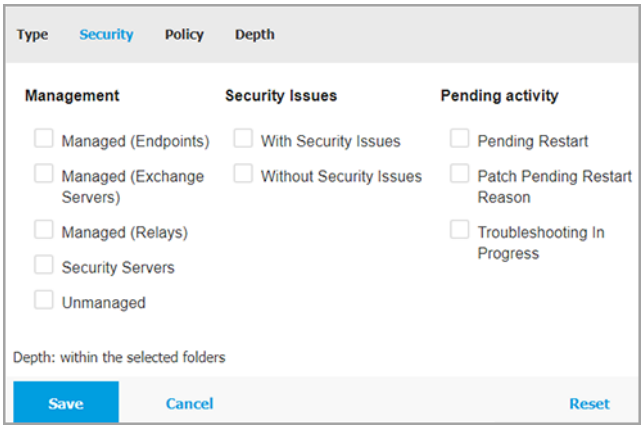
6.4.2. Filtrare gli endpoint

Per filtrare le entità della rete, usa il menu **Filtri** nel lato superiore dell'area dei pannelli della rete.

1. Seleziona il gruppo desiderato nel pannello a sinistra.
2. Clicca sul menu **Filtri** nel lato superiore dell'area dei pannelli della rete.
3. Usa i criteri di filtro come segue:
   - **Tipo**. Seleziona il tipo di entità che vuoi mostrare (computer, virtual machine, cartelle).

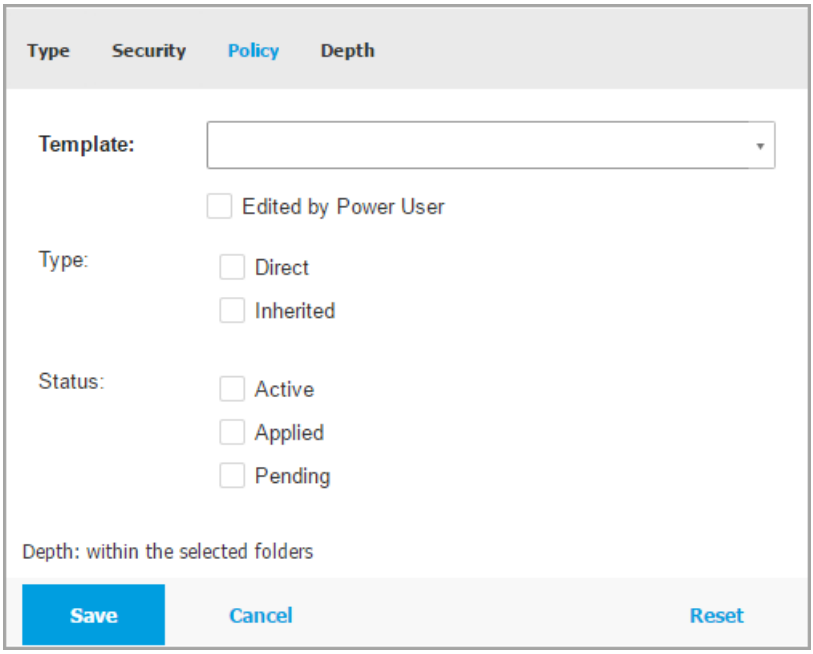
     Endpoint - Filtra per tipo

   - **Sicurezza**. Scegli di mostrare gli endpoint in base alla gestione della protezione, oltre allo stato della sicurezza o le attività in sospeso.



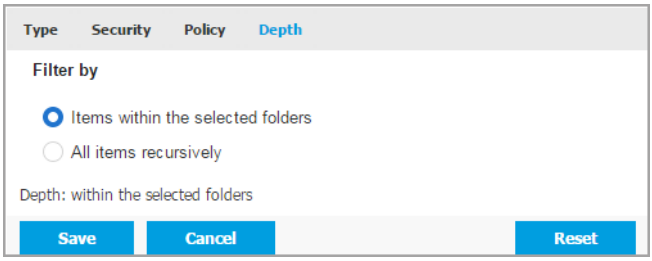
Endpoint - Filtra per sicurezza

- **Policy**. Seleziona lo schema della policy per cui vuoi filtrare gli endpoint, il tipo di assegnazione della policy (diretta o ereditata), oltre allo stato di assegnazione della policy (attiva, applicata o in corso). Puoi anche scegliere di mostrare solo entità con policy modificate nella modalità Utente esperto.



Endpoint - Filtra per policy

- **Profondità**. Quando si gestisce una rete strutturata ad albero, gli endpoint collocati nei sottogruppi non vengono visualizzati selezionando il gruppo base. Seleziona **Tutti gli elementi ricorsivamente** per visualizzare tutti gli endpoint inclusi nel gruppo attuale e tutti i suoi sottogruppi.



Endpoint - Filtra per profondità

Scegliendo di visualizzare tutti gli elementi ricorsivamente, la Control Center li mostra in un semplice elenco. Per trovare la posizione di un elemento, seleziona l'elemento desiderato e clicca sul pulsante **Vai al contenitore** nel lato superiore della tabella. Sarai reindirizzato al contenitore principale dell'elemento selezionato.

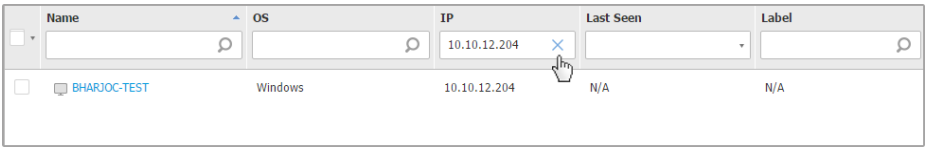
Nota
Puoi visualizzare tutti i criteri di filtro selezionati nella parte inferiore della finestra **Filtri**.
Se vuoi annullare tutti i filtri, clicca sul pulsante **Reimposta**.

4. Clicca su **Salva** per filtrare gli endpoint con i criteri selezionati. Il filtro resta attivo nella pagina **Rete** finché non esci o lo reimposti.

6.4.3. Cercare gli endpoint

1. Seleziona il gruppo desiderato nel pannello sulla sinistra.
2. Inserisci il termine da cercare nella casella corrispondente sotto le intestazioni della colonna nel pannello a destra. Per esempio, inserisci l'IP dell'endpoint che stai cercando nel campo **IP**. Nella tabella comparirà solo l'endpoint corrispondente.

   Cancella i contenuti nella casella di ricerca per mostrare l'elenco completo degli endpoint.



Ricerca degli endpoint

6.5. Inventario patch

GravityZone scopre le patch richieste dai tuoi software tramite le attività di **Scansione patch**, per poi aggiungerle all'inventario delle patch.

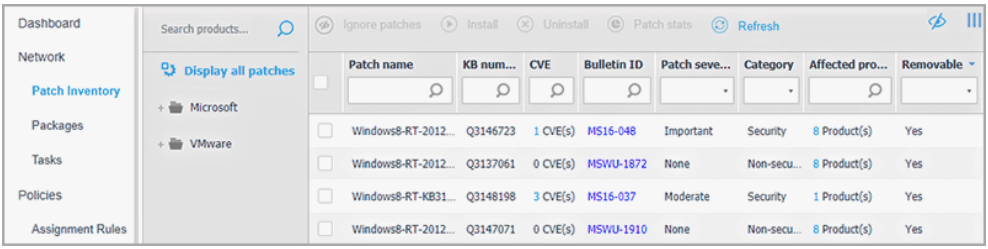
La pagina **Inventario patch** mostra tutte le patch trovate dal software installato sui tuoi endpoint e ti permette di eseguire diverse azioni su di esse.

Usa Inventario patch ogni volta che vuoi impiegare immediatamente determinate patch. Questa alternativa ti consente di risolvere facilmente determinati problemi rilevati. Per esempio, hai letto un articolo su una vulnerabilità software e conosci il CVE ID. Puoi cercare eventuali patch nell'inventario dedicate al CVE e poi visualizzare quali endpoint devono essere aggiornati.

Per accedere a Inventario patch, clicca sull'opzione **Rete > Inventario patch** nel menu principale della Control Center.

La pagina è suddivisa in due pannelli:

- Il pannello di sinistra mostra i prodotti software installati nella tua rete, raggruppati per fornitore.
- Il pannello di destra mostra una tabella con le patch disponibili e maggiori dettagli al riguardo.



Inventario patch

Poi, apprenderai come usare l'inventario. Ecco ciò che puoi fare:

- Visualizzare i dettagli delle patch
- Cercare e filtrare le patch
- Ignora le patch
- Installare le patch
- Disinstallare le patch
- Creare statistiche delle patch

6.5.1. Visualizzare i dettagli delle patch

La tabella delle patch fornisce informazioni in grado di aiutare a identificare le patch, valutarne l'importanza, visualizzare il loro stato di installazione e obiettivo. I dettagli sono descritti qui:

- **Nome patch.** Si tratta del nome del file eseguibile contenente la patch.
- **Numero KB.** Questo numero identifica l'articolo della KB che annuncia il rilascio della patch.
- **CVE.** Si tratta del numero di CVE risolte dalla patch. Cliccando sul numero, sarà visualizzato l'elenco di ID delle CVE.
- **ID bollettino.** Si tratta dell'ID del bollettino di sicurezza rilasciato dal venditore. Questo ID si collega all'articolo attuale, che descrive la patch e fornisce dettagli sull'installazione.
- **Severità patch.** Questa valutazione ti informa sull'importanza della patch in base ai danni che impedisce.
- **Categoria.** In base al tipo di problemi che risolvono, le patch sono raggruppate in due categorie: sicurezza e non sicurezza. Questo campo ti informa sulla categoria della patch.
- **Prodotti coinvolti.** Si tratta del numero di prodotti per cui la patch viene rilasciata. Il numero si collega all'elenco di questi prodotti software.
- **Rimovibile.** Se devi eseguire il rollback di una determinata patch, devi prima verificare che possa essere disinstallata. Usa questo filtro per individuare le patch che possono essere rimosse (tramite rollback). Per maggiori informazioni, fai riferimento a Disinstallare le patch.
- **Azienda**. Il numero di aziende che gestisci nelle quali la patch è attiva o ignorata, in base alla schermata selezionata.

Per personalizzare i dettagli mostrati nella tabella:

1. Clicca sul pulsante **Colonne** nel lato destro della Barra degli strumenti.
2. Seleziona le colonne che vuoi visualizzare.
3. Clicca sul pulsante **Reimposta** per tornare alla visuale delle colonne predefinita.

Mentre sei nella pagina, i processi di GravityZone in esecuzione in background potrebbero influenzare il database. Assicurati di visualizzare le informazioni più

recenti nella tabella, cliccando sul pulsante **Aggiorna** nel lato superiore della tabella.

GravityZone verifica una volta a settimana l'elenco delle patch disponibili ed elimina quelle non più applicabili perché le relative applicazioni o gli endpoint non esistono più.

Inoltre, GravityZone rivede ed elimina quotidianamente le patch non disponibili nell'elenco, nonostante possano essere presenti su alcuni endpoint.

6.5.2. Cercare e filtrare le patch

Di norma, la Control Center mostra tutte le patch disponibili per il tuo software. GravityZone ti offre diverse opzioni per trovare rapidamente le patch che ti servono.

Filtrare le patch per prodotto

1. Localizza il prodotto nel pannello di sinistra.

   Puoi farlo facendo scorrere l'elenco per trovare il rispettivo fornitore, o digitando il suo nome nella casella di ricerca nel lato superiore del pannello.
2. Clicca sul nome del fornitore per espandere l'elenco e visualizzare i suoi prodotti.
3. Seleziona il prodotto per vedere le patch disponibili, o deselezionalo per nascondere le sue patch.
4. Ripeti i passaggi precedenti per gli altri prodotti di tuo interesse.

Se vuoi visualizzare nuovamente le patch per tutti i prodotti, clicca sul pulsante **Mostra tutte le patch** nel lato superiore del pannello di sinistra.

Filtrare le patch per utilità

La Control Center mostra le patch ignorate in un altro modo. Clicca sul pulsante **Gestiti/Ignorati** nel lato destro della Barra degli strumenti per cambiare la visuale tra:

- - Per visualizzare le patch ignorate.
- - Per visualizzare le patch gestite.

Filtrare le patch per dettagli

Usa la ricerca per filtrare le patch in base a determinati criteri o dettagli noti. Inserisci i termini di ricerca nelle caselle di ricerca nel lato superiore della tabella delle patch. Le patch corrispondenti vengono mostrate nella tabella durante la digitazione o la selezione effettuata.

Cancellando i campi di ricerca reimposterai la ricerca.

6.5.3. Ignorare le patch

Per escludere dall'inventario le patch che non hai intenzione di installare sui tuoi endpoint, usa il comando **Ignora le patch**.

Inoltre puoi decidere di ignorare determinate patch per alcune delle aziende che gestisci, pur conservandole nell'inventario delle patch per le altre aziende.

Le patch ignorate verranno escluse dalle attività automatiche e dai rapporti relativi alle patch e non verranno considerate patch mancanti.

Per ignorare una patch:

1. Nella pagina **Inventario patch**, seleziona una o più patch da ignorare.
2. Clicca sul pulsante **Ignora le patch** nel lato superiore della tabella.

   Si aprirà una finestra di configurazione, nella quale potrai vedere i dettagli relativi alle patch selezionate, insieme a tutte le patch subordinate.

   Importante
   Selezionando l'azienda principale, le aziende subordinate non verranno selezionate automaticamente. Verifica di aver selezionato tutte le aziende da includere.

3. Clicca su **Ignora**. La patch verrà rimossa dall'elenco dell'inventario.

Puoi trovare ed eseguire azioni sulle patch ignorate in una specifica schermata:

- Clicca sul pulsante **Mostra patch ignorate** nell'angolo in alto a destra della tabella. Vedrai l'elenco di tutte le patch ignorate.
- Puoi ottenere maggiori informazioni su una determinata patch che hai ignorato generando un rapporto di statistiche sulle patch. Seleziona la patch ignorata che desideri e clicca sul pulsante **Statistiche delle patch** nella parte superiore della tabella. Per maggiori dettagli, fai riferimento a «Creare statistiche delle patch» (p. 73)
- Per ripristinare le patch ignorate, selezionale e fai clic sul pulsante **Ripristina patch** nel lato superiore della tabella.

  Si aprirà una finestra di configurazione, nella quale potrai vedere i dettagli relativi alle patch selezionate e selezionare le aziende per le quali le patch verranno ripristinate.

Clicca sul pulsante **Ripristina** per trasferire la patch nell'inventario.

6.5.4. Installare le patch

Per installare le patch da Inventario patch:

1. Vai su **Rete > Inventario patch**.
2. Localizza le patch che vuoi installare. Se necessario, usa le opzioni di filtraggio per trovarle rapidamente.
3. Seleziona le patch e clicca sul pulsante **Installa** nel lato superiore della tabella. Si aprirà una finestra di configurazione, dalla quale puoi modificare i dettagli di installazione delle patch.

   Vedrai le patch selezionate e tutte le relative patch subordinate.

   - Seleziona i gruppi bersaglio degli endpoint.
   - **Se necessario, riavvia gli endpoint dopo aver installato la patch**. Questa opzione riavvierà gli endpoint immediatamente dopo l'installazione delle patch, se è richiesto un riavvio del sistema. Nota che questa azione può interrompere l'attività degli utenti.

     Se questa opzione viene lasciata disattivata ed è necessario un riavvio del sistema, verrà mostrata l'icona dello stato di riavvio in sospeso nell'inventario di rete di GravityZone. In questo caso puoi scegliere tra le seguenti opzioni:

     – Puoi inviare in qualsiasi momento un'attività **Riavvia macchina** agli endpoint con riavvio in sospeso. Per maggiori dettagli, fai riferimento a «Riavvia macchina» (p. 104).

     – Configura la policy attiva per comunicare all'utente dell'endpoint che è necessario un riavvio. Per farlo, accedi alla policy attiva sull'endpoint di destinazione, vai su **Generale > Notifiche** e attiva l'opzione **Notifica riavvio endpoint**. In questo modo l'utente vedrà apparire un messaggio pop-up ogniqualvolta è necessario un riavvio dovuto a modifiche effettuate dal componente di GravityZone specificato (in questo caso da Gestione patch). Il messaggio pop-up permette di scegliere di posticipare il riavvio. Se l'utente sceglie di posticipare, la notifica del riavvio comparirà sullo schermo periodicamente, finché il sistema non sarà riavviato o fino a quando non è trascorso il tempo impostato nel campo Amministratore azienda.

Per maggiori dettagli, fai riferimento a «Notifica riavvio endpoint» (p. 141).

4. Clicca su **Installa**.

   Viene creata l'attività di installazione, insieme con le sotto-attività per ciascun endpoint bersaglio.

Nota

- Puoi installare una patch anche dalla pagina **Rete**, iniziando dagli specifici endpoint che desideri gestire. In questo caso seleziona gli endpoint dall'inventario di rete, clicca sul pulsante **Attività** nel lato superiore della tabella e scegli **Installazione patch**. Per maggiori informazioni, fai riferimento a «Installazione patch» (p. 90).
- Dopo aver installato una patch, ti consigliamo di inviare un'attività Scansione patch agli endpoint di destinazione. In questo modo verranno aggiornate le informazioni sulle patch archiviate in GravityZone per le reti che gestisci.

6.5.5. Disinstallare le patch

Potresti dover rimuovere delle patch che hanno causato malfunzionamenti negli endpoint di destinazione. GravityZone offre una funzionalità di rollback per le patch installate sulla tua rete, che ripristina il software allo stato precedente alla loro applicazione.

La funzionalità di disinstallazione è disponibile solo per le patch rimovibili. L'inventario delle patch di GravityZone include una colonna **Rimovibile**, dalla quale puoi filtrare le patch che possono o non possono essere rimosse.

Nota

La rimovibilità dipende da come la patch è stata realizzata dal produttore o dalle modifiche apportate dalla patch al software. In caso di patch che non possono essere rimosse, può essere necessario reinstallare il software.

Per disinstallare una patch:

1. Vai su **Rete > Inventario patch**.
2. Seleziona la patch che vuoi disinstallare. Per cercare una specifica patch usa i filtri disponibili nelle colonne, come il numero KB o CVE. Usa la colonna **Rimovibile** per visualizzare solo le patch disponibili che possono essere disinstallate.

Nota
Puoi disinstallare solo una patch per volta, per uno o più endpoint.

3. Clicca sul pulsante ⊗ **Disinstalla** nel lato superiore della tabella. Si aprirà una finestra di configurazione, dalla quale puoi modificare i dettagli dell'attività di disinstallazione.
   - **Nome attività**. Se vuoi puoi modificare il nome predefinito dell'attività di disinstallazione della patch. In questo modo potrai individuarla più facilmente nella pagina **Attività**.
   - **Aggiungi patch all'elenco delle patch ignorate**. Di solito non avrai più bisogno di una patch che vuoi disinstallare. Con questa opzione la patch viene aggiunta automaticamente all'elenco delle patch ignorate, una volta disinstallata.
   - **Se necessario, riavvia gli endpoint dopo aver disinstallato la patch**. Questa opzione riavvierà gli endpoint immediatamente dopo la disinstallazione delle patch, se è richiesto un riavvio del sistema. Nota che questa azione può interrompere l'attività degli utenti.

     Se questa opzione viene lasciata disattivata ed è necessario un riavvio del sistema, verrà mostrata l'icona dello stato di riavvio in sospeso nell'inventario di rete di GravityZone. In questo caso puoi scegliere tra le seguenti opzioni:
     - Puoi inviare in qualsiasi momento un'attività **Riavvia macchina** agli endpoint con riavvio in sospeso. Per maggiori dettagli, fai riferimento a «Riavvia macchina» (p. 104).
     - Configura la policy attiva per comunicare all'utente dell'endpoint che è necessario un riavvio. Per farlo, accedi alla policy attiva sull'endpoint di destinazione, vai su **Generale > Notifiche** e attiva l'opzione **Notifica riavvio endpoint**. In questo modo l'utente vedrà apparire un messaggio pop-up ogniqualvolta è necessario un riavvio dovuto a modifiche effettuate dal componente di GravityZone specificato (in questo caso da Gestione patch). Il messaggio pop-up permette di scegliere di posticipare il riavvio. Se l'utente sceglie di posticipare, la notifica del riavvio comparirà sullo schermo periodicamente, finché il sistema non sarà riavviato o fino a quando non è trascorso il tempo impostato nel campo Amministratore azienda.

Per maggiori dettagli, fai riferimento a «Notifica riavvio endpoint» (p. 141).

- Nella tabella **Rollback bersagli**, seleziona gli endpoint da cui vuoi disinstallare la patch.

  Puoi selezionare uno o più endpoint della stessa azienda. Per prima cosa seleziona l'azienda in cui si trovano gli endpoint dall'intestazione della colonna **Azienda**. Dopodiché puoi usare gli altri filtri disponibili per individuare l'endpoint che desideri.

  Nota
  La tabella mostra solo gli endpoint su cui è installata la patch selezionata.

4. Clicca su **Conferma**. Verrà creata e inviata agli endpoint un'attività **Disinstallazione patch**.

   Per ogni attività di disinstallazione di patch completata viene generato automaticamente un rapporto **Disinstallazione patch**, contenente informazioni dettagliate sulla patch, sugli endpoint di destinazione e sullo stato dell'attività.

Nota
Dopo aver disinstallato una patch, ti consigliamo di inviare un'attività Scansione patch agli endpoint di destinazione. In questo modo verranno aggiornate le informazioni sulle patch archiviate in GravityZone per le reti che gestisci.

6.5.6. Creare statistiche delle patch

Se ti servono dettagli sullo stato di una determinata patch per tutti gli endpoint, usa la funzionalità **Statistiche patch**, che genera un rapporto istantaneo per la patch selezionata:

1. Nella pagina **Inventario patch**, seleziona la patch che desideri nel pannello di destra.
2. Clicca sul pulsante **Statistiche patch** nel lato superiore della tabella.

   Compare un rapporto delle statistiche della patch, fornendo vari dettagli sullo stato della patch, tra cui:

   - Un diagramma, che mostra la percentuale di stato delle patch installate, fallite, mancanti e in sospeso per gli endpoint che hanno segnalato la patch.
   - Una tabella che mostra le seguenti informazioni:
     - **Name**, **FQDN**, **IP** e **SO** di ciascun endpoint che ha segnalato la patch.

- **Ultimo controllo**: il momento in cui la patch è stata controllata l'ultima volta sull'endpoint.
- **Stato patch**: installata, fallita, mancante o ignorata.

Nota
La funzionalità Statistiche delle patch sono disponibili sia per le patch gestite che ignorate.

6.6. Eseguire le attività

Dalla pagina **Rete**, puoi eseguire in remoto un certo numero di attività amministrative sugli endpoint.

Ecco ciò che puoi fare:

- «Esamina» (p. 75)
- «Scansione per IOC» (p. 84)
- «Scansione rischi» (p. 87)
- «Attività di patch» (p. 88)
- «Scansione Exchange» (p. 91)
- «Installa» (p. 95)
- «Disinstalla client» (p. 100)
- «Aggiorna client» (p. 101)
- «Riconfigura il client» (p. 102)
- «Ripara client» (p. 103)
- «Riavvia macchina» (p. 104)
- «Network Discovery» (p. 105)
- «Aggiorna Security Server» (p. 105)

Puoi scegliere di creare attività per ciascun endpoint o per gruppi di endpoint. Per esempio, puoi installare in remoto l'agente di sicurezza su un gruppo di endpoint non gestiti. In un secondo momento, puoi creare un'attività di scansione per un determinato endpoint dallo stesso gruppo.

Per ciascun endpoint, puoi eseguire solo attività compatibili. Per esempio, se selezioni un endpoint non gestito, puoi scegliere solo di installare l'agente di sicurezza, mentre tutte le altre attività saranno disattivate.

Per un gruppo, l'attività selezionata sarà creata solo per gli endpoint compatibili. Se nessun endpoint nel gruppo è compatibile con l'attività selezionata, sarai avvisato che non è possibile crearla.

Una volta creata, l'attività sarà eseguita immediatamente sugli endpoint online. Se un endpoint è offline, l'attività sarà eseguita non appena sarà di nuovo online.

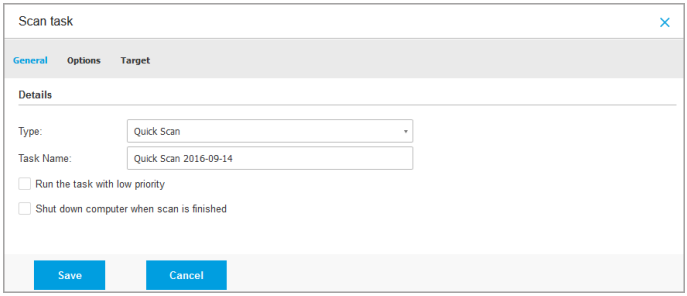
Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**. Per maggiori informazioni, fai riferimento a Visualizzare e gestire le attività.

Esamina

Per eseguire in remoto un'attività di scansione su uno o più endpoint:

1. Vai alla pagina **Rete**.
2. Seleziona il contenitore desiderato dal pannello a sinistra. Tutti gli endpoint del contenitore selezionato sono mostrati nella tabella a destra.
3. Seleziona le caselle di spunta degli endpoint o gruppi che vuoi esaminare.
4. Clicca sul pulsante **Attività** nel lato superiore della tabella e seleziona **Esamina**.

   Apparirà la finestra di configurazione.
5. Configura le opzioni di scansione:
   - Nella tabella **Generale**, puoi scegliere il tipo di scansione e inserire un nome per l'attività di scansione. Il nome dell'attività di scansione ti aiuta a identificare facilmente la scansione attuale nella pagina **Attività**.



Attività di scansione - Configurare le impostazioni generali

Selezionare il tipo di scansione dal menu **Tipo**:

– La **Scansione veloce** utilizza una scansione in-the-cloud per rilevare eventuali malware in esecuzione sul sistema. Questo tipo di scansione è preconfigurato per consentire di esaminare solo le ubicazioni critiche di sistemi come Windows e Linux. In genere eseguire una Scansione

veloce richiede meno di un minuto e usa una frazione delle risorse di sistema necessarie per una scansione standard.

Quando vengono rilevati malware o rootkit, Bitdefender procede automaticamente con la disinfezione. Se, per un qualche motivo, il file non può essere disinfettato, allora viene messo in quarantena. Questo tipo di scansione ignora i file sospetti.

– La **Scansione completa** esamina l'intero sistema per rilevare tutti i tipi di malware che minacciano la sua sicurezza, come virus, spyware, adware, rootkit e altri.

  Bitdefender prova a disinfettare automaticamente tutti i file in cui sono stati rilevati malware. Nel caso in cui i malware non possano essere rimossi, i file vengono messi in quarantena, dove non possono provocare danni. I file sospetti vengono ignorati. Se vuoi comunque intraprendere delle azioni sui file sospetti, o se desideri altre azioni predefinite per i file infetti, scegli di avviare una Scansione personalizzata.

– La **Scansione memoria** controlla i programmi in esecuzione nella memoria dell'endpoint.

– La **Scansione di rete** è un tipo di scansione personalizzata, che consente di esaminare le unità di rete utilizzando l'agente di sicurezza di Bitdefender installato sull'endpoint obiettivo.

  Per eseguire l'attività di scansione di rete:

  - Devi assegnare l'attività a un solo endpoint nella tua rete.
  - Devi inserire le credenziali di un account utente con permessi di lettura/scrittura sulle unità di rete obiettivo, in modo che l'agente di sicurezza possa accedere e intraprendere azioni su queste unità di rete. Le credenziali richieste possono essere configurate nella tabella **Bersaglio** della finestra delle attività.

– La **Scansione personalizzata** ti consente di scegliere le posizioni da esaminare e configurare le opzioni di scansione.

Per le scansioni di memoria, rete e personalizzate, hai anche le seguenti opzioni:

– **Esegui l'attività con bassa priorità**. Seleziona questa casella per ridurre la priorità del processo di scansione e consentire ad altri programmi di

funzionare più velocemente. Ciò aumenterà il tempo necessario per completare la scansione.

Nota
Questa opzione di applica solo a Bitdefender Endpoint Security Tools e Endpoint Security (agente datato).

– **Spegni il computer al termine della scansione**. Seleziona questa casella per disattivare la tua macchina se non intendi utilizzarla per un po'.

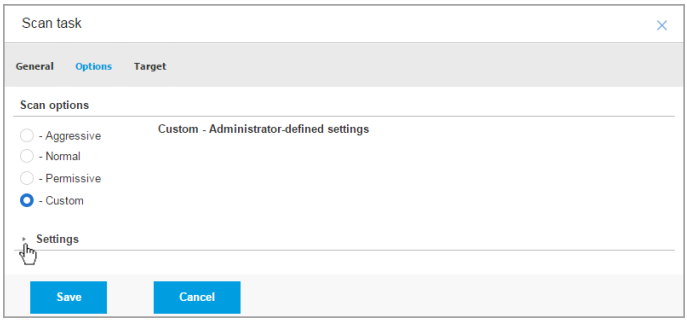
Nota
Questa opzione di applica a Bitdefender Endpoint Security Tools, Endpoint Security (agente datato) e Endpoint Security for Mac.

Nota
Queste due opzioni si applicano solo a Bitdefender Endpoint Security Tools e Endpoint Security (agente precedente).

Per le scansioni personalizzate, configura le seguenti impostazioni:

– Vai alla scheda **Opzioni** per impostare le opzioni della scansione. Clicca sul livello di sicurezza che si adatta meglio alle tue esigenze (Aggressivo, Normale o Permissivo). Usa la descrizione sul lato destro dell'indicatore per scegliere.

  In base al profilo selezionato, le opzioni della scansione nella sezione **Impostazioni** sono configurate in maniera automatica. Tuttavia, se lo desideri, puoi configurarle nei dettagli. Per farlo, seleziona la casella **Personalizzate** ed espandi la sezione **Impostazioni**.



Attività di scansione - Configurare una scansione personalizzata

Sono disponibili le seguenti opzioni:

- **Tipi di file.** Usa queste opzioni per specificare quali tipi di file vuoi che siano esaminati. Puoi impostare l'agente di sicurezza in modo che esamini tutti i file (indipendentemente dalla loro estensione), solo i file delle applicazioni o determinate estensioni che ritieni essere pericolose. Controllare tutti i file ti garantisce una protezione migliore, mentre controllare solo le applicazioni può essere utile per eseguire una scansione più veloce.

  Nota
  I file delle applicazioni sono più vulnerabili agli attacchi dei malware rispetto ad altri tipi di file. Per maggiori informazioni, fai riferimento a «Tipi di file applicazioni» (p. 458).

  Se vuoi che siano esaminate solo determinate estensioni, seleziona **Estensioni personalizzate** nel menu e poi inserisci le estensioni nel campo di modifica, premendo `Invio` dopo ciascuna estensione.

  Importante
  Gli agenti di sicurezza di Bitdefender installati su sistemi operativi Windows e Linux esaminano la maggior parte dei formati .ISO, ma non intraprendono alcuna azione su di essi.

Opzioni attività di scansione - Aggiungere estensioni personalizzate

- **Archivi.** Gli archivi contenenti file infetti non sono una minaccia immediata alla sicurezza del sistema. I malware possono colpire il sistema solo se il file infetto è estratto da un archivio ed eseguito senza aver attivato la protezione in tempo reale. Tuttavia, si consiglia di esaminare gli archivi per rilevare e rimuovere ogni potenziale minaccia, anche se non è immediata.

  Importante
  La scansione dei file archiviati incrementa la durata totale della scansione e richiede più risorse di sistema.

  – **Scansiona all'interno degli archivi.** Seleziona questa opzione se vuoi controllare i file archiviati per rilevare eventuali malware. Se decidi di utilizzare questa opzione, puoi configurare le seguenti opzioni di ottimizzazione:

    - **Limita dimensioni archivio a (MB).** Puoi impostare un limite massimo accettabile per le dimensioni degli archivi da esaminare. Seleziona la casella corrispondente e digita la dimensione massima dell'archivio (in MB).
    - **Profondità archivio massima (livelli).** Seleziona la casella corrispondente e scegli la dimensione massima dell'archivio nel menu. Per le migliori prestazioni, scegli il valore inferiore, mentre per la massima protezione, seleziona il valore maggiore.

  – **Scansiona archivi e-mail.** Seleziona questa opzione se desideri attivare la scansione dei file allegati ai messaggi e ai database di e-mail, tra cui formati di file come .eml, .msg, .pst, .dbx, .mbx, .tbb e altri.

Importante
La scansione degli archivi di e-mail richiede molte risorse e può influenzare le prestazioni del sistema.

- **Funzioni varie.** Seleziona le caselle corrispondenti per attivare le opzioni di scansione desiderate.
  - **Scansiona i settori di avvio.** Per esaminare i settori di avvio del sistema. Questo settore del disco rigido contiene il codice necessario per inizializzare il processo di avvio del computer. Quando un virus infetta il settore di boot, il disco potrebbe non essere accessibile e potrebbe non essere possibile avviare il sistema e accedere ai dati.
  - **Registro della scansione.** Seleziona questa opzione per controllare le chiavi del registro. Il registro di Windows è un database che memorizza le impostazioni e le opzioni di configurazione delle componenti del sistema operativo Windows, oltre a quelle delle applicazioni installate.
  - **Scansiona alla ricerca di rootkit.** Seleziona questa opzione per eseguire una scansione alla ricerca di rootkit e oggetti nascosti usando tale software.
  - **Scansiona per keylogger.** Seleziona questa opzione per eseguire una scansione alla ricerca di software keylogger.
  - **Scansiona condivisioni di rete.** Questa opzione esamina le unità di rete installate.

    Per le scansioni veloci, questa opzione è disattivata per impostazione predefinita. Per le scansioni complete, è attivata per impostazione predefinita. Per le scansioni personalizzate, se imposti il livello di sicurezza su **Aggressivo/Normale**, l'opzione **Controlla condivisioni di rete** è attivata automaticamente. Se imposti il livello di sicurezza su **Permissivo**, l'opzione **Controlla condivisioni di rete** è disattivata automaticamente.
  - **Scansiona memoria.** Seleziona questa opzione per controllare i programmi in esecuzione nella memoria di sistema.
  - **Scansiona i cookie.** Seleziona questa opzione per controllare i cookie memorizzati dai browser sul computer.

- **Scansiona solo file nuovi e modificati.** Controllando solo i file modificati o nuovi, potresti migliorare la prontezza generale del sistema, mantenendo un buon livello di sicurezza.
- **Esamina applicazioni potenzialmente non desiderate (PUA).** Un'applicazione potenzialmente indesiderata (PUA) è un programma che potrebbe essere indesiderato sul PC e a volte viene installato insieme a software freeware. Tali programmi possono essere installati senza il consenso dell'utente (vengono anche chiamati adware) o sono spesso inclusi in modo predefinito nei kit di installazione rapida (ad-supported). Gli effetti potenziali di questi programmi includono la visualizzazione di pop-up, l'installazione di barre degli strumenti non desiderate nel browser predefinito o l'esecuzione di vari processi in background con il conseguente rallentamento delle prestazioni del PC.
- **Esamina volumi rimovibili.** Seleziona questa opzione per esaminare qualsiasi unità di memorizzazione rimuovibile collegata all'endpoint.

- **Azioni.** In base al tipo di file rilevato, le seguenti azioni vengono intraprese automaticamente:
  - **Quando viene rilevato un file infetto.** Bitdefender rileva i file infetti attraverso diversi meccanismi avanzati, che includono tecnologie basate su firme dei malware, apprendimento automatico e intelligenza artificiale (IA). Normalmente, l'agente di sicurezza di Bitdefender può rimuovere il codice malware da un file infetto e ricostruire il file originale. Questa operazione è conosciuta come disinfezione.

    Di norma, se viene rilevato un file infetto, l'agente di sicurezza di Bitdefender tenterà di disinfettarlo automaticamente. Se la disinfezione dovesse fallire, il file sarà messo in quarantena per contenere l'infezione.

    Importante
    Per alcuni particolari tipologie di malware, non è possibile usare la disinfezione perché il file rilevato è interamente dannoso. In questi casi, il file infetto è eliminato dal disco.

- **Quando viene rilevato un file sospetto.** I file vengono rilevati come sospetti dall'analisi euristica e da altre tecnologie di Bitdefender. Queste forniscono un tasso di rilevazione elevato, ma in alcuni casi gli utenti devono fare attenzione a determinati falsi positivi (file puliti rilevati come sospetti). I file sospetti non possono essere disinfettati, perché non è disponibile alcuna routine di disinfezione.

  Le attività di scansione sono configurate in modo predefinito per ignorare i file sospetti. Potresti volere modificare l'azione predefinita in modo da mettere i file sospetti in quarantena. I file in quarantena vengono inviati regolarmente ai laboratori di Bitdefender per un'ulteriore analisi. Se viene confermata la presenza di malware, viene rilasciata una firma per consentirne la rimozione.

- **Quando viene individuato un rootkit.** I rootkit sono software specializzati che vengono usati per nascondere file al sistema operativo. Anche se non dannosi di natura, i rootkit sono spesso utilizzati per nascondere malware o celare la presenza di un intruso nel sistema.

  I rootkit rilevati e i file nascosti vengono ignorati per impostazione predefinita.

Anche se non consigliato, puoi modificare le azioni predefinite. Puoi specificare una seconda azione da intraprendere se la prima dovesse fallire, oltre a diverse azioni per ciascuna categoria. Scegli dai menu corrispondenti la prima e la seconda azione da intraprendere su ciascun tipo di file rilevato. Sono disponibili le seguenti opzioni:

Disinfetta
Rimuovi il codice malware dai file infetti. Si consiglia di impostarla sempre come prima azione da intraprendere sui file infetti.

Sposta i file in quarantena
Sposta i file rilevati dalla loro posizione originale alla cartella di quarantena. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Puoi gestire i file in quarantena dalla pagina Quarantena della console.

Elimina
Elimina i file rilevati dal disco, senza alcun avviso. È consigliabile evitare di usare questa azione.

Ignora
Nessuna azione verrà intrapresa sui file rilevati. Questi file appariranno solo nel registro della scansione.

– Vai alla scheda **Bersaglio** per configurare le posizioni che vuoi che vengano esaminate sugli endpoint di destinazione.

Nella sezione **Obiettivi scansione** puoi aggiungere un nuovo file o una nuova cartella da esaminare:

a. Scegli una posizione predefinita dal menu a discesa o inserisci i **Percorsi specifici** che vuoi esaminare.

b. Specifica il percorso dell'oggetto da esaminare nel campo di modifica.

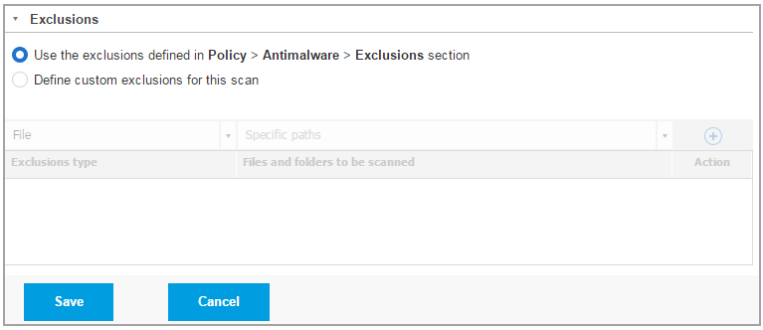
- Se hai scelto una posizione predefinita, completa il percorso come necessario. Per esempio, per esaminare l'intera cartella `Programmi`, è sufficiente selezionare la posizione predefinita e corrispondente dal menu a discesa. Per esaminare una determinata cartella in `Programmi`, devi completare il percorso aggiunto un backslash (\) e il nome della cartella.
- Se hai scelto **Percorsi specifici**, inserisci il percorso completo per l'oggetto da esaminare. È consigliabile utilizzare variabili di sistema (laddove appropriato) per assicurarsi che il percorso sia valido su tutti i computer di destinazione. Per maggiori informazioni sulle variabili di sistema, fai riferimento a «Variabili di sistema» (p. 460).

c. Clicca sul pulsante ⊕ **Aggiungi** corrispondente.

Per modificare una posizione esistente, cliccaci sopra. Per rimuovere una posizione dalla lista, clicca sul pulsante ⊗ **Elimina** corrispondente.

Per le attività di scansione della rete, devi inserire le credenziali di un account utente con permessi di lettura/scrittura sulle unità di rete obiettivo, in modo che l'agente di sicurezza possa accedere e intraprendere azioni su queste unità di rete.

Clicca sulla sezione **Eccezioni** se vuoi definire le eccezioni.



Attività di scansione - Definire le eccezioni

Per l'attività di scansione attuale, puoi utilizzare le eccezioni definite dalla policy oppure definire determinate eccezioni. Per maggiori dettagli sulle eccezioni, fai riferimento a «Eccezioni» (p. 180).

6. Clicca su **Salva** per creare l'attività di scansione. Apparirà un messaggio di conferma.

Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**. Per maggiori informazioni, fai riferimento a Visualizzare e gestire le attività.

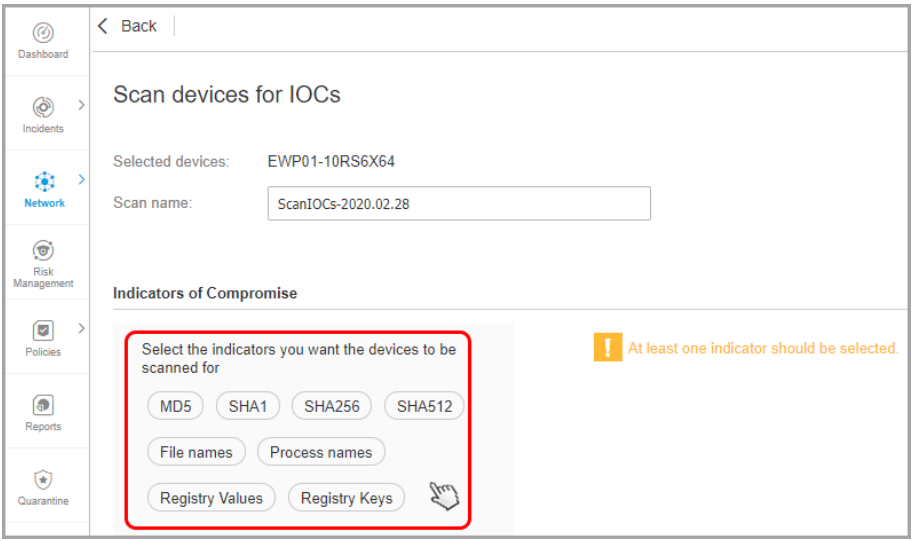
Nota
Per programmare un'attività di scansione, vai alla pagina **Policy**, seleziona la policy assegnata ai computer desiderati e aggiungi un'attività di scansione nella sezione **Antimalware > A richiesta**. Per maggiori informazioni, fai riferimento a «Su richiesta» (p. 162).

6.6.2. Scansione per IOC

Puoi scegliere in qualsiasi momento di eseguire una scansione a richiesta per indicatori di compromissione (IOC) noti sugli endpoint selezionati, nel seguente modo:

1. Vai alla pagina **Rete**.
2. Sfoglia i contenitori e seleziona gli endpoint che vuoi esaminare.
3. Clicca sul pulsante **Attività** e seleziona **Scansione per IOC**.

   Apparirà una pagina di configurazione, nella quale dovrai selezionare il tipo di indicatori da prendere in considerazione per la scansione per IOC.



Configurare un'attività di Scansione per IOC

Nota
Per creare un'attività valida, devi selezionare almeno un tipo di Indicatore di compromissione.

4. Seleziona uno o più tipi di IOC da considerare per la scansione e indica il nome di eventuali IOC noti nel campo appena aggiunto.

Aggiungere IOC

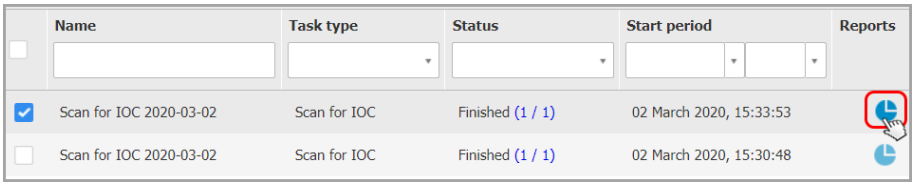
Puoi selezionarli tra queste tipologie:

- MD5
- SHA1
- SHA256
- SHA512
- Nomi dei file
- Nomi dei processi
- Valore del registro
- Chiavi di registro

Nota
I contenuti aggiunti in ciascun campo devono essere validi. Diversamente, riceverai un segnale e un messaggio di allerta.

5. Clicca su **Salva** per creare ed eseguire un'attività **Scansione per IOC**. Apparirà un messaggio di conferma.

   Puoi controllare i progressi dell'attività nella pagina **Rete/Attività**



Progressi dell'attività

6. Una volta terminata l'attività, puoi cliccare sul pulsante **Rapporti** per consultare il rapporto generato e determinare l'impatto della scansione per IOC.

Le estensioni dei file valide per gli IOC aggiunti all'attività sono: `exe`, `dll`, `com`, `scr`, `jar`, `msi`, `msc`, `bat`, `ps1`, `vbs`, `vbe`, `js`, `jse`, `wsf`, `wsh`, `psc1`, `lnk`, `doc`, `docx`, `docm`, `xls`, `xlsx`, `xlsm`, `ppt`, `pptx`, `pptm`, `eml`, `rtf`, `pdf`, `html`, `ppsx`, `pps`, `ppsm`, `pot`, `potx`, `potm`, `ocx`, `sys`, `fnr`, `fne` e `pif`.

L'attività **Scansione per IOC** esaminerà le seguenti posizioni:

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

Importante
Le attività di **Scansione per IOC** sugli endpoint non verranno eseguite/non verranno completate nei seguenti casi:

- L'endpoint non ha un sistema operativo Windows.
- La licenza dell'agente Bitdefender dell'endpoint non è valida.
- Il modulo **EDR** non è stato installato nel client di BEST presente sugli endpoint bersaglio.
- Più di 100 attività di **Scansione per IOC** attualmente in coda.
- Dati non validi inseriti dall'utente nella pagina di configurazione dell'attività di **Scansione per IOC**.

6.6.3. Scansione rischi

Puoi decidere in qualsiasi momento di eseguire attività di scansione dei rischi su richiesta sugli endpoint selezionati, nel seguente modo:

1. Vai alla pagina **Rete**.
2. Sfoglia i contenitori dal pannello a sinistra e seleziona gli endpoint da scansionare.

3. Clicca sul pulsante **Attività** e seleziona **Scansione per IOC**.

   Comparirà un messaggio che ti chiederà di confermare l'esecuzione dell'attività di scansione dei rischi.

   Nota
   L'attività di scansione dei rischi sarà eseguita con tutti gli indicatori di rischio attivati per impostazione predefinita.

4. Una volta completata l'attività con successo, puoi andare alla scheda Configurazioni errate della pagina **Rischi sicurezza**, analizzarli e scegliere quali indicatori ignorare, se necessario.

   Il punteggio di rischio globale dell'azienda sarà ricalcolato in base agli indicatori di rischio ignorati.

   Nota
   Per visualizzare l'elenco completo degli indicatori e la relativa descrizione, fai riferimento a questo articolo della KB.

Importante
Le attività di **Scansione dei rischi** sugli endpoint non verranno eseguite/non verranno completate nei seguenti casi:

- L'endpoint non ha un sistema operativo Windows.
- La licenza dell'agente Bitdefender dell'endpoint non è valida.
- Il modulo Gestione rischi è disattivato nella policy applicata all'endpoint.

Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**. Per maggiori informazioni, fai riferimento a Visualizzare e gestire le attività.

6.6.4. Attività di patch

Si consiglia di controllare regolarmente la presenza di aggiornamenti software e installarli il prima possibile. GravityZone automatizza questo processo tramite policy di sicurezza, ma se devi aggiornare il software su determinati endpoint, esegui le seguenti attività in quest'ordine:

1. Scansione patch
2. Installazione patch

Prerequisiti

- L'agente di sicurezza con il modulo Gestione patch viene installato sugli endpoint di destinazione.
- Affinché le attività di scansione e installazione abbiano successo, gli endpoint Windows devono soddisfare queste condizioni:
  - **Trusted Root Certification Authorities** conserva il certificato **DigiCert Assured ID Root CA**.
  - **Intermediate Certification Authorities** include il **DigiCert SHA2 Assured ID Code Signing CA**.
  - Gli endpoint devono aver installato le patch per Windows 7 e Windows Server 2008 R2 indicate in questo articolo di Microsoft: Microsoft Security Advisory 3033929

Scansione patch

Gli endpoint con software datato sono vulnerabili agli attacchi. Si consiglia di controllare regolarmente il software installato sugli endpoint e aggiornarlo il prima possibile. Per esaminare i tuoi endpoint per rilevare eventuali patch mancanti:

1. Vai alla pagina **Rete**.
2. Seleziona **Computer e Macchine Virtuali** dal selettore di visualizzazione.
3. Seleziona il contenitore desiderato dal pannello a sinistra. Tutti gli endpoint del contenitore selezionato sono mostrati nella tabella a destra.
4. Seleziona gli endpoint bersaglio.
5. Clicca sul pulsante **Attività** nel lato superiore della tabella e seleziona **Scansione patch**. Apparirà una finestra di conferma.
6. Clicca su **Sì** per confermare l'attività di scansione.

   Una volta completata l'attività, GravityZone aggiunge nell'Inventario delle patch, tutte le patch necessarie per il tuo software. Per maggiori dettagli, fai riferimento a «Inventario patch» (p. 65).

Nota
Per programmare una scansione delle patch, modifica le policy assegnate agli endpoint bersaglio e configura le impostazioni nella sezione **Gestione patch**. Per maggiori informazioni, fai riferimento a «Patch Management» (p. 223).

Installazione patch

Per installare una o più patch sugli endpoint bersaglio:

1. Vai alla pagina **Rete**.
2. Seleziona **Computer e Macchine Virtuali** dal selettore di visualizzazione.
3. Seleziona il contenitore desiderato dal pannello a sinistra. Tutti gli endpoint del contenitore selezionato sono mostrati nella tabella a destra.
4. Clicca sul pulsante **Attività** nel lato superiore della tabella e seleziona **Installa patch**.

   Apparirà la finestra di configurazione. Qui puoi visualizzare tutte le patch mancanti dagli endpoint bersaglio.
5. Se necessario, usa le opzioni di ordine e filtro nel lato superiore della tabella per trovare determinate patch.
6. Clicca sul pulsante **Colonne** nel lato superiore destro del pannello per visualizzare solo le informazioni importanti.
7. Seleziona le patch che vuoi installare.

   Alcune patch dipendono da altre. In tal caso, vengono selezionate automaticamente una volta con la patch.

   Cliccando sul numero di **CVE** o **Prodotti** comparirà un pannello nel lato sinistro. Il pannello include informazioni aggiuntive, come le CVE risolte dalla patch o i prodotti a cui la patch può essere applicata. Una volta finito di leggere, clicca su **Chiudi** per nascondere il pannello.
8. Seleziona **Se necessario, riavvia gli endpoint dopo aver installato la patch** per riavviare gli endpoint immediatamente dopo l'installazione della patch, se è necessario un riavvio del sistema. Nota che questa azione può interrompere l'attività degli utenti.
9. Clicca su **Installa**.

   Viene creata l'attività di installazione, insieme con le sotto-attività per ciascun endpoint bersaglio.

Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**. Per maggiori informazioni, fai riferimento a «Eseguire le attività» (p. 74).

Nota

- Per programmare l'impiego delle patch, modifica le policy assegnate agli endpoint bersaglio e configura le impostazioni nella sezione **Gestione patch**. Per maggiori informazioni, fai riferimento a «Patch Management» (p. 223).
- Puoi installare una patch anche dalla pagina **Inventario patch**, iniziando da una delle patch che ti interessano. In questo caso, seleziona la patch dall'elenco, clicca sul pulsante **Installa** nel lato superiore della tabella e configura i dettagli di installazione della patch. Per maggiori dettagli, fai riferimento a «Installare le patch» (p. 70).
- Dopo aver installato una patch, ti consigliamo di inviare un'attività Scansione patch agli endpoint di destinazione. In questo modo verranno aggiornate le informazioni sulle patch archiviate in GravityZone per le reti che gestisci.

Puoi disinstallare patch:

- Da remoto, inviando un'attività di disinstallazione patch da GravityZone.
- Localmente sull'endpoint. In questo caso, dovrai effettuare l'accesso come amministratore sull'endpoint ed eseguire l'applicazione di disinstallazione manualmente.

6.6.5. Scansione Exchange

Puoi esaminare in remoto il database di un Server Exchange eseguendo un'attività **Scansione Exchange**.

Per poter esaminare il database Exchange, devi attivare la scansione a richiesta fornendo le credenziali di un amministratore Exchange. Per maggiori informazioni, fai riferimento a «Scansione Store Exchange» (p. 241).

Per esaminare un database di un server Exchange:

1. Vai alla pagina **Rete**.
2. Dal pannello a sinistra, seleziona il gruppo contenente il server Exchange desiderato. Il server viene indicato nel pannello a destra.

Nota

In alternativa, puoi applicare dei filtri per trovare rapidamente il server desiderato:

- Clicca sul menu **Filtri** e seleziona le seguenti opzioni: **Gestito (Server Exchange)** dalla scheda **Sicurezza** e **Tutti gli elementi ricorsivamente** dalla scheda **Profondità**.

- Inserisci l'hostname o l'IP del server nei campi delle intestazioni delle colonne corrispondenti.

3. Seleziona la casella del Server Exchange di cui vuoi esaminare il database.
4. Clicca sul pulsante **Attività** nel lato superiore della tabella e seleziona **Scansione Exchange**. Apparirà la finestra di configurazione.
5. Configura le opzioni di scansione:
   - **Generale.** Inserisci un nome specifico per l'attività.

     Per i database maggiori, l'attività di scansione potrebbe richiedere molto tempo e influenzare le prestazioni del server. In questi casi, seleziona la casella **Ferma la scansione se impiega più di** e scegli un intervallo di tempo appropriato nei menu corrispondenti.
   - **Destinazione.** Scegli i contenitori e gli elementi da esaminare. Puoi scegliere di esaminare caselle di posta, cartelle pubbliche o entrambe. Oltre alle e-mail, puoi scegliere di esaminare altri oggetti, come **Contatti**, **Attività**, **Appuntamenti** e **Elementi pubblicati**. Inoltre, puoi impostare le seguenti restrizioni ai contenuti da sottoporre a scansione:
     – Solo messaggi non letti
     – Solo elementi con allegati
     – Solo nuovi elementi, ricevuti in un determinato intervallo di tempo

     Per esempio, puoi scegliere di esaminare solo le e-mail dalle caselle di posta dell'utente, ricevuti negli ultimi sette giorni.

     Seleziona la casella **Eccezioni**, se vuoi definire delle eccezioni per la scansione. Per creare un'eccezione, usa i campi nelle intestazioni della tabella nel seguente modo:
     a. Seleziona il tipo di archivio dal menu.
     b. In base al tipo di archivio, specifica l'elemento da escludere:

Tipo di archivio	Formato elemento
Casella di posta	Indirizzo e-mail
Cartella pubblica	Il percorso della cartella, a partire dalla radice
Base di dati	L'identità del database

Nota
Per ottenere l'identità del database, usa il comando shell di Exchange:
`Get-MailboxDatabase | fl name,identity`

Puoi inserire un solo elemento alla volta. Se hai diversi elementi dello stesso tipo, devi definire tante regole quante il numero di elementi.

c. Clicca sul pulsante ⊕ **Aggiungi** nel lato superiore della tabella per salvare l'eccezione e aggiungerla all'elenco.

Per rimuovere una regola di eccezione dall'elenco, clicca sul pulsante ⊖ **Elimina** corrispondente.

- **Opzioni.** Configura le opzioni di scansione per le e-mail che corrispondono alla regola:
  - **Tipi di file esaminati.** Usa questa opzione per specificare quali tipi di file vuoi che vengano esaminati. Puoi scegliere di esaminare tutti i file (indipendentemente dalla loro estensione), solo i file delle applicazioni o determinate estensioni che ritieni possano essere pericolose. Esaminare tutti i file ti garantisce la migliore protezione, mentre si consiglia di controllare solo le applicazioni per eseguire una scansione più veloce.

    Nota
    I file delle applicazioni sono più vulnerabili agli attacchi dei malware rispetto ad altri tipi di file. Per maggiori informazioni, fai riferimento a «Tipi di file applicazioni» (p. 458).

    Se vuoi esaminare solo i file con determinate estensioni, hai due alternative:
    - **Estensioni definite dall'utente**, dove devi fornire solo le estensioni da esaminare.
    - **Tutti i file, tranne determinate estensioni**, dove devi inserire solo le estensioni che la scansione deve ignorare.
  - **Dimensione massima allegati/corpo e-mail (MB).** Seleziona questa casella e inserisci un valore nel campo corrispondente per impostare la dimensione massima accettata di un file in allegato o del corpo dell'e-mail da esaminare.
  - **Profondità massima archivio (livelli).** Seleziona la casella e scegli la profondità massima dell'archivio nel campo corrispondente. Più il livello di profondità è basso, maggiori saranno le prestazioni e minore il grado di protezione.
  - **Esamina applicazioni potenzialmente non desiderate (PUA).** Seleziona questa casella per eseguire una scansione per possibili applicazioni dannose o non desiderate, come adware, che potrebbero essere installate sui sistemi senza il consenso dell'utente, modificare il comportamento di diversi prodotti software e ridurre le prestazioni del sistema.

- **Azioni.** Puoi specificare diverse azioni che l'agente di sicurezza può intraprendere automaticamente sui file, in base al tipo di rilevazione.

  Il tipo di rilevazione divide i file in tre categorie:
  - **File infetti.** Bitdefender rileva i file infetti attraverso diversi meccanismi avanzati, che includono tecnologie basate su firme dei malware, apprendimento automatico e intelligenza artificiale (IA).
  - **File sospetti.** Questi file vengono rilevati come sospetti dall'analisi euristica e da altre tecnologie di Bitdefender. Queste forniscono un tasso di rilevazione elevato, ma in alcuni casi gli utenti devono fare attenzione a determinati falsi positivi (file puliti rilevati come sospetti).
  - **File non esaminabili.** Questi file non possono essere esaminati. I file esaminabili includono, ma non solo, file protetti da password, cifrati o supercompressi.

  Per ogni tipo di rilevazione, hai un'azione predefinita o principale, e un'azione alternativa in caso di fallimento della principale. Anche se non consigliato, puoi modificare queste azioni nei menu corrispondenti. Scegli l'azione da intraprendere:
  - **Disinfetta.** Rimuove il codice malware dai file infetti e ricostruisce il file originale. Per alcuni particolari tipologie di malware, non è possibile usare la disinfezione perché il file rilevato è interamente dannoso. Si consiglia di impostarla sempre come prima azione da intraprendere sui file infetti. I file sospetti non possono essere disinfettati, perché non è disponibile alcuna routine di disinfezione.
  - **Respingi/Elimina e-mail.** Sui server con ruolo di Edge Transport, l'e-mail rilevata viene respinta con un codice di errore 550 SMTP. In tutti gli altri casi, l'e-mail viene eliminata senza alcun avviso. È consigliabile evitare di usare questa azione.
  - **Elimina file.** Elimina gli allegati con problemi senza alcun avviso. È consigliabile evitare di usare questa azione.
  - **Sostituisci file.** Elimina i file con problemi e inserisci un file di testo che avvisa l'utente delle azioni intraprese.
  - **Sposta file in quarantena.** Sposta i file rilevati nella cartella della quarantena e inserisce un file di testo che avvisa l'utente dell'azione intrapresa. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Puoi gestire i file in quarantena dalla pagina **Quarantena**.

Nota
Ti ricordiamo che la quarantena per Exchange Server richiede spazio su disco aggiuntivo nella partizione in cui l'agente di sicurezza viene installato. Lo spazio della quarantena dipende dal numero di oggetti memorizzati e dalla loro dimensione.

- **Non fare nulla.** Nessuna azione verrà intrapresa sui file rilevati. Questi file appariranno solo nel registro della scansione. Le attività di scansione sono configurate in modo predefinito per ignorare i file sospetti. Potresti volere modificare l'azione predefinita in modo da mettere i file sospetti in quarantena.
- Di norma, quando un'e-mail corrisponde all'applicazione di una regola, viene elaborata esclusivamente in conformità con la regola stessa, senza essere esaminata nuovamente per le altre regole. Se vuoi continuare il controllo in base alle altre regole, deseleziona la casella **Se le condizioni della regola vengono soddisfatte, blocca l'elaborazione di altre regole**.

6. Clicca su **Salva** per creare l'attività di scansione. Apparirà un messaggio di conferma.
7. Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**. Per maggiori informazioni, fai riferimento a Visualizzare e gestire le attività.

6.6.6. Installa

Per proteggere i tuoi endpoint con l'agente di sicurezza di Bitdefender, devi installarlo su ognuno di loro.

Una volta installato un agente relay, rileverà automaticamente eventuali endpoint non protetti nella stessa rete.

La protezione di Bitdefender può essere installata sugli agenti in remoto dalla Control Center.

L'installazione remota viene eseguita in background, senza che l'utente lo sappia.

Avvertimento
Prima dell'installazione, assicurati di disinstallare eventuali soluzioni antimalware e firewall esistenti dai computer. Installare la protezione di Bitdefender su un software di sicurezza esistente potrebbe influenzare la sua operatività e causare alcuni seri problemi al sistema. Windows Defender e Windows Firewall saranno disattivati automaticamente all'avvio dell'installazione.

Se vuoi impiegare l'agente di sicurezza su un computer con Bitdefender Antivirus for Mac 5.X, devi prima rimuovere quest'ultimo manualmente. Per dei passaggi di guida, fai riferimento a questo articolo della KB.
Impiegando un agente tramite un relay Linux, devono essere soddisfatte le seguenti condizioni:

- L'endpoint relay deve aver installato il pacchetto Samba (`smbclient`) in versione 4.1.0 o superiore, e il comando `net` binario per impiegare gli agenti Windows.

  Nota
  Il comando/binario `net` viene generalmente consegnato con i pacchetti samba-client e / o samba-common. In alcune distribuzioni Linux (come CentOS 7.4), il comando `net` viene installato unicamente quando si installa la suite completa di Samba (Common + Client + Server). Assicurati che il tuo endpoint relay abbia il comando `net` disponibile.

- Gli endpoint Windows bersaglio devono avere le opzioni Condivisione amministrativa e Condivisione rete attivate.
- Gli endpoint Linux e Mac bersaglio devono avere SSH attivate e il firewall disattivato.

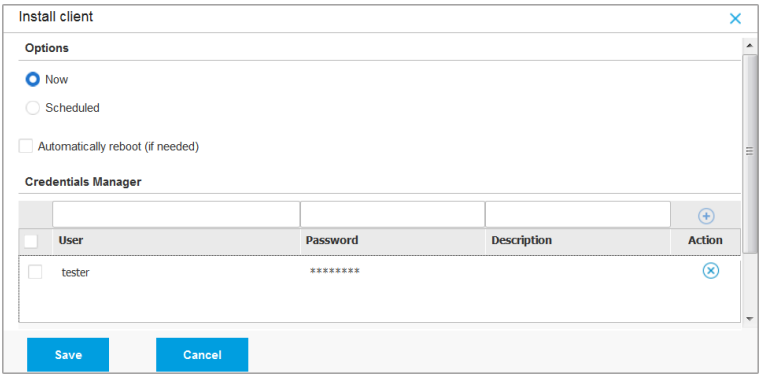
Per eseguire un'attività di installazione in remoto:

1. Connettiti e accedi alla Control Center.
2. Vai alla pagina **Rete**.
3. Seleziona il gruppo desiderato dal pannello sulla sinistra. Le entità contenute nel gruppo selezionato sono mostrate nel lato destro della tabella del pannello.

   Nota
   In alternativa, puoi applicare alcuni filtri per mostrare solo gli endpoint non gestiti. Clicca sul menu **Filtri** e seleziona le seguenti opzioni: **Non gestito** dalla scheda **Sicurezza** e **Tutti gli elementi ricorsivamente** dalla scheda **Profondità**.

4. Seleziona le entità (endpoint o gruppi di endpoint) su cui vuoi installare la protezione.
5. Clicca sul pulsante **Attività** nel lato superiore della tabella e seleziona **Installa**.

   Viene mostrata la procedura guidata **Installa client**.



Installare Bitdefender Endpoint Security Tools dal menu Attività

6. Nella sezione **Opzioni**, configura il momento dell'installazione:
   - **Ora**, per lanciare immediatamente l'impiego.
   - **Programmato**, per configurare l'intervallo di ricorrenza dell'impiego. In questo caso, seleziona l'intervallo di tempo che desideri (orario, giornaliero o settimanale) e configuralo in base alle tue necessità.

     Nota
     Per esempio, quando determinate operazioni sono necessarie sulla macchina bersaglio prima di installare il client (come disinstallare altri software e riavviare il SO), puoi programmare l'attività di impiego per essere eseguita ogni 2 ore. L'attività inizierà su ogni macchina bersaglio ogni 2 ore fin quando l'impiego non avrà successo.

7. Se vuoi che gli endpoint di destinazione vengano riavviati automaticamente per completare l'installazione, seleziona **Riavvio automatico (se necessario)**.
8. Nella sezione **Credentials Manager**, indica le credenziali amministrative richieste per l'autenticazione remota sugli endpoint di destinazione. Puoi aggiungere le credenziali, inserendo l'utente e la password per il sistema operativo di ogni bersaglio.

Importante
Per sistemi con Windows 8.1, devi fornire le credenziali dell'account da amministratore integrato o di un account amministratore del dominio. Per maggiori informazioni, fai riferimento a questo articolo della KB.

Per aggiungere le credenziali SO richieste:

a. Inserisci il nome utente e la password di un account amministratore nei campi corrispondenti dall'intestazione della tabella.

   Se i computer sono in un dominio, è sufficiente inserire le credenziali dell'amministratore del dominio.

   Usa le convenzioni di Windows nell'inserire il nome di un account utente:

   - Per le macchine Active Directory, utilizza queste sintassi: `username@domain.com` e `domain\username`. Per assicurare che le credenziali inserite funzioneranno, aggiungile in entrambi i moduli (`username@domain.com` e `domain\username`).
   - Per le macchine Workgroup, è sufficiente inserire solo il nome utente senza il nome del gruppo di lavoro.

   In alternativa, puoi aggiungere una descrizione che ti aiuterà a identificare ogni account più facilmente.

b. Clicca sul pulsante ⊕ **Aggiungi**. L'account è stato aggiunto all'elenco delle credenziali.

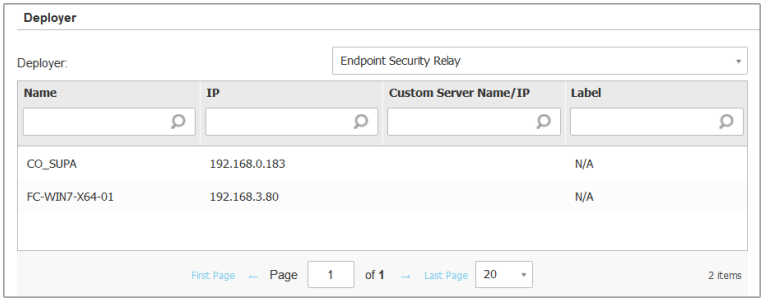
   Nota
   Le credenziali indicate vengono salvate automaticamente nel tuo Credentials Manager, in modo che non dovrai inserirle le prossime volte. Per accedere al Credentials Manager, punta al tuo nome utente nell'angolo in alto a destra della console.

   Importante
   Se le credenziali fornite non sono valide, l'impiego del client sugli endpoint corrispondenti non funzionerà. Assicurati di aggiornare le credenziali SO inserite nel Credentials Manager quando queste vengono modificate negli endpoint di destinazione.

9. Seleziona le caselle corrispondenti agli account che vuoi usare.

Nota
Viene visualizzato un messaggio di avviso finché non viene selezionata alcuna credenziale. Questo passaggio è obbligatorio per installare in remoto l'agente di sicurezza sugli endpoint.

10. Nella sezione **Gestore**, configura il relay a cui gli endpoint di destinazione si connetteranno per installare e aggiornare il client:
    - **Importante**
      Per funzionare, la porta 7074 deve essere aperta per l'impiego tramite l'agente relay.



11. Devi selezionare un pacchetto di installazione per l'impiego attuale. Clicca sull'elenco **Usa pacchetto** e seleziona il pacchetto di installazione che desideri. Qui puoi trovare tutti i pacchetti di installazione creati in precedenza per il tuo account e anche il pacchetto di installazione standard disponibile con la Control Center.
12. Se necessario, puoi modificare alcune delle impostazioni del pacchetto selezionato, cliccando sul pulsante **Personalizza** accanto al campo **Usa pacchetto**.

    Le impostazioni del pacchetto di installazione compariranno in basso e potrai effettuare le modifiche necessarie. Per scoprire altre informazioni sulla modifica dei pacchetti di installazione, fai riferimento alla Guida di installazione di GravityZone.

    Se vuoi salvare le modifiche come nuovo pacchetto, seleziona l'opzione **Salva come pacchetto** posizionata in fondo all'elenco delle impostazioni del pacchetto e inserisci un nome per il nuovo pacchetto di installazione.

13. Clicca su **Salva**. Apparirà un messaggio di conferma.

Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**.

Importante
Utilizzando VMware Horizon View Persona Management, si consiglia di configurare Active Directory Group Policy per escludere i seguenti processi di Bitdefender (senza il percorso completo):

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

Queste eccezioni devono essere applicate finché l'agente di sicurezza non viene eseguito sull'endpoint. Per maggiori dettagli, fai riferimento alla pagina della documentazione di VMware Horizon.

6.6.7. Fai l'upgrade del client

Questa attività è disponibile solo quando l'agente di Endpoint Security è installato e rilevato nella rete. Bitdefender consiglia di fare l'upgrade da Endpoint Security al nuovo Bitdefender Endpoint Security Tools, per una protezione per endpoint di ultima generazione.

Per trovare più facilmente i client che non hanno fatto l'upgrade, puoi generare un rapporto di stato di upgrade. Per maggiori dettagli su come creare i rapporti, fai riferimento a «Creare i rapporti» (p. 406).

6.6.8. Disinstalla client

Per disinstallare in remoto la protezione di Bitdefender:

1. Vai alla pagina **Rete**.
2. Seleziona il contenitore desiderato dal pannello a sinistra. Tutti gli endpoint del contenitore selezionato sono mostrati nella tabella a destra.
3. Seleziona le caselle degli endpoint da cui vuoi disinstallare l'agente di sicurezza di Bitdefender.

4. Clicca sul pulsante **Attività** nel lato superiore della tabella e seleziona **Disinstalla client**.
5. Viene mostrata una finestra di configurazione, che ti consente di scegliere se mantenere gli elementi in quarantena sulla macchina client.
6. Clicca su **Salva** per creare l'attività. Apparirà un messaggio di conferma.

   Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**. Per maggiori informazioni, fai riferimento a Visualizzare e gestire le attività.

Nota
Se vuoi reinstallare la protezione, assicurati di riavviare prima il computer.

6.6.9. Aggiorna client

Controlla regolarmente lo stato dei computer gestiti. Se noti un computer con problemi di sicurezza, clicca sul suo nome per mostrare la pagina **Informazioni**. Per maggiori informazioni, fai riferimento a «Stato sicurezza» (p. 43).

Client o contenuti di sicurezza non aggiornati rappresentano un problema per la sicurezza. In questi casi, devi eseguire un aggiornamento sul computer corrispondente. Questa attività può essere fatta localmente dal computer o in remoto dalla Control Center.

Per aggiornare in remoto il client e il contenuto di sicurezza sui computer gestiti:

1. Vai alla pagina **Rete**.
2. Seleziona il contenitore desiderato dal pannello a sinistra. Tutti gli endpoint del contenitore selezionato sono mostrati nella tabella a destra.
3. Seleziona le caselle degli endpoint in cui vuoi eseguire un aggiornamento del client.
4. Clicca sul pulsante **Attività** nel lato superiore della tabella e seleziona **Aggiorna**. Apparirà la finestra di configurazione.
5. Puoi scegliere di aggiornare solo il prodotto, solo il contenuto di sicurezza o entrambi.
6. Clicca su **Aggiorna** per eseguire l'attività. Apparirà un messaggio di conferma.

   Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**. Per maggiori informazioni, fai riferimento a Visualizzare e gestire le attività.

6.6.10. Riconfigura il client

Inizialmente, i moduli di protezione dell'agente di sicurezza, i ruoli e le modalità di scansione sono configurati nel pacchetto di installazione. Una volta installato l'agente di sicurezza nella tua rete, puoi modificare le impostazioni iniziali in qualsiasi momento, inviando un'attività remota **Riconfigura client** agli endpoint gestiti di tuo interesse.

Avvertimento
Ricordati che l'attività **Riconfigura client** sovrascriverà tutte le impostazioni di installazione e nessuna impostazione iniziale verrà mantenuta. Utilizzando questa attività, assicurati di riconfigurare tutte le impostazioni di installazione per gli endpoint di destinazione.

Nota
L'attività **Riconfigura il client** rimuoverà qualsiasi modulo non supportato dalle installazioni esistenti delle versioni meno recenti di Windows.

Puoi modificare le impostazioni di installazione dalla sezione **Rete** o dal rapporto **Stato moduli endpoint**.

Per modificare le impostazioni di installazione per uno o più endpoint:

1. Vai alla pagina **Rete**.
2. Seleziona il gruppo desiderato dal pannello a sinistra. Tutti gli endpoint del contenitore selezionato sono mostrati nella tabella a destra.
3. Seleziona le caselle degli endpoint per cui vuoi modificare le impostazioni di installazione.
4. Clicca sul pulsante **Attività** nel lato superiore della tabella e seleziona **Riconfigura client**.
5. Seleziona una delle seguenti azioni:
   - **Aggiungi**. Aggiungi nuovi moduli oltre a quelli esistenti.
   - **Rimuovi**. Rimuovi determinati moduli da quelli esistenti.
   - **Abbina elenco**. Abbina i moduli installati con la tua selezione.
6. Seleziona i moduli e i ruoli che intendi installare o rimuovere sugli endpoint bersaglio.

Avvertimento
Saranno installati solo i moduli supportati. Per esempio, Firewall si installa solo sulle workstation supportate di Windows.
Per maggiori informazioni, fai riferimento alla disponibilità dei livelli di protezione di GravityZone.

7. Seleziona **Rimuovi i concorrenti, se necessario** per assicurarti che i moduli selezionati non saranno in conflitto con altre soluzioni installate sugli endpoint bersaglio.
8. Seleziona una delle seguenti modalità di scansione:
   - **Automatica**. L'agente di sicurezza rileva quali motori di scansione sono adatti alle risorse dell'endpoint.
   - **Personalizzata**. Scegli direttamente quali motori di scansione usare.

     Per maggiori dettagli sulle opzioni disponibili, fai riferimento alla sezione Creare pacchetti di installazione della Guida di installazione.

     Nota
     Questa sezione è disponibile solo con **Abbina elenco**.

9. Nella sezione **Scheduler**, seleziona quando sarà eseguita l'attività:
   - **Ora**, per lanciare immediatamente l'attività.
   - **Programmato**, per configurare l'intervallo di ricorrenza dell'attività.

     In questo caso, seleziona l'intervallo di tempo (orario, giornaliero o settimanale) e configuralo in base alle tue esigenze.
10. Clicca su **Salva**. Apparirà un messaggio di conferma.

    Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**. Per maggiori informazioni, fai riferimento a Visualizzare e gestire le attività.

6.6.11. Ripara client

Usa l'attività Ripara client come attività iniziale di risoluzione dei problemi per qualsiasi numero di problemi degli endpoint. L'attività scarica il pacchetto di installazione più recente sull'endpoint bersaglio ed esegue una reinstallazione dell'agente.

Nota

- The modules currently configured on the agent will not be changed.
- L'attività di riparazione reimposterà l'agente di sicurezza alla versione Slow ring attuale.

Per inviare un'attività Ripara client al client:

1. Vai alla pagina **Rete**.
2. Seleziona il contenitore desiderato dal pannello a sinistra. Tutti gli endpoint del contenitore selezionato sono mostrati nella tabella a destra.
3. Seleziona le caselle degli endpoint in cui vuoi eseguire una riparazione del client.
4. Clicca sul pulsante **Attività** nel lato superiore della tabella e seleziona **Ripara client**. Apparirà una finestra di conferma.
5. Seleziona la casella **Ho compreso e accetto** e clicca sul pulsante **Salva** per eseguire l'attività.

   Nota
   Per completare l'attività di riparazione, potrebbe essere richiesto il riavvio del client.

   Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**. Per maggiori informazioni, fai riferimento a Visualizzare e gestire le attività.

6.6.12. Riavvia macchina

Puoi scegliere di riavviare in remoto gli endpoint gestiti.

Nota
Controlla la pagina **Rete > Attività** prima di riavviare determinati endpoint. Le attività create in precedenza potrebbero ancora essere elaborate sugli endpoint di destinazione.

1. Vai alla pagina **Rete**.
2. Seleziona il contenitore desiderato dal pannello a sinistra. Tutti gli endpoint del contenitore selezionato sono mostrati nella tabella a destra.
3. Seleziona le caselle di spunta degli endpoint che vuoi riavviare.

4. Clicca sul pulsante **Attività** nel lato superiore della tabella e seleziona **Riavvia macchina**.
5. Scegli l'opzione di pianificazione del riavvio:
   - Seleziona **Riavvia ora** per riavviare subito gli endpoint.
   - Seleziona **Riavvia alle** e usa i campi sottostanti per programmare il riavvio all'ora e alla data desiderate.
6. Clicca su **Salva**. Apparirà un messaggio di conferma.

   Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**. Per maggiori informazioni, fai riferimento a Visualizzare e gestire le attività.

6.6.13. Network Discovery

L'attività di Network discovery sarà eseguita automaticamente dagli agenti di sicurezza con ruolo di relay. Tuttavia, puoi eseguire manualmente l'attività di Network discovery dalla Control Center in qualsiasi momento, iniziando da qualsiasi macchina protetta da Bitdefender Endpoint Security Tools.

Per eseguire un'attività di Network discovery nella tua rete:

1. Vai alla pagina **Rete**.
2. Seleziona il contenitore desiderato dal pannello a sinistra. Tutti gli endpoint del contenitore selezionato sono mostrati nella tabella a destra.
3. Seleziona la casella di spunta dell'endpoint relay con cui vuoi eseguire l'attività di Network discovery.
4. Clicca sul pulsante **Attività** nel lato superiore della tabella e seleziona **Network Discovery**.
5. Apparirà un messaggio di conferma. Clicca su **Sì**.

   Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**. Per maggiori informazioni, fai riferimento a Visualizzare e gestire le attività.

6.6.14. Aggiorna Security Server

Puoi installare una appliance del Security Server solo scaricando il pacchetto di installazione del Security Server in una condivisione di rete o nell'host locale, impiegandolo manualmente sull'host. Una volta installato, il Security Server comparirà nella cartella **Gruppi personalizzati** appartenente alla sua rete. Puoi visualizzare i dettagli del Security Server cliccandoci sopra e mostrando la finestra

Informazioni. Per maggiori dettagli sull'installazione della appliance del Security Server, fai riferimento alla Guida di installazione di GravityZone.

Nota
La licenza del tuo prodotto potrebbe non includere questa funzionalità.

Se un Security Server è datato, puoi inviargli un'attività di aggiornamento:

1. Vai alla pagina **Rete**.
2. Seleziona il gruppo in cui è stato installato il Security Server.

   Per localizzare facilmente il Security Server, puoi utilizzare il menu **Filtri** come segue:

   - Vai alla scheda **Sicurezza** e seleziona solo **Server di sicurezza**.
   - Vai alla scheda **Profondità** e seleziona **Tutti gli elementi ricorsivamente**.
3. Clicca sul pulsante **Attività** nel lato superiore della tabella e seleziona **Aggiorna Security Server**.
4. Dovrai confermare la tua azione. Clicca su **Sì** per creare l'attività.

   Puoi visualizzare e gestire l'attività nella pagina **Rete > Attività**. Per maggiori informazioni, fai riferimento a Visualizzare e gestire le attività.

6.7.1. Integrazione con Active Directory

L'integrazione permette a GravityZone di importare l'inventario del computer da Active Directory in locale e da Active Directory eseguito su Microsoft Azure. In questo modo, puoi facilmente impiegare e gestire la protezione sugli endpoint di Active Directory. L'integrazione viene eseguita tramite un endpoint gestito chiamato Integratore di Active Directory.

Per gestire l'Integrazione di Active Directory:

- Impostare l'Integratore di Active Directory
- Rimuovi l'Integratore di Active Directory
- Rimuovi l'integrazione

Impostare l'Integratore di Active Directory

Puoi definire più integratori di Active Directory per lo stesso dominio e anche per ogni dominio disponibile.

Prerequisiti

L'Integratore di Active Directory deve soddisfare le seguenti condizioni:

- Funziona con un sistema operativo Windows.
- Si è unito ad Active Directory.
- È protetto da Bitdefender Endpoint Security Tools.
- È sempre online. Diversamente, potrebbe influenzare la sincronizzazione con Active Directory.

Importante
Si consiglia di connettere gli endpoint in Active Directory per assegnargli direttamente la policy. Tutti gli endpoint scoperti in un dominio Active Directory saranno spostati dalla loro cartella originale alla cartella Active Directory. In questo caso, se questi endpoint hanno una policy ereditata, verrà assegnata la policy impostata come predefinita.

Impostare l'Integratore di Active Directory

Puoi definire più integratori di Active Directory per lo stesso dominio e anche per ogni dominio disponibile.

Per impostare un endpoint come Integratore di Active Directory:

1. Vai alla pagina **Rete**.
2. Esplora l'inventario di rete fino al gruppo in cui si trova l'endpoint e selezionalo.

   Nota
   Se vuoi definire più integratori, devi selezionare un endpoint alla volta.

3. Clicca sul pulsante **Integrazioni** nel lato superiore della tabella e seleziona **Imposta come Integratore Active Directory**.
4. Conferma la tua azione cliccando su **Sì**.

   Puoi notare la nuova icona dell'endpoint che indica che si tratta di un Integratore di Active Directory. In un paio di minuti, potrai visualizzare lo schema di **Active Directory** accanto a **Computer e Gruppi**. Per le reti di Active Directory maggiori, la sincronizzazione potrebbe richiedere più tempo per essere completata. Gli endpoint connessi allo stesso dominio come Integratore di Active Directory passeranno da **Computer e Gruppi** al contenitore Active Directory.

Sincronizzare con Active Directory

GravityZone si sincronizza automaticamente con Active Directory ogni ora.

GravityZone non è in grado di sincronizzarsi con un dominio di Active Directory, se si verificano le seguenti condizioni:

- Tutti i ruoli di Integratore di Active Directory sono stati rimossi
- Connessione persa tra gli Integratori di Active Directory e GravityZone per almeno 2 ore.
- Nessuno degli Integratori di Active Directory dello stesso dominio può comunicare con il Domain Controller.

In uno di questi casi, si attiverà un problema di Active Directory nell'**area delle notifiche**. Per maggiori informazioni, fai riferimento a «Notifiche» (p. 436).

Rimuovi l'Integratore di Active Directory

Per rimuovere il ruolo di Integratore di Active Directory da un endpoint:

1. Vai alla pagina **Rete**.
2. Esplora l'inventario di rete fino al gruppo in cui si trova l'Integratore di Active Directory e selezionalo.

   Nota
   Se vuoi rimuovere più integratori, devi selezionare un endpoint alla volta.

3. Clicca sul pulsante **Integrazioni** nel lato superiore della tabella e seleziona **Rimuovi Integratore Active Directory**.
4. Apparirà un messaggio di conferma.
   - Se non c'è un altro endpoint con ruolo di Integratore di Active Directory nello stesso dominio, il messaggio di conferma avviserà anche che l'attuale dominio non sarà più sincronizzato con GravityZone.
   - Se l'endpoint è offline, il ruolo di Integratore di Active Directory sarà rimosso dopo che sarà stato attivato.

Puoi verificare se un Integratore di Active Directory è stato rimosso dalla tua rete gestita nella sezione **Attività utente**, filtrando i registri utente con i seguenti criteri:

- **Area**: Active Directory

- **Azione**: rimosso Integratore AD

Per maggiori informazioni, fai riferimento a «Rapporto attività utente» (p. 433).

Rimuovi l'integrazione di Active Directory

Puoi scegliere di rimuovere uno o più domini dalla cartella di Active Directory, come segue:

1. Vai alla pagina **Rete**.
2. Nello schema **Rete** dal pannello a sinistra, seleziona la cartella **Active Directory**.
3. Vai al pannello a destra e seleziona la cartella del dominio che vuoi rimuovere.
4. Clicca sul pulsante **Integrazioni** nel lato superiore della tabella e seleziona **Rimuovi Integrazione Active Directory**.
5. Apparirà un messaggio di conferma. Un'opzione disponibile con questo messaggio ti consente di scegliere se vuoi eliminare gli endpoint gestiti dall'inventario di rete oppure no. Fai attenzione, di norma, questa opzione è attivata. Clicca su **Conferma** per procedere.
6. Tutti gli endpoint nel dominio selezionato saranno posizionati nella cartella **Computer e Gruppi** (o i loro gruppi originali) e il ruolo Integratore di Active Directory sarà rimosso dagli endpoint assegnati di questo dominio.

6.8. Creare rapporti veloci

Puoi scegliere di creare rapporti istantanei sugli endpoint gestiti partendo dalla pagina **Rete**:

1. Vai alla pagina **Rete**.
2. Seleziona il gruppo che desideri dal pannello a sinistra. Tutti gli endpoint del gruppo selezionato vengono mostrati nella tabella del pannello a destra.

   In alternativa, puoi filtrare i contenuti del gruppo selezionato solo dagli endpoint gestiti.
3. Seleziona le caselle di spunta dei computer che vuoi includere nel rapporto.
4. Clicca sul pulsante **Rapporto** nel lato superiore della tabella e seleziona il tipo di rapporto nel menu.

   Per maggiori informazioni, fai riferimento a «Rapporti per computer e virtual machine» (p. 389).

5. Configura le opzioni del rapporto. Per maggiori informazioni, fai riferimento a «Creare i rapporti» (p. 406).
6. Clicca su **Genera**. Il rapporto viene mostrato immediatamente.

   Il tempo necessario per la creazione dei rapporti può variare in base al numero di endpoint selezionati.

6.9. Assegnare le policy

Puoi gestire le impostazioni di sicurezza sugli endpoint utilizzando le policy.

Dalla pagina **Rete** puoi visualizzare, modificare e assegnare le policy per ciascun endpoint o gruppo di endpoint.

Nota
Le impostazioni di sicurezza sono disponibili solo per gli endpoint gestiti. Per visualizzare e gestire più facilmente le impostazioni di sicurezza, puoi filtrare l'inventario di rete solo per gli endpoint gestiti.

Per visualizzare la policy assegnata a un particolare endpoint:

1. Vai alla pagina **Rete**.
2. Seleziona il gruppo desiderato dal pannello a sinistra. Tutti gli endpoint del gruppo selezionato sono mostrati nella tabella a destra.
3. Clicca sul nome dell'endpoint gestito che ti interessa. Apparirà una finestra di informazioni.
4. Nella scheda **Generale**, nella sezione **Policy**, clicca sul nome della policy attuale per visualizzare le sue impostazioni.
5. Puoi cambiare le impostazioni di sicurezza in base a ogni necessità, a condizione che il proprietario della policy abbia consentito ad altri utenti di effettuare cambiamenti a tale policy. Nota che qualsiasi modifica effettuata influenzerà tutti gli endpoint a cui è stata assegnata la stessa policy.

   Per maggiori informazioni sulle impostazioni di cambio della policy, fai riferimento a «Policy per computer e virtual machine» (p. 135).

Per assegnare una policy a un computer o un gruppo:

1. Vai alla pagina **Rete**.
2. Seleziona il gruppo desiderato dal pannello a sinistra. Tutti gli endpoint del gruppo selezionato sono mostrati nella tabella a destra.

3. Seleziona la casella di spunta dell'endpoint o del gruppo che desideri. Puoi selezionare uno o più elementi dello stesso tipo solo dallo stesso livello.
4. Clicca sul pulsante **Aggiungi policy** nel lato superiore della tabella.
5. Effettua le impostazioni necessarie nella finestra **Assegnazione della policy**. Per maggiori informazioni, fai riferimento a «Assegnare le policy» (p. 126).

6.10.1. Utilizzare Recovery manager per i volumi cifrati

Se gli utenti dell'endpoint dimenticano le proprie password di cifratura e non possono più accedere ai volumi cifrati nelle loro macchine, puoi aiutarli recuperando le chiavi di ripristino dalla pagina **Rete**.

Per recuperare un codice di ripristino:

1. Vai alla pagina **Rete**.
2. Clicca sul pulsante **Recovery manager** nella barra degli strumenti nel riquadro a sinistra. Comparirà una nuova finestra.
3. Nella sezione **Identificatore** della finestra, inserisci i seguenti dati:
   a. L'ID della chiave di ripristino del volume cifrato. L'ID della chiave di ripristino è una sequenza di numeri e lettere disponibile nell'endpoint, nella schermata di ripristino di BitLocker.

      In Windows, l'ID della chiave di ripristino è una sequenza di numeri e lettere disponibile nell'endpoint, nella schermata di ripristino di BitLocker.

      In alternativa, puoi usare l'opzione **Ripristino** nella scheda **Protezione** dei dettagli del computer per inserire automaticamente l'ID della chiave di ripristino, sia per endpoint Windows che macOS.
   b. La password del tuo account di GravityZone.
4. Clicca su **Rivela**. La finestra si espande.

   Nelle **Informazioni sul volume**, ti vengono presentati i seguenti dati:
   a. Nome del volume
   b. Tipo di volume (avviabile o non avviabile).
   c. Nome dell'endpoint (come indicato nell'inventario di rete)
   d. Chiave di ripristino. Su Windows, la chiave di ripristino è una password generata automaticamente quando il volume è stato cifrato. Su Mac, la chiave di ripristino è in realtà la password dell'account utente.

5. Invia la chiave di ripristino all'utente dell'endpoint.

Per dettagli sulla cifratura e decifratura dei volumi con GravityZone, fai riferimento a «Cifratura» (p. 263).

6.11. Assegnare Security Server

Come Fornitore di servizi, puoi offrire ai tuoi clienti con poche risorse la possibilità di scaricare la scansione dai loro endpoint, condividendo i tuoi Security Server con loro. Queste aziende devono avere la licenza mensile. Puoi condividere o assegnare uno o più Security Server a una o più aziende alla volta.

Per assegnare Security Server:

1. Vai alla pagina **Rete**.
2. Apri la cartella **Aziende** nel pannello a sinistra.
3. Nel lato destro, seleziona le aziende con cui vuoi condividere i Security Server.
4. Clicca sul pulsante **Assegna Security Servers** nel lato superiore della tabella. Puoi anche assegnare un Security Server cliccando con il pulsante destro del mouse su un'azienda bersaglio e selezionando questa opzione dal menu contestuale.

   Comparirà una finestra di configurazione, che mostra i Security Server installati nella tua rete e le aziende selezionate.
5. Seleziona i Security Server da assegnare.

   Per ciascuna azienda, puoi visualizzare i Security Server già assegnati. Nel caso in cui i Security Server fossero già stati assegnati e vuoi continuare a usarli, seleziona tutti i bersagli selezionati che hanno lo stesso Security Server assegnato e assicurati di selezionare anche gli stessi Security Server. Se l'assegnazione non è omogenea, potresti riconsiderare di fare un'altra selezione dei bersagli. L'assegnazione attuale sovrascriverà tutte le assegnazioni precedenti nei bersagli selezionati. Per esempio, hai i Security Server SS1e SS2, e le aziende C1 e C2. Il Security Server SS1 è stato assegnato all'azienda C1. Assegna SS2 a entrambe le aziende. Dopo questa nuova assegnazione, C1 non avrà più SS1 assegnato.
6. Clicca su **Termina**.

   Poi, le aziende bersaglio possono iniziare a usare i Security Server condivisi con loro, nei pacchetti di installazione e nelle policy antimalware.

Per revocare un Security Server da un'azienda, assegna gli stessi Security Server, tranne quello che vuoi revocare.

Importante
Revocando un Security Server da un'azienda, lo eliminerai anche dalle policy esistenti di quell'azienda.

6.12. Eliminare gli endpoint dall'inventario di rete

Di norma, l'inventario di rete include la cartella **Eliminati** , creata per memorizzare gli endpoint che non desideri gestire.

L'azione **Elimina** ha i seguenti effetti:

- Quando gli endpoint non gestiti vengono eliminati, vengono spostati direttamente nella cartella **Eliminati**.
- Quando gli endpoint gestiti vengono eliminati:
  - Viene creata un'attività di disinstallazione client
  - Viene rilasciato un posto della licenza
  - Gli endpoint vengono spostati nella cartella **Eliminati**

Per eliminare gli endpoint dall'inventario di rete:

1. Vai alla pagina **Rete**.
2. Nel pannello di sinistra, seleziona il gruppo di rete che ti interessa.

   Nota
   Puoi eliminare solo endpoint mostrati in **Computer e gruppi**, che sono rilevati esternamente a ogni infrastruttura di rete integrata.

3. Nel pannello di destra, seleziona la casella dell'endpoint che desideri eliminare.
4. Clicca sul pulsante ⊖ **Elimina** nel lato superiore della tabella. Dovrai confermare la tua azione cliccando su **Sì**.

   Se l'endpoint eliminato è gestito, sarà creata un'attività **Disinstalla client** nella pagina **Attività**, e l'agente di sicurezza sarà disinstallato dall'endpoint, rilasciando un posto della licenza.
5. L'endpoint viene spostato nella cartella **Eliminati**.

Puoi spostare gli endpoint in qualsiasi momento dalla cartella **Eliminati** in **Computer e Gruppi**, utilizzando la funzione trascina e rilascia.

Nota

- Se vuoi escludere in modo permanente alcuni endpoint dalla gestione, devi mantenerli nella cartella **Eliminati**.
- Se elimini gli endpoint dalla cartella **Eliminati**, saranno completamente rimossi dal database di GravityZone. Tuttavia, gli endpoint esclusi che sono online saranno rilevati con la prossima attività di Network Discovery e compariranno nell'inventario di rete come nuovi endpoint.

6.13. Visualizzare e gestire le attività

La pagina **Rete > Attività** ti consente di visualizzare e gestire tutte le attività che hai creato.

Una volta creata un'attività per uno di vari elementi di rete, puoi visualizzarla nella tabella delle attività.

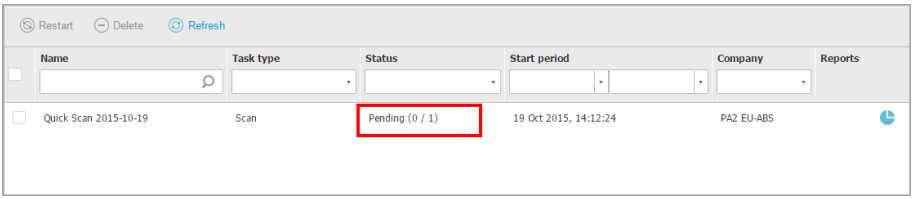
Nella pagina **Rete > Attività** puoi fare le seguenti operazioni:

- Controllare lo stato dell'attività
- Visualizzare i rapporti dell'attività
- Attività riavvio
- Fermare le attività di scansione di Exchange
- Elimina attività

6.13.1. Controllare lo stato dell'attività

Ogni volta che crei un'attività per uno o più elementi della rete, vorrai controllare i suoi progressi ed essere avvisato quando si verifica un errore.

Vai alla pagina **Rete > Attività** e controlla la colonna **Stato** per ogni attività che ti interessa. Puoi verificare lo stato dell'attività principale e puoi anche ottenere informazioni dettagliate su ogni sotto-attività.



La pagina Attività

- **Controllare lo stato dell'attività principale**.

  L'attività principale riguarda l'azione avviata su elementi di rete (come installare client o scansioni) e include un certo numero di sotto-attività, una per ciascun elemento di rete selezionato. Per esempio, un'attività di installazione principale creata per otto computer include otto sotto-attività. I numeri tra parentesi rappresentano il tasso di completamento delle sotto-attività. Per esempio, (2/8) significa che due sotto-attività su otto sono state completate.

  Lo stato dell'attività principale può essere:
  - **In sospeso**, quando nessuna sotto-attività è ancora iniziata.
  - **In corso**, quando tutte le sotto-attività sono in esecuzione. Lo stato dell'attività principale resta "In corso" fino al completamento della sotto-attività.
  - **Completata**, quando tutte le sotto-attività sono state completate (con successo oppure no). In caso di sotto-attività fallita, viene mostrato un simbolo di avvertimento.

- **Controllare lo stato delle sotto-attività**.

  Vai all'attività a cui sei interessato e clicca sul link disponibile nella colonna **Stato** per aprire la finestra **Stato**. Puoi visualizzare l'elenco degli elementi di rete assegnati con l'attività principale e lo stato della sotto-attività corrispondente. Lo stato della sotto-attività può essere:

  - **In corso,** quando la sotto-attività è ancora in esecuzione.

    Inoltre, per le attività di scansione a richiesta di Exchange, puoi visualizzare anche lo stato di completamento.

  - **Completata**, quando la sotto-attività è stata completata con successo.

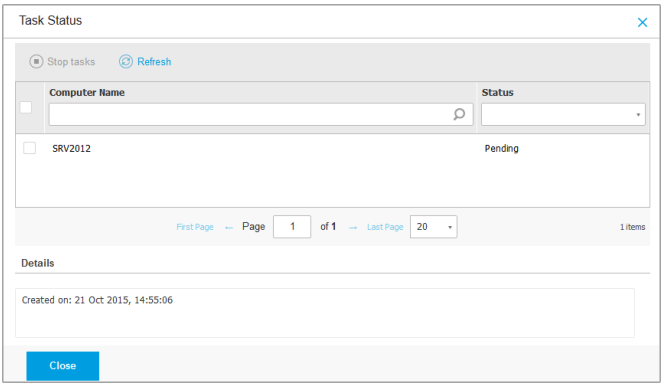
  - **In sospeso**, quando la sotto-attività non è ancora iniziata. Ciò può succedere nelle seguenti situazioni:

- La sotto-attività sta aspettando in una coda.
- Ci sono problemi di connettività tra la Control Center e l'elemento di rete desiderato.

– **Fallita**, quando la sotto-attività potrebbe non essere stata avviata oppure è stata interrotta a causa di errori, come credenziali di autenticazione errate e poco spazio di memoria.

– **In fase di arresto**, quando la scansione a richiesta sta impiegando troppo tempo per terminare e hai scelto di arrestarla.

Per visualizzare i dettagli di ciascuna sotto-attività, selezionala e verifica la sezione **Dettagli** sul fondo della tabella.



Dettagli stato attività

Otterrai informazioni relative a:

– Data e ora dell'inizio dell'attività.

– Data e ora del termine dell'attività.

– Descrizione degli errori riscontrati.

6.13.2. Visualizzare i rapporti dell'attività

Nella pagina **Rete > Attività**, hai l'opzione per visualizzare i rapporti delle attività della scansione veloce.

1. Vai alla pagina **Rete > Attività**.

2. Seleziona la casella corrispondente per l'attività di scansione che ti interessa.
3. Clicca sul pulsante corrispondente dalla colonna **Rapporti**. Attendi fino alla visualizzazione del rapporto. Per maggiori informazioni, fai riferimento a «Utilizzare i rapporti» (p. 388).

6.13.3. Riavviare le attività

Per diversi motivi, le attività di installazione, disinstallazione o aggiornamento potrebbero non essere completate. Puoi scegliere di riavviare tali attività fallite invece di crearne delle nuove, seguendo questi passaggi:

1. Vai alla pagina **Rete > Attività**.
2. Seleziona le caselle di spunta corrispondenti alle attività fallite.
3. Clicca sul pulsante **Riavvia** nel lato superiore della tabella. Le attività selezionate saranno riavviate e lo stato delle attività cambierà in **Nuovo tentativo**.

Nota
Per le attività con più sotto-attività, l'opzione **Riavvia** è disponibile solo quando tutte le sotto-attività sono state completate ed eseguirà solo le sotto-attività fallite.

6.13.4. Fermare le attività di scansione di Exchange

Esaminare lo Store di Exchange potrebbe richiedere una considerevole quantità di tempo. Se per un qualche motivo, desideri fermare la scansione a richiesta di Exchange, segui i passaggi qui indicati:

1. Vai alla pagina **Rete > Attività**.
2. Clicca sul link nella colonna **Stato** per aprire la finestra **Stato attività**.
3. Seleziona la casella di spunta corrispondente alle sotto-attività in sospeso o in esecuzione che vuoi arrestare.
4. Clicca sul pulsante **Ferma attività** nel lato superiore della tabella. Dovrai confermare la tua azione cliccando su **Sì**.

Nota
Puoi anche fermare una scansione a richiesta dello Store di Exchange dall'area degli eventi di Bitdefender Endpoint Security Tools.

6.13.5. Eliminare le attività

GravityZone elimina automaticamente le attività in sospeso dopo due giorni, e quelle completate dopo 30 giorni. Se hai ancora molte attività, ti consigliamo di eliminare le attività che non ti servono più, per evitare di ingombrare la lista.

1. Vai alla pagina **Rete > Attività**.
2. Seleziona la casella di spunta corrispondente all'attività che vuoi eliminare.
3. Clicca sul pulsante ⊖ **Elimina** nel lato superiore della tabella. Dovrai confermare la tua azione cliccando su **Sì**.

Avvertimento
Eliminare un'attività in sospeso annullerà anche l'attività.
Se un'attività in corso viene eliminata, ogni sotto-attività in sospeso sarà annullata. In questo caso, tutte le sotto-attività completate non possono essere annullate.

6.14. Configurare le impostazioni di rete

Nella pagina **Configurazione e Impostazioni di rete**, puoi configurare le impostazioni relative all'Inventario di rete, come salvataggio dei filtri, mantenimento dell'ultima posizione esplorata, creazione e gestione delle regole pianificate per l'eliminazione delle virtual machine non utilizzate.

Le opzioni sono organizzate nelle seguenti sezioni:

- Impostazioni Inventario di rete
- Pulizia macchine offline

6.14.1. Impostazioni Inventario di rete

Nella sezione **Impostazioni Inventario di rete**, sono disponibili le seguenti opzioni:

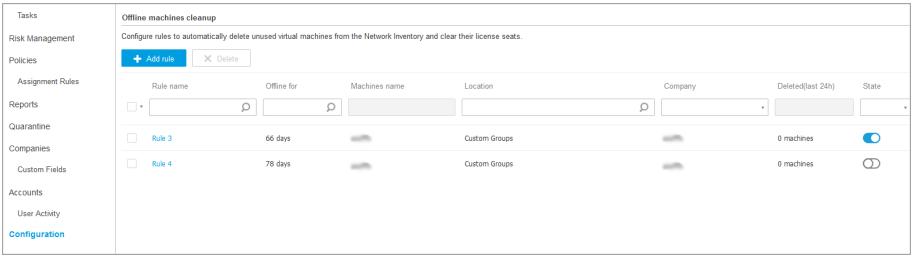
- **Salva filtri Inventario di rete**. Seleziona questa casella per salvare i tuoi filtri nella pagina **Rete** tra le sessioni di Control Center.
- **Ricorda l'ultima posizione esplorata nell'inventario di rete fino alla mia uscita**. Seleziona questa casella per salvare l'ultima posizione a cui hai avuto accesso quando hai lasciato la pagina **Rete**. La posizione non è stata salvata tra le sessioni.
- **Evita duplicati degli endpoint clonati**. Seleziona questa opzione per attivare un nuovo tipo di elementi di rete in GravityZone, chiamati golden image. In questo

modo è possibile differenziare gli endpoint di origine dai propri cloni. In seguito, è necessario contrassegnare ciascun endpoint che cloni nel seguente modo:

1. Vai alla pagina **Rete**.
2. Seleziona l'endpoint che vuoi clonare.
3. Dal suo menu contestuale, seleziona **Marca come golden image**.

6.14.2. Pulizia macchine offline

Nella sezione **Pulizia macchine offline**, puoi configurare le regole per l'eliminazione automatica delle virtual machine non utilizzate dall'inventario di rete.



Configurazione - Impostazioni di rete - Pulizia macchine offline

Creare Regole

Per creare una regola di pulizia:

1. Nella sezione **Pulizia macchine offline**, clicca sul pulsante della regola **Aggiungi**.
2. Nella pagina di configurazione:
   a. Inserisci un nome della regola.
   b. Seleziona un'ora per la pulizia quotidiana.
   c. Definisci i criteri di pulizia:
      - Il numero di giorni in cui le macchine sono state offline (da 1 a 90).
      - Un modello di nome, che può essere applicato a una singola o più virtual machine.

Per esempio, usa `machine_1` per eliminare la macchina con questo nome. In alternativa, aggiungi `machine_*` per eliminare tutte le macchine il cui nome inizia con `machine_`.

Il campo è sensibile all'uso delle maiuscole e accetta solo lettere, numeri e i caratteri speciali asterisco (*), trattino basso (_) e trattino (-). Il nome non può iniziare con un asterisco (*).

- L'azienda in cui si trovano le virtual machine. Usa il menu a discesa per effettuare una scelta.

d. Seleziona i gruppi bersaglio di endpoint nell'inventario di rete, dove applicare la regola.

3. Clicca su **Salva**.

Visualizzare e gestire le regole

La sezione **Impostazioni di rete > Pulizia macchine offline** mostra tutte le regole che hai creato. Una tabella dedicata ti fornisce i seguenti dettagli:

- Nome della regola.
- Il numero di giorni trascorsi da quando le macchine sono offline.
- Modello del nome delle macchine.
- Posizione nell'inventario di rete.
- Nome azienda.
- Il numero di macchine eliminate nelle ultime 24 ore.
- Stato: attivato, disattivato o non valido.

Nota
Una regola non è valida quando i bersagli non sono più validi, a causa di determinati motivi. Per esempio, le virtual machine sono state eliminate o non vi puoi più accedere.

Una regola di nuova creazione viene attivata in maniera predefinita. Puoi attivare e disattivare le regole in qualsiasi momento usando l'interruttore Sì/No nella colonna **Stato**.

La tabella mostra le regole esistenti per l'azienda selezionata. Per visualizzare le regole per un'altra azienda, usa il menu a discesa nella colonna **Azienda** per effettuare una selezione diversa.

Se necessario, usa le opzioni di ordine e filtro nel lato superiore della tabella per trovare determinate regole.

Per modificare una regola:

1. Clicca sul nome della regola.
2. Nella pagina di configurazione, modifica i dettagli della regola.
3. Clicca su **Salva**.

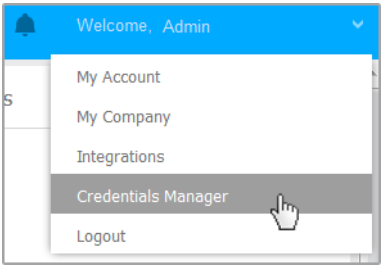
Per eliminare una o più regole:

1. Usa le caselle per selezionare una o più regole.
2. Clicca sul pulsante **Elimina** nel lato superiore della tabella.

6.15. Credentials Manager

Il Credentials Manager ti aiuta a definire le credenziali richieste per l'autenticazione remota su diversi sistemi operativi nella tua rete.

Per aprire il Credentials Manager, clicca sul tuo nome utente nell'angolo in alto a destra della pagina e seleziona **Credentials Manager**.

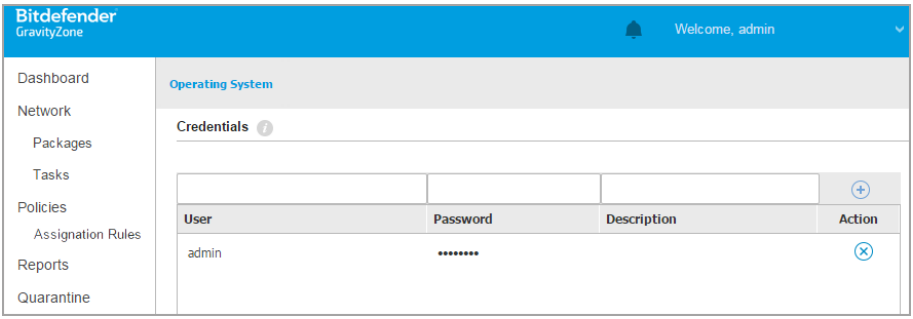


Il menu Credentials Manager

6.15.1. Aggiungere credenziali al Credentials Manager

Con il Credentials Manager puoi gestire le credenziali amministrative richieste per l'autenticazione remota durante le attività di installazione inviate ai computer e alle macchine virtuali nella tua rete.

Per aggiungere un set di credenziali:



Credentials Manager

1. Inserisci il nome utente e la password di un account da amministratore per ciascun sistema operativo bersaglio nei campi corrispondenti nella parte superiore dell'intestazione della tabella. In alternativa, puoi aggiungere una descrizione che ti aiuterà a identificare ogni account più facilmente. Se i computer sono in un dominio, è sufficiente inserire le credenziali dell'amministratore del dominio.

   Usa le convenzioni di Windows nell'inserire il nome di un account utente:

   - Per le macchine Active Directory, utilizza queste sintassi: `username@domain.com` e `domain\username`. Per assicurare che le credenziali inserite funzioneranno, aggiungile in entrambi i moduli (`username@domain.com` e `domain\username`).
   - Per le macchine Workgroup, è sufficiente inserire solo il nome utente senza il nome del gruppo di lavoro.

2. Clicca sul pulsante ⊕**Aggiungi** nel lato destro della tabella. Il nuovo set di credenziali viene aggiunto alla tabella.

> **Nota**
> Se non hai specificato le credenziali di autenticazione, ti sarà richiesto di inserirle all'esecuzione delle attività di installazione. Le credenziali indicate vengono salvate automaticamente nel tuo Credentials manager, in modo che non dovrai inserirle le prossime volte.

6.15.2. Eliminare le credenziali dal Credentials Manager

Per eliminare credenziali obsolete dal Credentials Manager:

1. Cerca la riga nella tabella contenente le credenziali che vuoi eliminare.
2. Clicca sul pulsante ⊗ **Elimina** sul lato destro della corrispondente riga della tabella. L'account selezionato sarà eliminato.

7. POLICY DI SICUREZZA

Una volta installata, la protezione di Bitdefender può essere configurata e gestita dalla Control Center usando le policy di sicurezza. Una policy specifica le impostazioni di sicurezza da applicare ai computer.

Immediatamente dopo l'installazione, gli elementi dell'inventario di rete vengono assegnati con la policy predefinita, che è preconfigurata con le impostazioni di protezione consigliate. Non puoi modificare o eliminare la policy predefinita. Puoi solo utilizzarla come modello per creare nuove policy.

Puoi creare quante policy ti servono in base ai requisiti di sicurezza. Un approccio diverso è quello di creare policy separate per ciascuna delle reti di clienti.

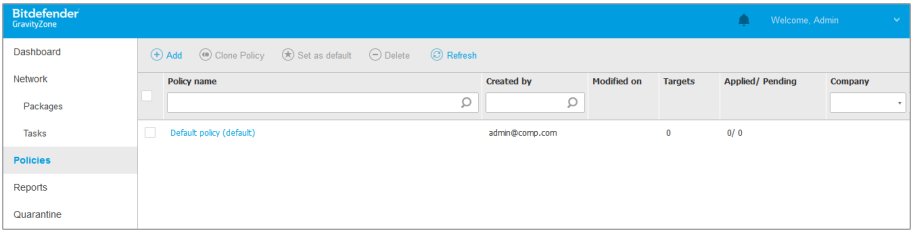
Ecco cosa devi sapere sulle policy:

- Le policy sono create nella pagina **Policy** e assegnate agli elementi di rete dalla pagina **Rete**.
- Le policy possono ereditare diverse impostazioni dei moduli da altre policy.
- Puoi configurare l'assegnamento della policy agli endpoint in modo che una policy possa essere applicata in qualsiasi momento o solo in determinate condizioni, in base alla posizione dell'endpoint. Inoltre, un endpoint può avere più policy assegnate.
- Gli endpoint possono avere una policy attiva alla volta.
-
- Le policy vengono inviate agli elementi di rete desiderati subito dopo averle create o modificate. Le impostazioni devono essere applicate agli elementi di rete in meno di un minuto (a condizione che siano online). Se un elemento di rete non è online, le impostazioni saranno applicate non appena tornerà online.
- La policy si applica solo ai moduli di protezione installati.
- La pagina **Policy** mostra solo i seguenti tipi di policy:
  - Le policy create da te.
  - Le altre policy (come la policy predefinita o i modelli creati dagli altri utenti), che sono stati assegnate agli endpoint nel tuo account.
- Non puoi modificare le policy create dagli altri utenti (a meno che i proprietari della policy non lo consentano nelle impostazioni della policy), ma puoi sovrascriverle assegnando un'altra policy agli elementi di destinazione.
- I computer in un account aziendale possono essere gestiti tramite policy sia dall'amministratore aziendale che dal partner che ha creato l'account. Le policy create dall'account partner non possono essere modificate dall'account aziendale.

Avvertimento
Solo i moduli della policy supportata saranno applicati agli endpoint di destinazione. Ricordati che solo il modulo antimalware è supportato per i sistemi operativi server.

7.1. Gestire le policy

Puoi visualizzare e gestire le policy nella pagina **Policy**.



La pagina Policy

Nella tabella, vengono mostrate le policy esistenti. Per ciascuna policy, puoi visualizzare:

- Nome policy.
- L'utente che ha creato la policy.
- Data e ora di quando la policy è stata modificata l'ultima volta.

Per personalizzare i dettagli della policy mostrati nella tabella:

1. Clicca sul pulsante **Colonne** nel lato destro della Barra degli strumenti.
2. Seleziona le colonne che vuoi visualizzare.
3. Clicca sul pulsante **Reimposta** per tornare alla visuale delle colonne predefinita.

Puoi ordinare le policy disponibili e anche cercare determinate policy usando i criteri disponibili.

7.1.1. Creare le policy

Puoi creare policy aggiungendone una nuova o duplicando (clonando) una policy esistente.

Per creare una policy di sicurezza:

1. Vai alla pagina **Policy**

2. Seleziona il metodo di creazione della policy:
   - **Aggiungi una nuova policy**.
     – Clicca sul pulsante ⊕**Aggiungi** nel lato superiore della tabella. Questo comando crea una nuova policy partendo dal modello della policy predefinita.
   - **Clona una policy esistente**.
     a. Seleziona la casella di spunta della policy che vuoi duplicare.
     b. Clicca sul pulsante **Clona** nel lato superiore della tabella.
3. Configura le impostazioni della policy. Per informazioni dettagliate, fai riferimento a «Policy per computer e virtual machine» (p. 135).
4. Clicca su **Salva** per creare la policy e tornare alla lista delle policy.

7.1.2. Assegnare le policy

Inizialmente, agli endpoint viene assegnata la policy predefinita. Una volta definita le policy necessarie nella pagina **Policy**, puoi assegnarle agli endpoint.

Puoi assegnare le policy in due modi:

- Assegnazione basata su dispositivo, significa che devi selezionare manualmente gli endpoint di destinazione a cui assegnare le policy. Queste policy sono anche conosciute come policy dispositivo.
- Assegnazione basata su regola, significa che una policy viene assegnata a un endpoint gestito se le impostazioni di rete sull'endpoint corrispondono alle condizioni date di una regola di assegnazione esistente.

Nota
Puoi assegnare solo policy create da te. Per assegnare una policy creata da un altro utente, devi prima clonarla nella pagina **Policy**.

Assegnare le policy dispositivo

In GravityZone, puoi assegnare le policy in molti modi:

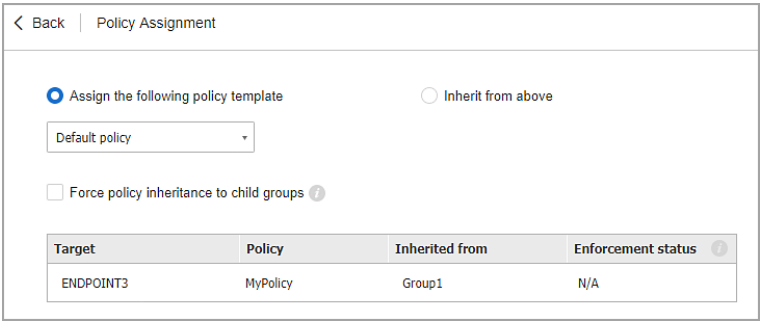
- Assegna la policy direttamente al bersaglio.
- Assegna la policy del gruppo parentale tramite ereditarietà.
- Forza l'ereditarietà della policy per il bersaglio.

Di norma, ogni endpoint o gruppo di endpoint eredita la policy del gruppo parentale. Se modifichi la policy del gruppo parentale, tutti i discendenti ne saranno influenzati, tranne quelli con una policy forzata.

Per assegnare una policy dispositivo:

1. Vai alla pagina **Rete**.
2.
3. Clicca sul pulsante **Assegna policy** nel lato superiore della tabella, o seleziona l'opzione **Assegna policy** nel menu contestuale.

   Compare la pagina **Assegnazione policy**:



Impostazioni assegnazione policy

4. Controlla la tabella con gli endpoint bersaglio. Per ogni endpoint, puoi visualizzare:
   - La policy assegnata.
   - Il gruppo parentale da cui il bersaglio ha ereditato la policy, se presente.

     Se il gruppo sta applicando la policy, puoi cliccare sul suo nome per vedere la pagina **Assegnazione policy** con questo gruppo come bersaglio.
   - Lo stato di applicazione.

     Questo stato mostra se il bersaglio sta applicando l'ereditarietà della policy o è obbligato a ereditare la policy.

     Nota i bersagli con una policy obbligata (stato **obbligata**). Le loro policy non possono essere sostituite. In tali casi, viene mostrato un messaggio di avviso.

5. In caso di avviso, clicca sul link **Escludi questi bersagli** per continuare.
6. Scegli una delle opzioni disponibili per assegnare la policy:
   - **Assegna il seguente modello di policy**, per designare una determinata policy direttamente agli endpoint bersaglio.
   - **Eredita dall'alto**, per usare la policy del gruppo parentale.
7. Se hai scelto di assegnare un modello di policy:
   a. Seleziona la policy dall'elenco a discesa.
   b. Seleziona **Forza ereditarietà policy a gruppi figli** per:
      - Assegnare la policy a tutti i discendenti dei gruppi bersaglio, senza alcuna eccezione.
      - Prevenirne ogni cambiamento da qualsiasi posizione inferiore nella gerarchia.

      Una nuova tabella mostra in modo ricorrente tutti gli endpoint o gruppi di endpoint influenzati, insieme alle policy che saranno sostituite.
8. Clicca su **Fine** per salvare e applicare le modifiche. Diversamente, clicca su **Indietro** o **Annulla** per tornare alla pagina precedente.

Una volta finito, le policy vengono subito inviate agli endpoint bersaglio. Le impostazioni devono essere applicate agli endpoint in meno di un minuto (a condizione che siano online). Se un endpoint non è online, le impostazioni saranno applicate non appena tornerà online.

Per verificare se la policy è stata assegnata con successo:

1. Nella pagina **Rete**, clicca sul nome dell'endpoint di tuo interesse. Control Center mostrerà la finestra **Informazioni**.
2. Controlla la sezione **Policy** per visualizzare lo stato della policy attuale. Deve indicare **Applicata**.

Assegnare le policy basate su regole

La pagina **Policy > Assegnazione regole** ti consente di definire l'assegnazione delle regole per le policy, per una determinata posizione. Per esempio, puoi applicare regole di firewall più restrittive se l'utente si connette a Internet da fuori azienda o puoi definire le frequenze per le attività a richiesta quando si è fuori dall'azienda.

Ecco cosa devi sapere sull'assegnazione delle regole:

- Gli endpoint possono avere solo una policy attiva alla volta.
- Una policy applicata tramite una regola sovrascriverà la policy del dispositivo impostata sull'endpoint.
- Se non è applicabile alcuna regola di assegnazione, allora viene applicata la policy del dispositivo.
- Le regole sono ordinate ed elaborate in base alla priorità, con `1` che rappresenta la più alta. Si possono avere diverse regole per lo stesso bersaglio. In questo caso, sarà applicata la prima regola che corrisponde alle impostazioni della connessione attiva sull'endpoint di destinazione.

  Per esempio, se un endpoint corrisponde a una regola utente con priorità 4 e una regola di posizione con priorità 3, sarà applicata la regola di posizione.

Avvertimento
Assicurati di considerare impostazioni sensibili come eccezioni, comunicazione o dettagli del proxy nel creare le regole.
Come migliore prassi, si consiglia di utilizzare l'ereditarietà della policy per mantenere le impostazioni critiche della policy del dispositivo anche nella policy utilizzata dalle regole di assegnazione.

Per creare una nuova regola:

1. Vai alla pagina **Regole di assegnazione**.
2. Clicca sul pulsante ⊕**Aggiungi** nel lato superiore della tabella.
3. Seleziona il tipo di regola:
   - Regola posizione
   - Regola utente
4. Configura le impostazioni della regola come necessario.
5. Clicca su **Salva** per salvare le modifiche e applicare la regola agli endpoint di destinazione della policy.

Per modificare le impostazioni di una regola esistente:

1. Nella pagina **Regole di assegnazione**, trova la regola che stai cercando e clicca sul suo nome per modificarla.
2. Configura le impostazioni della regola come necessario.

3. Clicca su **Salva** per applicare le modifiche e chiudere la finestra. Per lasciare la finestra senza salvare le modifiche, clicca su **Annulla**.

Se non vuoi più utilizzare una regola, seleziona la regola e clicca sul pulsante **Elimina** nel lato superiore della tabella. Ti sarà chiesto di confermare la tua azione cliccando su **Sì**.

Per assicurarsi che vengano visualizzate le informazioni più recenti, clicca sul pulsante **Aggiorna** nel lato superiore della tabella.

Configurare le regole posizione

Una posizione è un segmento di rete identificato da una o più impostazioni di rete, come un gateway specifico, un determinato DNS utilizzato per risolvere gli URL, o un sottoinsieme di IP. Per esempio, puoi definire posizioni come la LAN aziendale, le server farm o un ufficio.

Nella finestra di configurazione delle regole, segui questi passaggi:

1. Inserisci un nome indicativo e una descrizione per la regola che vuoi creare.
2. Imposta la priorità della regola. Le regole sono ordinate in base alla priorità, con la prima regola che la massima priorità. La stessa priorità non può essere impostata due o più volte.
3. Seleziona l'azienda a cui applicare la policy.
4. Seleziona la policy per cui creare la regola di assegnazione.
5. Definisci le posizioni per cui si applica la regola.
   a. Seleziona il tipo di impostazioni di rete dal menu nel lato superiore della tabella Posizioni. Sono disponibili i seguenti tipi:

Tipo	Valore
Range indirizzo IP/IP	Specifica gli indirizzi IP in una rete o nelle sottoreti. Per le sottoreti, usa il formato CIDR. Per esempio: `10.10.0.12` o `10.10.0.0/16`
Indirizzo gateway	Indirizzo IP del gateway
Indirizzo server WINS	Indirizzo IP del server WINS

Tipo	Valore
	Importante Questa opzione non si applica ai sistemi Linux e Mac.
Indirizzo server DNS	Indirizzo IP del server DNS
Suffisso DNS connessione DHCP	Il nome del DNS senza l'hostname per una determinata connessione DHCP Per esempio: `hq.company.biz`
L'endpoint può risolvere l'host	Hostname. Per esempio: `fileserv.company.biz`
Tipo di rete	Wireless/Ethernet Selezionando Wireless, puoi anche aggiungere l'SSID della rete. **Importante** Questa opzione non si applica ai sistemi Linux e Mac.

Hostname	Hostname
	Per esempio: `cmp.bitdefender.com`
	Importante
	Puoi usare anche caratteri jolly. L'asterisco (*) sostituisce lo zero o altri caratteri, mentre il punto interrogativo (?) sostituisce esattamente un carattere. Esempi:
	`*.bitdefender.com`
	`cmp.bitdefend??.com`

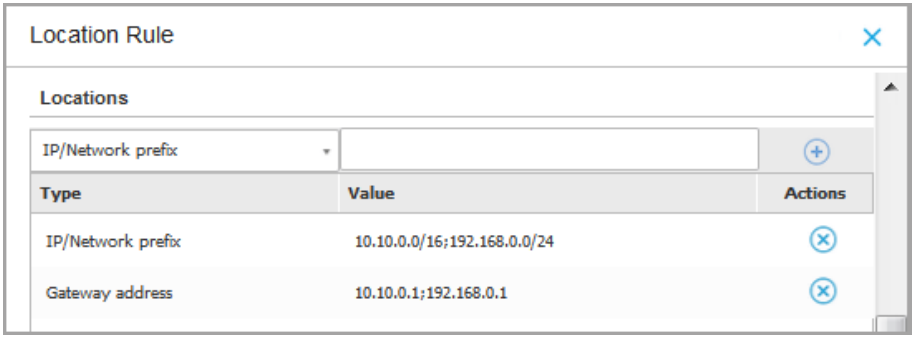
b. Inserisci il valore per il tipo selezionato. Dove applicabile, puoi inserire più valori nel campo dedicato, separati da un punto e virgola (;) e senza spazi aggiuntivi. Per esempio, inserendo `10.10.0.0/16;192.168.0.0/24`, la

regola viene applicata agli endpoint di destinazione con gli IP che corrispondo a OGNUNA di queste sottoreti.

Avvertimento
Puoi usare solo un tipo di impostazioni di rete per la regola posizione. Per esempio, se hai aggiunto una posizione utilizzando il **prefisso rete/IP**, non puoi utilizzare nuovamente questa impostazione nella stessa regola.

c. Clicca sul pulsante **Aggiungi** nel lato destro della tabella.

Le impostazioni di rete sugli endpoint devono corrispondere a TUTTE le posizioni fornite, affinché la regola si applichi ad esse. Per esempio, per identificare la rete della LAN aziendale, puoi inserire il gateway, il tipo di rete e il DNS. Inoltre, aggiungendo una sottorete, puoi identificare un ufficio all'interno della LAN aziendale.



Regola posizione

Clicca sul campo **Valore** per modificare i criteri esistenti e poi premi `Invio` per salvare le modifiche.

Per rimuovere una posizione, selezionala e clicca sul pulsante **Elimina**.

6. Potresti voler escludere determinate posizioni dalla regola. Per creare un'eccezione, definisci le posizioni da escludere dalla regola:
   a. Seleziona la casella di spunta **Eccezioni** nella tabella Posizioni.
   b. Seleziona il tipo di impostazioni di rete dal menu nel lato superiore della tabella Eccezioni. Per maggiori informazioni sulle opzioni, fai riferimento a «Configurare le regole posizione» (p. 130).

c. Inserisci il valore per il tipo selezionato. Puoi inserire più valori nel campo dedicato, separati da un punto e virgola (;) e senza spazi aggiuntivi.

d. Clicca sul pulsante **Aggiungi** nel lato destro della tabella.

Le impostazioni di rete sugli endpoint devono corrispondere a TUTTE le condizioni indicate nella tabella Eccezioni, affinché un'eccezione venga effettivamente applicata.

Clicca sul campo **Valore** per modificare i criteri esistenti e poi premi `Invio` per salvare le modifiche.

Per rimuovere un'eccezione, clicca sul pulsante **Elimina** nel lato destro della tabella.

7. Clicca su **Salva** per salvare la regola di assegnazione e applicarla.

   Una volta creata, la regola posizione viene applicata automaticamente a tutti gli endpoint di destinazione gestiti.

Configurare le regole utente

Importante

- Puoi creare le regole utente solo se è disponibile un'integrazione di Active Directory.
- Puoi definire le regole utente solo per gli utenti e i gruppi di Active Directory. Le regole basate sui gruppi di Active Directory non sono supportate dai sistemi Linux.

Nella finestra di configurazione delle regole, segui questi passaggi:

1. Inserisci un nome indicativo e una descrizione per la regola che vuoi creare.
2. Imposta la priorità. Le regole sono ordinate in base alla priorità, con la prima regola che la massima priorità. La stessa priorità non può essere impostata due o più volte.
3. Seleziona la policy per cui creare la regola di assegnazione.
4. Nella sezione **Bersagli**, seleziona gli utenti e i gruppi di sicurezza a cui si desidera applicare la regola della policy. Puoi visualizzare la tua selezione nella tabella sulla destra.
5. Clicca su **Salva**.

   Una volta creata, la regola dell'utente si applica agli endpoint bersaglio gestiti all'accesso dell'utente.

7.1.3. Modificare le impostazioni di una policy

Le impostazioni della policy possono essere inizialmente configurate durante la creazione della policy. In seguito, puoi modificarle in base alla necessità, in qualsiasi momento.

Nota
Di norma, solo l'utente che ha creato la policy può modificarla. Per modificarla, il proprietario della policy deve selezionare l'opzione **Consenti ad altri utenti di modificare questa policy** dalla pagina **Dettagli** della policy.

Per modificare le impostazioni di una policy esistente:

1. Vai alla pagina **Policy**
2. Trova la policy che stai cercando nell'elenco e clicca sul suo nome per modificarla.
3. Configura le impostazioni della policy come necessario. Per informazioni dettagliate, fai riferimento a «Policy per computer e virtual machine» (p. 135).
4. Clicca su **Salva**.

   Le policy vengono spinte agli elementi di rete bersaglio subito dopo aver modificato le assegnazioni o le impostazioni della policy. Le impostazioni devono essere applicate agli elementi di rete in meno di un minuto (a condizione che siano online). Se un elemento di rete non è online, le impostazioni saranno applicate non appena tornerà online.

7.1.4. Rinominare le policy

Le policy devono avere nomi indicativi in modo che tu o altri amministratori possiate identificarle rapidamente.

Per rinominare una policy:

1. Vai alla pagina **Policy**
2. Clicca sul nome della policy. Così si aprirà la pagina della policy.
3. Inserisci un nuovo nome della policy.
4. Clicca su **Salva**.

Nota
Il nome della policy è unico. Devi inserire un nome diverso per ciascuna nuova policy.

7.1.5. Eliminare le policy

Se una policy non ti serve più, eliminala. Una volta che una policy viene eliminata, agli elementi di rete a cui era stata applicata sarà assegnata la policy del gruppo parentale. Se non si applica nessun'altra policy, alla fine entrerà in vigore quella predefinita. Eliminando una policy con sezioni ereditate da altre policy, le impostazioni delle sezioni ereditate vengono memorizzate nelle policy figlie.

Nota
Di norma, solo l'utente che ha creato la policy può eliminarla. Per modificarla, il proprietario della policy deve selezionare l'opzione **Consenti ad altri utenti di modificare questa policy** dalla pagina **Dettagli** della policy.

Per eliminare una policy:

1. Vai alla pagina **Policy**
2. Seleziona la casella di spunta della policy che vuoi eliminare.
3. Clicca sul pulsante ⊖ **Elimina** nel lato superiore della tabella. Dovrai confermare la tua azione cliccando su **Sì**.

7.2. Policy per computer e virtual machine

Le impostazioni della policy possono essere inizialmente configurate durante la creazione della policy. In seguito, puoi modificarle in base alla necessità, in qualsiasi momento.

Per configurare le impostazioni di una policy:

1. Vai alla pagina **Policy**
2. Clicca sul nome della policy. Così si aprirà la pagina delle impostazioni della policy.
3. Configura le impostazioni della policy come necessario. Le impostazioni sono organizzate nelle seguenti sezioni:
   - Generale
   - Antimalware
   - Sandbox Analyzer
   - Firewall
   - Protezione rete
   - Patch Management
   - Controllo dispositivi

- Relay
- Exchange Protection
- Cifratura
- Sensore incidenti
- Gestione rischi

Spostati tra le sezioni usando il menu sul lato sinistro della pagina.

4. Clicca su **Salva** per salvare le modifiche e applicarle ai computer di destinazione. Per lasciare la pagina della policy senza salvare le modifiche, clicca su **Annulla**.

Nota
Per scoprire come lavorare con le policy, fai riferimento a «Gestire le policy» (p. 125).

7.2.1. Generale

Le impostazioni generali aiutano a gestire le opzioni di visualizzazione dell'interfaccia utente, la protezione tramite password, le impostazioni proxy, le impostazioni utente esperto, le opzioni di comunicazione e le preferenze di aggiornamento per gli endpoint di destinazione.

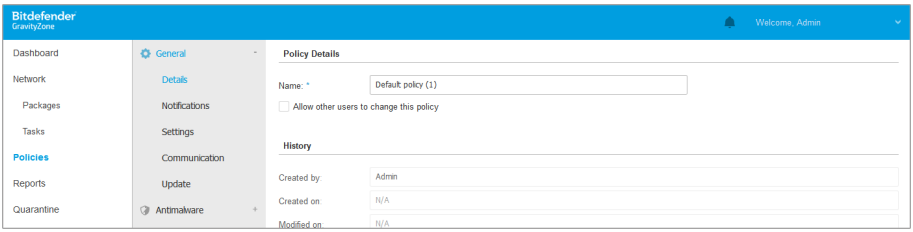
Le impostazioni sono organizzate nelle seguenti sezioni:

- Dettagli
- Notifiche
- Impostazioni
- Comunicazione
- Aggiornamento

Dettagli

La pagina **Dettagli** contiene diversi dettagli generali sulla policy:

- Nome policy
- L'utente che ha creato la policy
- Data e ora di quando la policy è stata creata
- Data e ora di quando la policy è stata modificata l'ultima volta



Policy per computer e virtual machine

Puoi rinominare la policy inserendo il nuovo nome nel campo corrispondente e cliccando sul pulsante **Salva** nella parte inferiore. Le policy devono avere nomi indicativi in modo che tu o altri amministratori possiate identificarle rapidamente.

Nota
Di norma, solo l'utente che ha creato la policy può modificarla. Per modificarla, il proprietario della policy deve selezionare l'opzione **Consenti ad altri utenti di modificare questa policy** dalla pagina **Dettagli** della policy.

Regole eredità

Puoi impostare le sezioni da ereditare da altre policy. Per farlo:

1. Seleziona il modulo e la sezione che vuoi ereditare dalla policy attuale. Tutte le sezioni sono ereditabili, tranne **Generali > Dettagli**.
2. Specifica la policy da cui vuoi ereditare la sezione.
3. Clicca sul pulsante **Aggiungi** nel lato destro della tabella.

Se una policy sorgente viene eliminata, quella ereditata si interrompe e le impostazioni delle sezioni ereditate vengono memorizzate nella policy figlia.

Le sezioni ereditate non possono essere ulteriormente ereditate da altre policy. Considera il seguente esempio:

La policy A eredita la sezione **Antimalware > A richiesta** dalla policy B. La policy C non può ereditare la sezione **Antimalware > A richiesta** dalla policy A.

Informazioni supporto tecnico

Puoi personalizzare le informazioni di contatto e del supporto tecnico disponibili nella finestra dell'agente di sicurezza **Info**, compilando i seguenti campi.

Per configurare un indirizzo e-mail nella finestra **Info**, in modo che si apra l'applicazione e-mail predefinita sull'endpoint, devi aggiungerlo nel campo **E-mail** con il prefisso "mailto:". Esempio: `mailto:name@domain.com`.

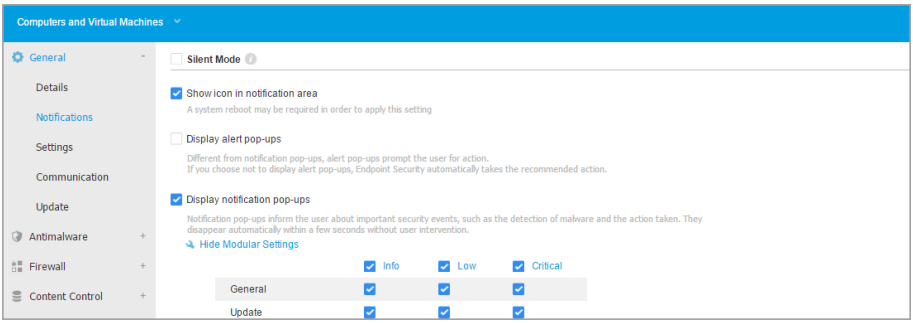
Gli utenti possono accedere a queste informazioni dalla console dell'agente di sicurezza, cliccando con il pulsante destro del mouse sull'icona Bitdefender nella barra delle applicazioni e selezionando **Info**.

Come Fornitore di servizi in grado di offrire servizi interamente gestiti, personalizzare queste informazioni può aiutarti a indirizzare le richieste del cliente finale ai tuoi dipartimenti vendite e al supporto tecnico.

Notifiche

In questa sezione, puoi configurare l'interfaccia utente dell'agente di sicurezza di Bitdefender affinché mostri le diverse opzioni in modo completo e intuitivo.

Con un semplice clic, puoi attivare o disattivare un intero tipo di notifiche, mantenendo solo quelle importanti per te. Inoltre, nella stessa pagina, ottieni un controllo totale sulla visibilità dei problemi a livello di endpoint.



Policy - Impostazioni di visualizzazione

- **Modalità silenziosa.** Usa la casella di spunta per attivare o disattivare la modalità silenziosa. La modalità silenziosa è stata progettata per aiutarti a disattivare facilmente l'interazione dell'utente nell'agente di sicurezza. Attivando la modalità silenziosa, vengono eseguite le seguenti modifiche alla configurazione della policy:
  - Le opzioni **Mostra l'icona nell'area delle notifiche**, **Mostra pop-up di notifica** e **Mostra pop-up di avviso** in questa sezione saranno disattivate.

- Se il livello di protezione del firewall è stata impostato su **Set di regole e chiedere** o **Set di regole, file noti e chiedere**, sarà modificato in **Set di regole, file noti e consentire**. Diversamente, l'impostazione del livello di protezione resterà immutata.

- **Mostra l'icona nell'area delle notifiche.** Seleziona questa opzione per mostrare l'icona Bitdefender nell'area delle notifiche (nota anche come barra delle applicazioni). L'icona informa gli utenti sullo stato della loro protezione cambiando il suo aspetto e mostrando una notifica pop-up corrispondente. Inoltre, gli utenti possono cliccarci sopra con il pulsante destro per aprire rapidamente la finestra principale dell'agente di sicurezza o la finestra **Info**.
- **Mostra pop-up di avviso.** Gli utenti vengono informati tramite pop-up sugli eventi di sicurezza che richiedono la loro attenzione. Scegliendo di non visualizzare i pop-up di avviso, l'agente di sicurezza intraprende automaticamente l'azione consigliata. I pop-up di avviso vengono generati nelle seguenti situazioni:
  - Se il firewall è impostato per richiedere l'azione dell'utente ogni volta che applicazioni sconosciute richiedono l'accesso alla rete o a Internet.
  - Se Advanced Threat Control / Intrusion Detection System è attivato, ogni volta che viene rilevata un'applicazione potenzialmente pericolosa.
  - Se la scansione dei dispositivi è attivata, ogni volta che un dispositivo di archiviazione esterno viene connesso al computer. Puoi configurare questa impostazione nella sezione **Antimalware > A richiesta**.
- **Mostra pop-up di notifica.** Diversamente dagli avvisi pop-up, le notifiche pop-up informano gli utenti sui diversi eventi di sicurezza. I pop-up scompaiono automaticamente entro pochi secondi senza alcun intervento dell'utente.

  Seleziona **Mostra pop-up di notifica** e clicca sul link **Mostra impostazioni modulari** per decidere di quali eventi, forniti dal modulo, gli utenti siano informati. Ci sono tre diversi tipi di notifiche pop-up, in base alla severità degli eventi:
  - **Informazioni** Gli utenti vengono informati sugli eventi di sicurezza più significativi ma innocui. Per esempio, un'applicazione che si è connessa a Internet.
  - **Basso**. Gli utenti vengono informati sugli eventi di sicurezza più importanti che potrebbero richiedere la loro attenzione. Per esempio, la scansione all'accesso ha rilevato una minaccia e il file è stato eliminato o messo in quarantena.

- **Critico**. Queste notifiche pop-up informano gli utenti su situazioni pericolose, come quando la scansione all'accesso rileva una minaccia e l'azione predefinita della policy è **Non fare nulla**, perciò il malware è ancora presente sull'endpoint, o quando non è stato possibile completare un processo di aggiornamento.

Seleziona la casella di spunta associata al nome della tipologia per attivare quel tipo di pop-up per tutti i moduli contemporaneamente. Clicca sulle caselle di spunta associate ai singoli moduli per attivare o disattivare determinate notifiche.

La lista dei moduli potrebbe variare in base alla tua licenza.

- **Visibilità problemi endpoint.** Gli utenti possono determinare quando il proprio endpoint ha problemi di configurazione o altri rischi di sicurezza, in base agli avvisi relativi allo stato. Per esempio, gli utenti possono visualizzare quando si verifica un problema relativo alla propria protezione antimalware, come modulo di scansione all'accesso disattivato o una scansione completa del sistema in ritardo. Gli utenti vengono informati sullo stato della loro protezione in due modi:
  - Verificando l'area di stato della finestra principale, che mostra un messaggio di stato appropriato e modifica il proprio colore in base alla severità dei problemi di sicurezza. Gli utenti hanno la possibilità di visualizzare anche eventuali dettagli sui problemi, cliccando sul pulsante disponibile.
  - Verificando l'icona Bitdefender nella barra delle applicazioni, che modifica il suo aspetto quando vengono rilevati dei problemi.

  L'agente di sicurezza di Bitdefender utilizza il seguente schema di colori nell'area di notifica:
  - Verde: non è stato rilevato alcun problema.
  - Giallo: l'endpoint ha problemi non critici che influenzano la sua sicurezza. Gli utenti non devono interrompere il proprio lavoro attuale per risolvere questi problemi.
  - Rosso: l'endpoint ha problemi critici che richiedono l'attenzione immediata dell'utente.

  Seleziona **Visibilità problemi endpoint** e clicca sul link **Mostra impostazioni modulari** per personalizzare gli avvisi di stato mostrati nell'interfaccia utente dell'agente di Bitdefender.

Per ciascun modulo, puoi scegliere di mostrare l'avviso come allarme o problema critico, o non mostrarlo del tutto. Le opzioni sono descritte qui:

- **Generali**. L'avviso di stato viene generato quando un riavvio del sistema è necessario durante o dopo l'installazione del prodotto, e anche quando l'agente di sicurezza non ha potuto connettersi ai servizi cloud di Bitdefender.
- **Antimalware**. Gli avvisi di stato vengono generati nelle seguenti situazioni:
  - La scansione all'accesso viene attivata ma saltando diversi file locali.
  - Sono trascorsi diversi giorni da quando una scansione completa di sistema è stata eseguita sulla macchina.

    Puoi selezionare come mostrare gli avvisi e definire il numero di giorni dall'ultima scansione completa di sistema.
  - Per completare il processo di disinfezione è necessario riavviare il sistema.
- **Firewall**. Questo avviso di stato viene generato quando il modulo firewall è disattivato.
- **Controllo contenuti**. Questo avviso di stato viene generato quando il modulo Controllo contenuti è disattivato.
- **Aggiornamento**. L'avviso di stato viene generato ogni volta che un riavvio del sistema è necessario per completare un'operazione di aggiornamento.

- **Notifica riavvio endpoint.** Con questa opzione viene mostrato un avviso di riavvio sull'endpoint ogniqualvolta è necessario riavviare il sistema a cause di modifiche apportate sull'endpoint dai moduli di GravityZone selezionati nelle impostazioni modulari.

  Nota
  Gli endpoint che richiedono un riavvio del sistema sono mostrati nell'inventario di GravityZone con una specifica icona di stato ( ).

  Puoi personalizzare ulteriormente gli avvisi di riavvio cliccando su **Mostra impostazioni modulari**. Sono disponibili le seguenti opzioni:

  - **Aggiornamento** - Seleziona questa opzione per attivare le notifiche di riavvio per aggiornamento dell'agente.
  - **Gestione patch** - Seleziona questa opzione per attivare le notifiche di riavvio di installazione delle patch.

Nota
Puoi anche impostare un limite alle ore con cui un utente può posticipare un riavvio. Per farlo, seleziona **Riavvia automaticamente la macchina dopo** e inserisci un valore compreso tra 1 e 46.

L'avviso di riavvio richiede all'utente di scegliere una delle seguenti azioni:

- **Riavvia ora**. In questo caso, il sistema si riavvierà immediatamente.
- **Posticipa riavvio**. In questo caso, una notifica di riavvio comparirà periodicamente, finché l'utente non riavvia il sistema o fin quando il tempo impostato dall'Amministratore aziendale non sarà trascorso.

Impostazioni

In questa sezione, puoi configurare le seguenti impostazioni:

- **Configurazione password.** Per prevenire gli utenti con diritti di amministratore dal disinstallare la protezione, devi impostare una password.

  La password di disinstallazione può essere configurata prima dell'installazione, personalizzando il pacchetto di installazione. Se l'hai fatto, seleziona **Mantieni impostazioni installazione** per mantenere la password attuale.

  Per impostare la password o modificare la password attuale, seleziona **Attiva password** e inserisci la password desiderata. Per rimuovere la protezione della password, seleziona **Disattiva password**.

- **Configurazione proxy**

  Se la tua rete si trova dietro un server proxy, devi definire le impostazioni proxy che consentiranno ai tuoi endpoint di comunicare con le componenti della soluzione GravityZone. In questo caso, devi attivare l'opzione **Configurazione proxy** e inserire i parametri richiesti:
  - **Server** - Inserisci l'IP del server proxy
  - **Porta** - Inserisci la porta usata per connettersi al server proxy.
  - **Nome utente** - Inserisci un nome utente riconosciuto dal proxy.
  - **Password** - Inserisci la password corretta per l'utente indicato

- **Utente esperto**

  Il modulo Utente esperto consente di garantire diritti di amministrazione a livello di endpoint, permettendo all'utente dell'endpoint di accedere e modificare le impostazioni della policy, tramite l'interfaccia di Bitdefender Endpoint Security Tools.

Se vuoi che determinati endpoint abbiano diritti di Utente esperto, devi prima includere questo modulo nell'agente di sicurezza installato negli endpoint di destinazione. In seguito, devi configurare le impostazioni di Utente esperto nella policy applicata a questi endpoint:

Importante
Il modulo Utente esperto è disponibile solo per i sistemi operativi Windows desktop e server supportati.

1. Attiva l'opzione **Utente esperto**.
2. Definisci una password Utente esperto nei campi sottostanti.

   Agli utenti che accedono alla modalità Utente esperto dall'endpoint locale sarà chiesto di inserire la password impostata.

Per accedere al modulo Utente esperto, gli utenti devono cliccare con il pulsante destro del mouse sull'icona Bitdefender nella barra delle applicazioni e scegliere **Utente esperto** nel menu contestuale. Dopo aver fornito la password nella finestra di accesso, comparirà una console contenente le impostazioni della policy attualmente applicata, in cui l'utente dell'endpoint può visualizzare e modificare le impostazioni della policy.

Nota
È possibile accedere localmente solo a determinate funzionalità di sicurezza tramite la console Utente esperto, relative ai moduli Antimalware, Firewall, Controllo contenuti e Controllo dispositivi.

Per annullare le modifiche fatte in modalità Utente esperto:

- Nella Control Center, apri il modello di policy assegnato all'endpoint con i diritti di Utente esperto e clicca su **Salva**. In questo modo, le impostazioni originali saranno applicate nuovamente all'endpoint di destinazione.
- Assegna una nuova policy all'endpoint con diritti di Utenti esperto.
- Accedi all'endpoint locale, apri la console Utente esperto e clicca su **Risincronizza**.

Per trovare facilmente gli endpoint con policy modificate nella modalità Power User:

- Nella pagina **Rete**, clicca sul menu **Filtri** e seleziona l'opzione **Modificata da Utente esperto** nella scheda **Policy**.

– Nella pagina **Rete**, clicca sull'endpoint di tuo interesse per mostrare la finestra **Informazioni**. Se la policy è stata modificata in modalità Utente esperto, nella scheda **Generale** sezione **Policy** sarà mostrata una notifica.

> **Importante**
> Il modulo Utente esperto è stato progettato appositamente per risolvere eventuali problemi, consentendo all'amministratore di rete di visualizzare e modificare facilmente le impostazioni della policy nei computer locali. L'assegnazione di diritti di Utente esperto agli altri utenti nell'azienda deve essere limitata al personale autorizzato, per assicurarsi che le policy di sicurezza siano sempre applicate su tutte gli endpoint della rete aziendale.

- **Opzioni**

  In questa sezione, puoi definire le seguenti impostazioni:

  – **Rimuovi eventi più vecchi di (giorni).** L'agente di sicurezza di Bitdefender mantiene un registro dettagliato degli eventi riguardanti la sua attività sul computer (include anche le attività dei computer monitorati dal Controllo contenuti). Di norma, gli eventi vengono eliminati dal registro dopo 30 giorni. Se vuoi modificare questo intervallo, scegli un'opzione diversa dal menu.

  – **Invia rapporti sui blocchi a Bitdefender.** Seleziona questa opzione per inviare i rapporti ai laboratori di Bitdefender per l'analisi, se l'agente di sicurezza dovesse bloccarsi. I rapporti aiuteranno i nostri ingegneri a scoprire le cause del problema impedendo che si verifichi nuovamente. Non sarà inviata alcuna informazione personale.

Comunicazione

In questa sezione, puoi assegnare una o più macchine relay agli endpoint di destinazione, poi configurare le preferenze proxy per la comunicazione tra gli endpoint di destinazione e GravityZone.

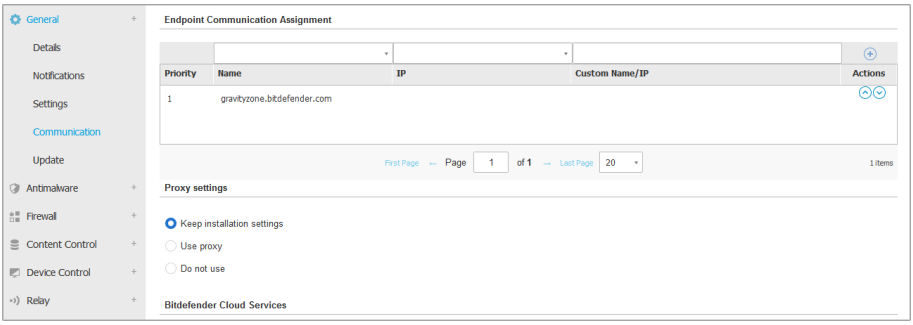
Assegnazione comunicazione endpoint

Quando nella rete bersaglio sono disponibili più agenti relay, puoi assegnare ai computer selezionati uno o più endpoint relay tramite la policy.

Per assegnare gli endpoint relay ai computer di destinazione:

1. Nella tabella **Assegnazione comunicazione endpoint**, clicca sul campo **Nome**. Viene visualizzato l'elenco degli endpoint relay rilevati nella tua rete.

2. Seleziona un'entità.



Policy - Impostazioni di comunicazione

3. Clicca sul pulsante **Aggiungi** nel lato destro della tabella.

   L'endpoint relay viene aggiunto all'elenco. Tutti i computer di destinazione comunicheranno con la Control Center tramite l'endpoint relay specificato.

4. Segui gli stessi passaggi per aggiungere i relay di sicurezza, se disponibili.

5. Puoi configurare la priorità degli endpoint relay utilizzando le frecce su e giù, disponibili sul lato destro di ciascuna entità. La comunicazione con i computer bersaglio sarà eseguita tramite l'entità posizionata in cima all'elenco. Quando la comunicazione con questa entità non può essere eseguita, sarà considerata la prossima.

6. Per eliminare un'entità dall'elenco, clicca sul pulsante **Elimina** corrispondente nel lato destro della tabella.

Comunicazione tra endpoint e relay / GravityZone

In questa sezione, puoi configurare le preferenze del proxy per la comunicazione tra gli endpoint di destinazione e le macchine relay assegnate, o tra gli endpoint di destinazione e GravityZone Control Center (quando non sono stati assegnati relay):

- **Mantieni impostazioni installazione** per utilizzare le stesse impostazioni proxy definite con il pacchetto di installazione.
- **Usa proxy definito nella sezione General**, per usare le impostazioni proxy definite nella policy attuale, nella sezione **Generale > Impostazioni**.

- **Non usarla**, quando gli endpoint di destinazione non comunicano con determinate componenti di GravityZone tramite proxy.

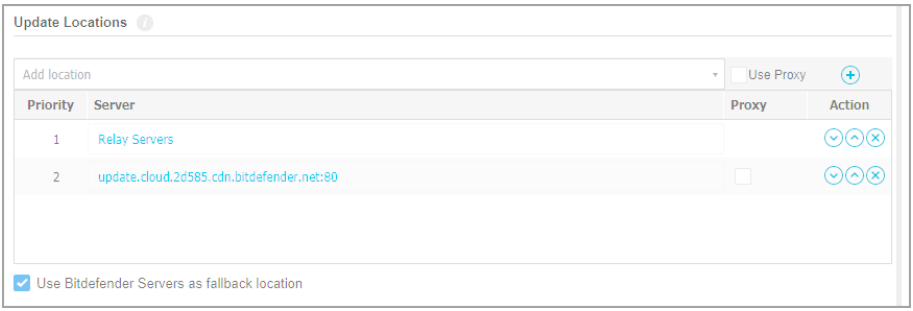
Comunicazione tra endpoint e servizi cloud

In questa sezione, puoi configurare le preferenze del proxy per la comunicazione tra gli endpoint di destinazione e i servizi cloud di Bitdefender:

- **Mantieni impostazioni installazione** per utilizzare le stesse impostazioni proxy definite con il pacchetto di installazione.
- **Usa proxy definito nella sezione General**, per usare le impostazioni proxy definite nella policy attuale, nella sezione **Generale > Impostazioni**.
- **Non usarla**, quando gli endpoint di destinazione non comunicano con determinate componenti di GravityZone tramite proxy.

Aggiornamento

Gli aggiornamenti sono molto importanti in quanto consentono di contrastare le minacce più recenti. Bitdefender pubblica tutti gli aggiornamenti del prodotto e del contenuto di sicurezza attraverso i server di Bitdefender su Internet. Tutti gli aggiornamenti sono cifrati e firmati digitalmente, in modo che non possano essere manomessi. Quando è disponibile un nuovo aggiornamento, l'agente di sicurezza di Bitdefender controlla la firma digitale dell'aggiornamento per verificarne l'autenticità, e i contenuti del pacchetto per l'integrità. Poi, ciascun file dell'aggiornamento viene analizzato e la sua versione verificata rispetto a quella installata. I file più nuovi vengono scaricati a livello locale e controllati nuovamente nell'hash MD5 per assicurarsi che non siano stati alterati. In questa sezione, puoi configurare l'agente di sicurezza di Bitdefender e le impostazioni di aggiornamento del contenuto di sicurezza.



Policy - Opzioni di aggiornamento

- **Aggiornamento del prodotto.** L'agente di sicurezza di Bitdefender controlla, scarica e installa automaticamente gli aggiornamenti ogni ora (impostazione predefinita). Gli aggiornamenti automatici vengono eseguiti in modo silenzioso, in background.
  - **Ricorrenza**. Per modificare la ricorrenza automatica degli aggiornamenti, seleziona una diversa opzione nel menu e configurala in base alle tue esigenze nei campi successivi.
  - **Posticipa riavvio**. Alcuni aggiornamenti richiedono un riavvio del sistema per essere installati e funzionare correttamente. Di norma, il prodotto continuerà a lavorare con i file precedenti finché il computer non viene riavviato. Una volta fatto, saranno applicati gli ultimi aggiornamenti. Una notifica nell'interfaccia utente chiederà all'utente di riavviare il sistema ogni volta che è necessario eseguire un aggiornamento. Si consiglia di lasciare attivata questa opzione. Diversamente, il sistema si riavvierà automaticamente dopo aver installato un aggiornamento che richiede un riavvio. Gli utenti saranno invitati a salvare il proprio lavoro, ma il riavvio non potrà essere annullato.
  - Scegliendo di posticipare il riavvio, puoi impostare un momento migliore per riavviare il computer automaticamente, se (ancora) necessario. Ciò può essere molto utile per i server. Seleziona **Se necessario, riavvia dopo aver installato gli aggiornamenti** e specifica quando è meglio riavviare (giornalmente o settimanalmente in un certo giorno, a una certa ora).
  - Per un maggior controllo sulla modifica della configurazione e sull'aggiornamento del processo di staging, puoi configurare l'agente BEST

sulle tue macchine Linux per eseguire gli aggiornamenti del modulo del kernel EDR tramite **Aggiornamento prodotto**.

Quando la casella **Aggiornamento prodotto** è attivata:

- Se attivi la casella **Aggiorna i moduli EDR usando l'aggiornamento del prodotto**, GravityZone aggiornerà le versioni del kernel tramite **Aggiornamento prodotto**.
- Lasciando questa opzione disattivata, le versioni del kernel saranno aggiornate tramite **Aggiornamento contenuti di sicurezza**.

> **Nota**
> Se attivi la casella **Aggiorna i moduli EDR Linux usando l'aggiornamento del prodotto**, ma disattivi l'opzione **Aggiornamento prodotto**, i moduli EDR Linux non saranno aggiornati.

- **Aggiornamento del contenuto di sicurezza.** Il contenuto di sicurezza fa riferimento a mezzi statici e dinamici di rilevamento delle minacce, come, a titolo esemplificativo, motori di scansione, modelli di apprendimento automatico, euristiche, regole, firme e blacklist. L'agente di sicurezza di Bitdefender controlla automaticamente la presenza di aggiornamenti del contenuto di sicurezza ogni ora (impostazione predefinita). Gli aggiornamenti automatici vengono eseguiti in modo silenzioso, in background. Per modificare la ricorrenza automatica degli aggiornamenti, seleziona una diversa opzione nel menu e configurala in base alle tue esigenze nei campi successivi.
- **Ubicazioni aggiornamento**. Il percorso di aggiornamento predefinito dell'agente di sicurezza di Bitdefender è http://upgrade.bitdefender.com. Aggiungi un percorso di aggiornamento selezionando i percorsi predefiniti nel menu a discesa o inserendo l'IP o il nome dell'host di uno o più server di aggiornamento nella tua rete. Configura la loro priorità utilizzando i pulsanti su e giù mostrati passandoci sopra con il mouse. Se il primo percorso di aggiornamento non è disponibile, viene utilizzato il successivo e così via.

  Per impostare un indirizzo di aggiornamento locale:

  1. Inserisci l'indirizzo del server di aggiornamento nel campo **Aggiungi percorso**. Puoi:
     - Seleziona un percorso predefinito:

- **Server relay**. L'endpoint si connetterà automaticamente al suo server relay assegnato.

  Avvertimento
  I server relay non sono supportati sui sistemi operativi datati. Per maggiori informazioni, fai riferimento alla Guida di installazione.

  Nota
  Puoi controllare il server relay assegnato nella finestra **Informazioni**. Per maggiori dettagli fai riferimento a Visualizzare i dettagli del computer.

- **update.cloud.2d585.cdn.bitdefender.net**. Si tratta del percorso di aggiornamento predefinito di Bitdefender, da cui Bitdefender fornisce gli aggiornamenti. Questo percorso di aggiornamento deve sempre essere l'ultima opzione nell'elenco.

– Inserisci l'IP o il nome dell'host di uno o più server di aggiornamento nella tua rete. Usa una di queste sintassi:

  - `update_server_ip:port`
  - `update_server_name:port`

  La porta standard è 7074.

  La casella di spunta **Usa server Bitdefender come percorso alternativo** è selezionata per impostazione predefinita. Se i percorsi di aggiornamento non sono disponibili, sarà utilizzato il percorso alternativo.

  Avvertimento
  Disattivare il percorso alternativo, bloccherà gli aggiornamenti automatici, lasciando la rete vulnerabile se i percorsi indicati non fossero disponibili.

2. Se i computer client si connettono al server di aggiornamento locale attraverso un server proxy, seleziona **Usa proxy**.
3. Clicca sul pulsante **Aggiungi** nel lato destro della tabella.
4. Utilizza le frecce Su / Giù nella colonna **Azione** per impostare la priorità dei percorsi di aggiornamento definiti. Se il primo percorso di aggiornamento non è disponibile, viene considerato il successivo e così via.

Per rimuovere una posizione dalla lista, clicca sul pulsante ⊗ **Elimina** corrispondente. Sebbene tu possa rimuovere il percorso di aggiornamento predefinito, non è consigliabile farlo.

- **Aggiorna Ring.** Puoi implementare gli aggiornamenti del prodotto in fasi, utilizzando i ring di aggiornamento:
  - **Slow Ring**. Le macchine con una policy slow ring riceveranno gli aggiornamenti in un momento successivo, in base alla risposta ricevuta dagli endpoint fast ring. È una misura precauzionale nel processo di aggiornamento. È l'impostazione predefinita.
  - **Fast Ring**. Le macchine con una policy fast ring riceveranno i nuovi aggiornamenti disponibili. Questa impostazione è consigliata per le macchine non critiche nell'ambiente produttivo.

Importante

- Nell'improbabile evento che si verifichi un problema nel fast ring sulle macchine con una particolare configurazione, prima sarà eseguito l'aggiornamento slow ring.
- BEST for Windows Legacy non supporta la fase di test. Gli endpoint "legacy" in posizione di staging deve essere portati in posizione di produzione.

Telemetria sicurezza

Nota
Questa funzionalità richiede una licenza EDR ed è disponibile solo per gli endpoint Windows.

Con Telemetria sicurezza, hai accesso ai dati sottostanti relativi agli eventi di sicurezza, in modo da poter creare correlazioni personalizzate.

Per garantire una traccia digitale dei dati e prestazioni ottimali, gli agenti inviano solo eventi rilevanti per la sicurezza della tua rete. Tali eventi si riferiscono a:

- Processi: crea, termina
- File: crea, leggi, modifica, sposta, elimina
- Registro: crea ed elimina codici, modifica ed elimina valore
- Accesso utente: login

- Connessione di rete

L'agente Bitdefender invia queste informazioni in un formato standard del settore (JSON, CEF) direttamente alla soluzione SIEM che utilizzi.

Per inviare gli eventi di sicurezza dagli endpoint bersaglio alla soluzione SIEM, configura la policy come segue:

- Seleziona la casella **Telemetria sicurezza** per consentire la funzionalità.
- Seleziona la soluzione SIEM a cui ti connetti.
- Fornisci l'URL del server SIEM.

  Avvertimento
  È richiesto il protocollo HTTPS con TLS 1.2 o superiore. In caso contrario, l'invio dell'evento fallirà.

- Inserisci il token di autorizzazione che protegge la connessione.
- In **Comunicazione tra endpoint e SIEM**, scegli se utilizzare un server proxy.

  Nota
  Per la comunicazione con il SIEM, l'agente utilizza lo stesso server proxy utilizzato per la comunicazione con GravityZone. Puoi verificare le sue impostazioni nella sezione **Generale > Impostazioni**.

Una volta che la policy è stata applicata agli endpoint, l'agente inizia a inviare gli eventi non appena si verificano sul server SIEM configurato.

7.2.2. Antimalware

Nota
Questo modulo è disponibile per:

- Windows for workstations
- Windows for servers
- Linux
- macOS

Il modulo antimalware protegge il sistema da ogni tipo di minaccia malware (virus, Trojan, spyware, rootkit, adware e così via). La protezione è divisa in tre categorie:

- Scansione all'accesso: impedisce alle nuove minacce malware di accedere al sistema.
- Scansione all'esecuzione: protegge in modo proattivo dalle minacce, scoprendo e bloccando automaticamente attacchi privi di file in fase di pre-esecuzione.
- Scansione a richiesta: consente di rilevare e rimuovere malware già presenti nel sistema.

Quando rileva un virus o un altro malware, l'agente di sicurezza di Bitdefender tenterà automaticamente di rimuovere il codice malware dal file infetto, ricostruendo il file originale. Questa operazione è denominata disinfezione. I file che non possono essere disinfettati vengono messi in quarantena per contenere l'infezione. Quando un virus è in quarantena, non può più arrecare alcun danno in quanto non può essere eseguito o letto.

Gli utenti più esperti possono configurare le eccezioni della scansione, se non desiderano controllare determinati file o estensioni.

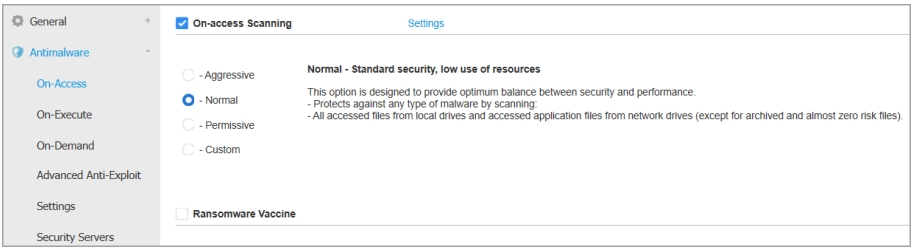
Le impostazioni sono organizzate nelle seguenti sezioni:

- All'accesso
- In esecuzione
- Su richiesta
- HyperDetect
- Anti-exploit avanzato
- Impostazioni
- Server di sicurezza

All'accesso

In questa sezione puoi configurare le componenti che forniscono protezione quando si accede a un file o un'applicazione:

- Scansione all'accesso
- Vaccino per ransomware



Policy - Impostazioni all'accesso

Scansione all'accesso

La scansione all'accesso impedisce alle nuove minacce malware di accedere al sistema esaminando i file di rete e locali all'accesso (apertura, spostamento, copiatura o esecuzione), settori di boot e applicazioni potenzialmente indesiderate (PUA).

Nota
Questa funzionalità ha alcune limitazioni sui sistemi basati su Linux. Per maggiori dettagli, fai riferimento al capitolo dedicato ai requisiti della Guida di installazione di GravityZone.

Per configurare la scansione all'accesso:

1. Usa la casella di spunta per attivare o disattivare la scansione all'accesso.

   Avvertimento
   Disattivando la scansione all'accesso, gli endpoint saranno vulnerabili ai malware.

2. Per una configurazione rapida, clicca sul livello di sicurezza che si adatta meglio alle tue esigenze (Aggressivo, Normale o Permissivo). Usa la descrizione sul lato destro dell'indicatore per scegliere.
3. Puoi configurare le impostazioni di scansione in dettaglio, selezionando il livello di protezione **Personalizzato** e cliccando sul link **Impostazioni**. Comparirà la finestra **Impostazioni scansione all'accesso**, contenente diverse opzioni organizzate in due schede, **Generali** e **Avanzate**.

   Le opzioni nella scheda **Generali** sono descritte di seguito:
   - **Posizione file**. Usa queste opzioni per specificare quali tipi di file vuoi che siano esaminati. Le preferenze della scansione possono essere configurare separatamente per i file locali (memorizzati sull'endpoint locale) o i file di

rete (memorizzati su condivisioni di rete). Se la protezione antimalware è installata su tutti i computer nella rete, puoi disattivare la scansione dei file di rete per consentire un accesso alla rete più rapido.

Puoi impostare l'agente di sicurezza in modo che esamini tutti i file a cui si accede (indipendentemente dalla loro estensione), solo i file delle applicazioni o determinate estensioni che ritieni essere pericolose. Controllare tutti i file a cui si ha avuto accesso fornisce una protezione migliore, mentre controllare solo le applicazioni può essere usato per ottenere prestazioni migliori.

Nota
I file delle applicazioni sono più vulnerabili agli attacchi dei malware rispetto ad altri tipi di file. Per maggiori informazioni, fai riferimento a «Tipi di file applicazioni» (p. 458).

Se vuoi che siano esaminate solo determinate estensioni, seleziona **Estensioni definite dall'utente** nel menu e poi inserisci le estensioni nel campo di modifica, premendo `Invio` dopo ciascuna estensione.

Nota
Sui sistemi basati su Linux, le estensioni dei file sono sensibili alle maiuscole e i file con lo stesso nome ma diversa estensione vengono considerati come elementi distinti. Per esempio, `file.txt` è diverso da `file.TXT`.

Per motivi di prestazioni del sistema, puoi anche escludere i file di maggiori dimensioni dalla scansione. Seleziona la casella **Dimensione massima (MB)** e indica la dimensione limite dei file da esaminare. Usa questa opzione con attenzione, perché i malware possono influenzare anche i file di maggiori dimensioni.

- **Esamina.** Seleziona le caselle corrispondenti per attivare le opzioni di scansione desiderate.
  - **Solo file nuovi o modificati.** Controllando solo i file modificati o nuovi, potresti migliorare la prontezza generale del sistema, mantenendo un buon livello di sicurezza.
  - **Settori di avvio.** Per esaminare i settori di avvio del sistema. Questo settore del disco rigido contiene il codice necessario per inizializzare il processo di avvio. Quando un virus infetta il settore di boot, il disco potrebbe non essere accessibile e potrebbe non essere possibile avviare il sistema e accedere ai dati.

- **Per keylogger.** I keylogger registrano ciò che digiti sulla tastiera per poi inviare queste informazioni tramite Internet a un hacker. L'hacker può trovare informazioni sensibili nei dati rubati, come numeri e password di un conto corrente, e usarle per ottenere benefici personali.
- **Per applicazioni potenzialmente non desiderate (PUA).** Un'applicazione potenzialmente indesiderata (PUA) è un programma che potrebbe essere indesiderato sul PC e a volte viene installato insieme a software freeware. Tali programmi possono essere installati senza il consenso dell'utente (vengono anche chiamati adware) o sono spesso inclusi in modo predefinito nei kit di installazione rapida (ad-supported). Gli effetti potenziali di questi programmi includono la visualizzazione di pop-up, l'installazione di barre degli strumenti non desiderate nel browser predefinito o l'esecuzione di vari processi in background con il conseguente rallentamento delle prestazioni del PC.
- **Archivi**. Seleziona questa opzione se vuoi attivare la scansione all'accesso dei file archiviati. La scansione degli archivi è un processo lento e che richiede molte risorse, che quindi non è consigliato per la protezione in tempo reale. Gli archivi contenenti file infetti non sono una minaccia immediata alla sicurezza del sistema. I malware possono colpire il sistema solo se il file infetto è estratto da un archivio ed eseguito senza aver attivato la scansione all'accesso.

  Se decidi di utilizzare questa opzione, puoi configurare le seguenti opzioni di ottimizzazione:
  - **Dimensione massima archivio (MB).** Puoi impostare un limite massimo accettabile per le dimensioni degli archivi da esaminare all'accesso. Seleziona la casella corrispondente e digita la dimensione massima dell'archivio (in MB).
  - **Profondità massima archivio (livelli).** Seleziona la casella corrispondente e scegli la dimensione massima dell'archivio nel menu. Per le migliori prestazioni, scegli il valore inferiore, mentre per la massima protezione, seleziona il valore maggiore.
- **Scansione rinviata.** Ritardare la scansione migliora le prestazioni del sistema quando si eseguono le operazioni di accesso al file. Per esempio, le risorse di sistema non sono influenzate quando si copiano grandi file. Di norma, questa opzione è attivata.

- **Esamina azioni**. In base al tipo di file rilevato, le seguenti azioni vengono intraprese automaticamente:

– **Azione predefinita per i file infetti.** Bitdefender rileva i file infetti attraverso diversi meccanismi avanzati, che includono tecnologie basate su firme dei malware, apprendimento automatico e intelligenza artificiale (IA). Normalmente, l'agente di sicurezza di Bitdefender può rimuovere il codice malware da un file infetto e ricostruire il file originale. Questa operazione è conosciuta come disinfezione.

  Di norma, se viene rilevato un file infetto, l'agente di sicurezza di Bitdefender tenterà di disinfettarlo automaticamente. Se la disinfezione dovesse fallire, il file sarà messo in quarantena per contenere l'infezione. Puoi modificare questa sequenza consigliata in base alle tue necessità.

  Importante
  Per alcuni particolari tipologie di malware, non è possibile usare la disinfezione perché il file rilevato è interamente dannoso. In questi casi, il file infetto è eliminato dal disco.

– **Azione predefinita per i file sospetti.** I file vengono rilevati come sospetti dall'analisi euristica e da altre tecnologie di Bitdefender. Queste forniscono un tasso di rilevazione elevato, ma in alcuni casi gli utenti devono fare attenzione a determinati falsi positivi (file puliti rilevati come sospetti). I file sospetti non possono essere disinfettati, perché non è disponibile alcuna routine di disinfezione.

  Quando viene rilevato un file sospetto, agli utenti viene negata la possibilità di accedervi per prevenire una potenziale infezione.

Anche se non consigliato, puoi modificare le azioni predefinite. Puoi definire due azioni per ciascun tipo di file. Sono disponibili le seguenti opzioni:

Nega l'accesso
Negare l'accesso ai file rilevati.

Importante
Per endpoint Mac, viene intrapresa l'azione **Sposta in quarantena** al posto di **Nega l'accesso**.

Disinfetta
Rimuovi il codice malware dai file infetti. Si consiglia di impostarla sempre come prima azione da intraprendere sui file infetti.

Elimina
Elimina i file rilevati dal disco, senza alcun avviso. È consigliabile evitare di usare questa azione.

Sposta i file in quarantena
Sposta i file rilevati dalla loro posizione originale alla cartella di quarantena. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Puoi gestire i file in quarantena dalla pagina Quarantena della console.

Non fare nulla
Segnalare solo i file infetti rilevati da Bitdefender.

La scheda **Avanzate** include anche la scansione all'accesso per macchine Linux. Usa la casella per attivarla o disattivarla.

Nella tabella sottostante, puoi configurare le cartelle Linux che vuoi esaminare. Di norma, ci sono cinque valori, ognuno corrispondente a una precisa posizione sugli endpoint: `/home`, `/bin`, `/sbin`, `/usr`, `/etc`.

Per aggiungere nuovi valori:

- Scrivi il nome di ogni posizione personalizzata nel campo di ricerca, nel lato superiore della tabella.
- Seleziona le cartelle predefinite nell'elenco mostrato quando, cliccando sulla freccia nel lato destro del campo di ricerca.

Clicca sul pulsante ⊕ **Aggiungi** per salvare una posizione nella tabella e sul pulsante ⊗ **Elimina** per rimuoverla.

Vaccino per ransomware

Il vaccino per ransomware immunizza le tue macchine dai ransomware **noti**, bloccando il processo di cifratura persino se il computer è infetto. Usa la casella per attivare o disattivare il vaccino per ransomware.

La funzionalità Vaccino per ransomware è disattivata per impostazione predefinita. Bitdefender Labs analizzano il comportamento dei ransomware più diffusi e con ogni aggiornamento del contenuto di sicurezza rilasciano nuove firme, per affrontare le minacce più recenti.

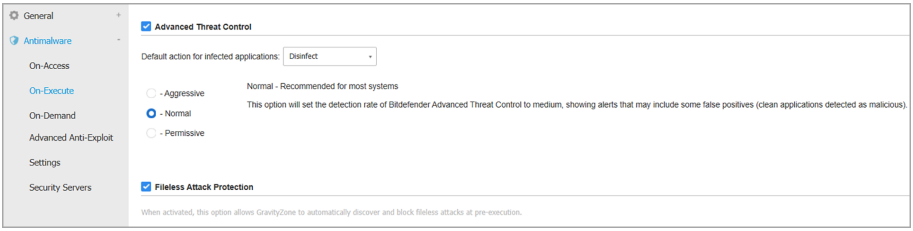
Avvertimento
Per aumentare ulteriormente la protezione dalle infezioni dei ransomware, fai molta attenzione ad allegati sospetti o non richiesti, assicurandoti che il contenuto di sicurezza sia sempre aggiornato.

Nota
Il vaccino per ransomware è disponibile solo con Bitdefender Endpoint Security Tools per Windows.

In esecuzione

In questa sezione, puoi configurare la protezione dai processi dannosi, quando vengono eseguiti. Riguarda i seguenti livelli di protezione:

- Rilevamento minacce basato sul cloud
- Advanced Threat Control
- Protezione attacchi privi di file
- Mitigazione di ransomware



Policy - Impostazioni all'esecuzione

Advanced Threat Control

Nota
Questo modulo è disponibile per:

- Windows for workstations
- Windows for servers
- macOS

Bitdefender Advanced Threat Control è una tecnologia di rilevamento proattiva, che utilizza metodi euristici avanzati per rilevare nuove minacce potenziali in tempo reale.

Advanced Threat Control monitora continuamente le applicazioni in esecuzione sull'endpoint, cercando azioni simili a malware. A ognuna viene assegnato un punteggio e per ogni processo viene poi assegnato un punteggio totale. Quando il punteggio totale di un processo raggiunge una data soglia, il processo è considerato dannoso.

Advanced Threat Control tenterà di disinfettare automaticamente il file rilevato. Se la disinfezione dovesse fallire, Advanced Threat Control eliminerà il file.

Nota
Prima di applicare l'azione di disinfezione, una copia del file viene messa in quarantena, così da poter eventualmente ripristinare il file in un secondo momento, se dovesse rivelarsi essere un falso positivo. Questa azione può essere configurata utilizzando l'opzione **Copia i file in quarantena prima di applicare l'azione di disinfezione** disponibile nella scheda **Antimalware > Impostazioni** delle impostazioni della policy. Questa opzione viene attivata in modo predefinito nei modelli della policy.

Per configurare Advanced Threat Control:

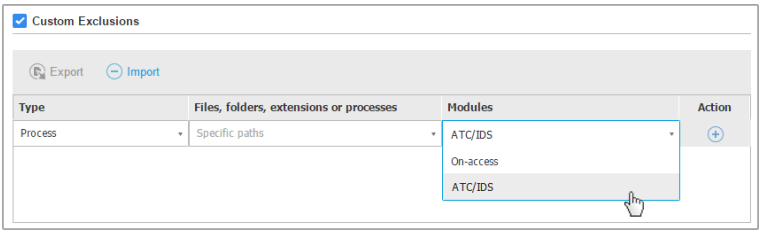
1. Usa la casella per attivare o disattivare Advanced Threat Control.

   Avvertimento
   Disattivando Advanced Threat Control, i computer saranno vulnerabili a malware sconosciuti.

2. L'azione predefinita per le applicazioni infette rilevate da Advanced Threat Control è la disinfezione. Puoi impostare un'altra azione predefinita, utilizzando il menu disponibile:
   - **Blocca**, per negare l'accesso all'applicazione infettata.
   - **Non fare nulla**, solo segnalare le applicazioni infettate rilevate da Bitdefender.
3. Clicca sul livello di sicurezza che si adatta meglio alle tue esigenze (**Aggressivo, Normale o Permissivo**). Usa la descrizione sul lato destro dell'indicatore per scegliere.

   Nota
   Se imposti il livello di protezione più elevato, Advanced Threat Control richiederà un minor numero di comportamenti simili a malware per segnalare un processo.

Ciò comporterà un numero più elevato di applicazioni rilevate e, allo stesso tempo, a un aumento della probabilità di falsi positivi (applicazioni legittime rilevate come dannose).
Si consiglia vivamente di creare regole di eccezioni per le applicazioni più comuni o utilizzate, così da prevenire i falsi positivi (rilevazioni errate di applicazioni legittime). Vai alla scheda Antimalware > Impostazioni e configura le regole di eccezione dei processi ATC/IDS per le applicazioni affidabili.



Policy - Esclusione processi ATC/IDS

Protezione attacchi privi di file

Nota
Questo modulo è disponibile per:

- Windows for workstations
- Windows for servers

Protezione da attacchi privi di file rileva e blocca malware privi di file in fase di pre-esecuzione, oltre a terminare linee di comando dannose in esecuzione in PowerShell, bloccare il traffico dannoso, analizzare il buffer di memoria prima dell'inserimento di codice e bloccare il processo di iniezione del codice.

Mitigazione di ransomware

Mitigazione ransomware utilizza tecnologie di rilevamento e risanamento per mantenere al sicuro i tuoi dati dagli attacchi ransomware. Non importa che il ransomware sia noto o nuovo, GravityZone rileva tentativi di cifratura anomali, bloccandoli. Poi, ripristina i file dalle copie di backup nella propria posizione originale.

Importante
Mitigazione ransomware richiede Active Threat Control.

Nota
Questo modulo è disponibile per:

- Windows for workstations
- Windows for servers

Per configurare Mitigazione ransomware:

1. Seleziona la casella **Mitigazione ransomware** nella sezione della policy **Antimalware > In esecuzione** per attivare la funzionalità.
2. Seleziona le modalità di monitoraggio che vuoi utilizzare:
   - Localmente. GravityZone monitora i processi e rileva gli attacchi ransomware iniziati localmente sull'endpoint. È consigliato per le workstation. Utilizzalo con cautela sui server per via dell'impatto sulle prestazioni.
   - In remoto. GravityZone monitora l'accesso ai percorsi condivisi della rete e rileva gli attacchi ransomware che vengono avviati da un'altra macchina. Utilizza questa opzione se l'endpoint è un file server o ha condivisioni di rete attivate.
3. Seleziona il metodo di ripristino:
   - A richiesta. Puoi scegliere manualmente gli attacchi da cui ripristinare i file. Puoi farlo nella pagina **Rapporti > Attività ransomware** in qualsiasi momento a tua discrezione, ma non oltre 30 giorni dall'attacco. In seguito, il ripristino non sarà più possibile.
   - Automatico. GravityZone ripristina automaticamente i file dopo aver rilevato un attacco ransomware.

   Affinché il ripristino abbia successo, gli endpoint devono essere disponibili.

Una volta attivata, avrai più opzioni per verificare se la tua rete è sotto un attacco ransomware:

- Controlla le notifiche e cerca **Rilevamento ransomware**.

  Per maggiori informazioni su questa notifica, fai riferimento a «Tipi di notifiche» (p. 436).
- Controlla il rapporto **Verifica sicurezza**.

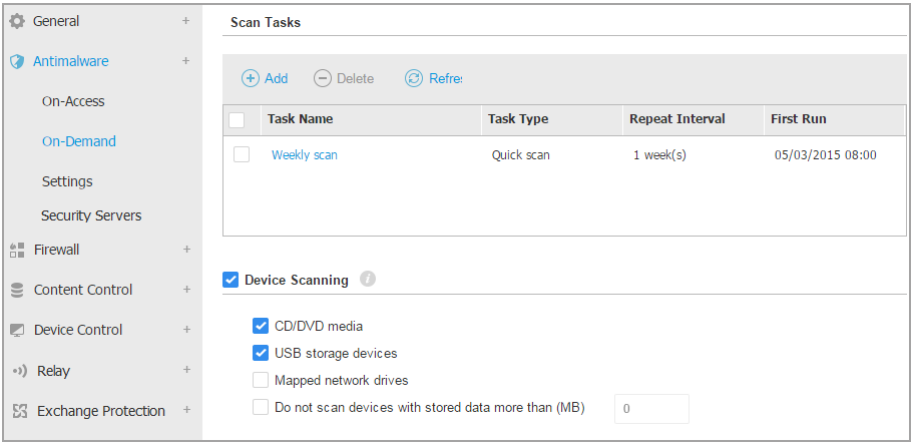
- Controlla la pagina **Attività ransomware**.

  Più avanti, da questa pagina, se necessario, potrai avviare le attività di ripristino. Per maggiori informazioni, fai riferimento a ???.

Nel caso notassi un rilevamento relativo a un processo di cifratura legittimo, avrai determinati percorsi in cui consenti la cifratura dei file o l'accesso remoto da determinate macchine. Aggiungi le eccezioni nella sezione della policy **Antimalware > Impostazioni > Eccezioni personali**. Mitigazione ransomware consente eccezioni per cartelle, processi e IP/maschere. Per maggiori informazioni, fai riferimento a «Eccezioni» (p. 180).

Su richiesta

In questa sezione, puoi aggiungere e configurare attività di scansione antimalware che saranno eseguite regolarmente sui computer di destinazione, in base alla programmazione definita.



Policy - Attività di scansione a richiesta

La scansione viene eseguita silenziosamente in background, indipendentemente dal fatto che l'utente abbia eseguito l'accesso al sistema oppure no.

Anche se non obbligatorio, si consiglia di programmare una scansione di sistema completa settimanale su tutti gli endpoint. Esaminare gli endpoint regolarmente è una misura di sicurezza proattiva che può aiutare a rilevare e bloccare i malware che potrebbero sfuggire alle funzionalità di protezione in tempo reale.

Oltre alle scansioni regolari, puoi anche configurare la rilevazione e scansione automatica dei supporti di memorizzazione esterni.

Gestire le attività di scansione

La tabella Attività di scansione ti informa sulle attività di scansione esistenti, fornendo informazioni importanti su ognuna di loro:

- Nome e tipo di attività.
- Pianificazione in base alla quale l'attività viene eseguita regolarmente (ricorrenza).
- Il momento in cui l'attività è stata eseguita la prima volta.

Puoi aggiungere e configurare i seguenti tipi di attività di scansione:

- La **Scansione veloce** utilizza una scansione in-the-cloud per rilevare eventuali malware in esecuzione sul sistema. In genere eseguire una Scansione veloce richiede meno di un minuto e usa una frazione delle risorse di sistema necessarie per una scansione standard.

  Quando vengono rilevati malware o rootkit, Bitdefender procede automaticamente con la disinfezione. Se, per un qualche motivo, il file non può essere disinfettato, allora viene messo in quarantena. Questo tipo di scansione ignora i file sospetti.

  La Scansione rapida è un'attività di scansione predefinita con opzioni preconfigurate che non possono essere modificate. Puoi aggiungere solo un'attività di scansione rapida per la stessa policy.

- La **Scansione completa** esamina l'intero endpoint per rilevare tutti i tipi di malware che minacciano la sua sicurezza, come virus, spyware, adware, rootkit e altri.

  Bitdefender prova a disinfettare automaticamente tutti i file in cui sono stati rilevati malware. Nel caso in cui i malware non possano essere rimossi, i file vengono messi in quarantena, dove non possono provocare danni. I file sospetti vengono ignorati. Se vuoi comunque intraprendere delle azioni sui file sospetti, o se desideri altre azioni predefinite per i file infetti, scegli di avviare una Scansione personalizzata.

  La Scansione completa è un'attività di scansione predefinita con opzioni preconfigurate che non possono essere modificate. Puoi aggiungere solo un'attività di scansione completa per la stessa policy.

- La **Scansione personalizzata** ti consente di scegliere determinate posizioni da esaminare e configurare le opzioni di scansione.
- La **Scansione di rete** è un tipo di scansione personalizzata che consente di assegnare a un singolo endpoint gestito la scansione delle unità di rete, per poi configurare le opzioni di scansione e le specifiche posizioni da esaminare. Per le attività di scansione della rete, devi inserire le credenziali di un account utente con permessi di lettura/scrittura sulle unità di rete obiettivo, in modo che l'agente di sicurezza possa accedere e intraprendere azioni su queste unità di rete.

  L'attività di scansione di rete ricorrente sarà inviata solo all'endpoint scanner selezionato. Se l'endpoint selezionato non è disponibile, saranno applicate le impostazioni della scansione locale.

  Nota
  Puoi creare attività di scansione di rete solo in una policy già applicata a un endpoint, utilizzabile come scanner.

Oltre alle attività di scansione predefinite (che puoi eliminare o duplicare), puoi creare quante attività di scansione personalizzate o di rete vuoi.

Per creare e configurare una nuova attività, clicca sul pulsante ⊕ **Aggiungi** nel lato destro della tabella. Per modificare le impostazioni di un'attività di scansione esistente, clicca sul nome di quell'attività. Fai riferimento al seguente documento per scoprire come configurare le impostazioni dell'attività.

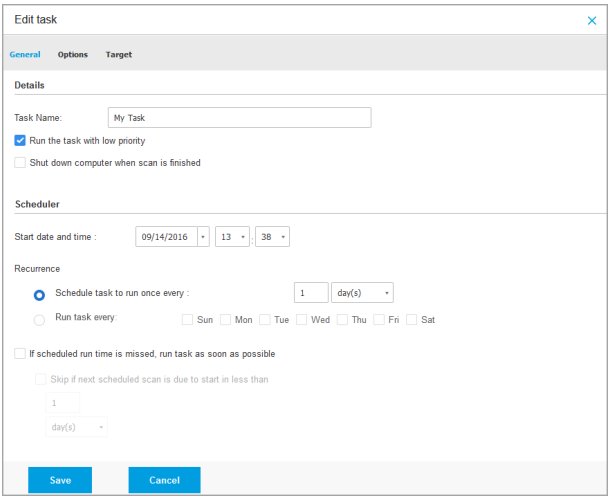
Per rimuovere un'attività dall'elenco, seleziona l'attività e clicca sul pulsante ⊖ **Elimina** sul lato destro della tabella.

Configurare un Compito di Scansione

Le impostazioni dell'attività di scansione sono organizzate con tre schede:

- **Generali**: imposta il nome dell'attività e la programmazione dell'esecuzione.
- **Opzioni**: seleziona un profilo di scansione per una rapida configurazione delle impostazioni di scansione e definisci le impostazioni per una scansione personalizzata.
- **Bersaglio**: seleziona i file e le cartelle da esaminare e definisci le eccezioni della scansione.

Le opzioni sono descritte qui di seguito dalla prima all'ultima scheda:



Policy - Configurare le impostazioni generali delle attività di scansione a richiesta

- **Dettagli** - Seleziona un nome suggestivo per l'attività, così da identificarne facilmente le caratteristiche. Selezionando un nome, considera il bersaglio dell'attività di scansione e possibilmente le impostazioni della scansione.

  Di norma, le attività di scansione vengono eseguite con priorità ridotta. In questo modo, Bitdefender consente ad altri programmi di funzionare più velocemente, incrementando però il tempo necessario per terminare il processo di scansione. Usa la casella **Esegui l'attività con bassa priorità** per disattivare o riattivare questa funzionalità.

  Nota
  Questa opzione di applica solo a Bitdefender Endpoint Security Tools e Endpoint Security (agente datato).

  Seleziona la casella **Spegni il computer al termine della scansione** per spegnere la macchina se non intendi utilizzarla per un certo periodo.

  Nota
  Questa opzione di applica a Bitdefender Endpoint Security Tools, Endpoint Security (agente datato) e Endpoint Security for Mac.

- **Programmazione.** Usa le opzioni di programmazione per configurare il programma della scansione. Puoi impostare la scansione per essere eseguita ogni tot ore, giorni o settimane, partendo da una determinata ora o data.

  Gli endpoint devono essere accesi al momento pianificato. Una scansione programmata non sarà eseguita se la macchina è spenta, in stato di ibernazione o in modalità riposo. In tali situazioni, la scansione sarà rinviata alla volta successiva.

  > **Nota**
  > La scansione programmata sarà eseguita nell'ora locale dell'endpoint di destinazione. Per esempio, se la scansione programmata è impostata per avviarsi alle 18:00 e l'endpoint si trova in un fuso orario diverso della Control Center, la scansione inizierà alle 18:00 (ora dell'endpoint).

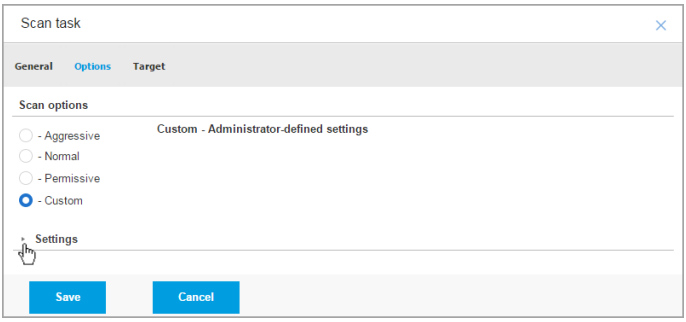
  Facoltativamente, puoi specificare cosa succede quando l'attività di scansione non riesce ad avviarsi al momento pianificato (endpoint offline o spento). Usa l'opzione **Se il periodo di esecuzione pianificato salta, esegui l'attività il prima possibile** in base alle tue esigenze:

  – Se lasci l'opzione deselezionata, verrà effettuato un nuovo tentativo di esecuzione dell'attività di scansione al momento programmato successivo.

  – Se selezioni l'opzione, forzerai l'esecuzione della scansione il prima possibile. Per impostare il momento migliore per la scansione ed evitare di disturbare l'utente durante l'orario di lavoro, seleziona **Salta se la prossima scansione pianificata inizia tra meno di**, quindi specifica l'intervallo desiderato.

- **Opzioni di scansione.** Clicca sul livello di sicurezza che si adatta meglio alle tue esigenze (Aggressivo, Normale o Permissivo). Usa la descrizione sul lato destro dell'indicatore per scegliere.

  In base al profilo selezionato, le opzioni della scansione nella sezione **Impostazioni** sono configurate in maniera automatica. Tuttavia, se lo desideri, puoi configurarle nei dettagli. Per farlo, seleziona la casella **Personalizzate** e vai alla sezione **Impostazioni**.



Attività di scansione - Configurare una scansione personalizzata

- **Tipi di file.** Usa queste opzioni per specificare quali tipi di file vuoi che siano esaminati. Puoi impostare l'agente di sicurezza in modo che esamini tutti i file (indipendentemente dalla loro estensione), solo i file delle applicazioni o determinate estensioni che ritieni essere pericolose. Controllare tutti i file ti garantisce una protezione migliore, mentre controllare solo le applicazioni può essere utile per eseguire una scansione più veloce.

  Nota
  I file delle applicazioni sono più vulnerabili agli attacchi dei malware rispetto ad altri tipi di file. Per maggiori informazioni, fai riferimento a «Tipi di file applicazioni» (p. 458).

  Se vuoi che siano esaminate solo determinate estensioni, seleziona **Estensioni definite dall'utente** nel menu e poi inserisci le estensioni nel campo di modifica, premendo `Invio` dopo ciascuna estensione.

- **Archivi.** Gli archivi contenenti file infetti non sono una minaccia immediata alla sicurezza del sistema. I malware possono colpire il sistema solo se il file infetto è estratto da un archivio ed eseguito senza aver attivato la protezione in tempo reale. Tuttavia, si consiglia di usare questa opzione per rilevare e rimuovere ogni minaccia potenziale, anche se non è immediata.

  Nota
  La scansione dei file archiviati incrementa la durata totale della scansione e richiede più risorse di sistema.

- **Scansiona all'interno degli archivi.** Seleziona questa opzione se vuoi controllare i file archiviati per rilevare eventuali malware. Se decidi di utilizzare questa opzione, puoi configurare le seguenti opzioni di ottimizzazione:
  - **Limita dimensioni archivio a (MB).** Puoi impostare un limite massimo accettabile per le dimensioni degli archivi da esaminare. Seleziona la casella corrispondente e digita la dimensione massima dell'archivio (in MB).
  - **Profondità archivio massima (livelli).** Seleziona la casella corrispondente e scegli la dimensione massima dell'archivio nel menu. Per le migliori prestazioni, scegli il valore inferiore, mentre per la massima protezione, seleziona il valore maggiore.
- **Scansiona archivi e-mail.** Seleziona questa opzione se desideri attivare la scansione dei file allegati ai messaggi e ai database di e-mail, tra cui formati di file come .eml, .msg, .pst, .dbx, .mbx, .tbb e altri.

  Nota
  La scansione degli archivi di e-mail richiede molte risorse e può influenzare le prestazioni del sistema.

- **Funzioni varie.** Seleziona le caselle corrispondenti per attivare le opzioni di scansione desiderate.
  - **Scansiona i settori di avvio.** Per esaminare i settori di avvio del sistema. Questo settore del disco rigido contiene il codice necessario per inizializzare il processo di avvio. Quando un virus infetta il settore di boot, il disco potrebbe non essere accessibile e potrebbe non essere possibile avviare il sistema e accedere ai dati.
  - **Registro della scansione.** Seleziona questa opzione per controllare le chiavi del registro. Il registro di Windows è un database che memorizza le impostazioni e le opzioni di configurazione delle componenti del sistema operativo Windows, oltre a quelle delle applicazioni installate.
  - **Scansiona alla ricerca di rootkit.** Seleziona questa opzione per eseguire una scansione alla ricerca di rootkit e oggetti nascosti usando tale software.
  - **Scansiona per keylogger.** Seleziona questa opzione per eseguire una scansione alla ricerca di software keylogger.

- **Scansiona condivisioni di rete.** Questa opzione esamina le unità di rete installate.

  Per le scansioni veloci, questa opzione è disattivata per impostazione predefinita. Per le scansioni complete, è attivata per impostazione predefinita. Per le scansioni personalizzate, se imposti il livello di sicurezza su **Aggressivo/Normale**, l'opzione **Controlla condivisioni di rete** è attivata automaticamente. Se imposti il livello di sicurezza su **Permissivo**, l'opzione **Controlla condivisioni di rete** è disattivata automaticamente.

- **Scansiona memoria.** Seleziona questa opzione per controllare i programmi in esecuzione nella memoria di sistema.

- **Scansiona i cookie.** Seleziona questa opzione per controllare i cookie memorizzati dai browser sull'endpoint.

- **Scansiona solo file nuovi e modificati.** Controllando solo i file modificati o nuovi, potresti migliorare la prontezza generale del sistema, mantenendo un buon livello di sicurezza.

- **Esamina applicazioni potenzialmente non desiderate (PUA).** Un'applicazione potenzialmente indesiderata (PUA) è un programma che potrebbe essere indesiderato sul PC e a volte viene installato insieme a software freeware. Tali programmi possono essere installati senza il consenso dell'utente (vengono anche chiamati adware) o sono spesso inclusi in modo predefinito nei kit di installazione rapida (ad-supported). Gli effetti potenziali di questi programmi includono la visualizzazione di pop-up, l'installazione di barre degli strumenti non desiderate nel browser predefinito o l'esecuzione di vari processi in background con il conseguente rallentamento delle prestazioni del PC.

- **Azioni.** In base al tipo di file rilevato, le seguenti azioni vengono intraprese automaticamente:

  - **Azione predefinita per i file infetti.** Bitdefender rileva i file infetti attraverso diversi meccanismi avanzati, che includono tecnologie basate su firme dei malware, apprendimento automatico e intelligenza artificiale (IA). Normalmente, l'agente di sicurezza può rimuovere il codice malware da un file infetto e ricostruire il file originale. Questa operazione è conosciuta come disinfezione.

Se viene rilevato un file infetto, l'agente di sicurezza tenterà di disinfettarlo automaticamente. Se la disinfezione dovesse fallire, il file sarà messo in quarantena per contenere l'infezione.

Importante
Per alcuni particolari tipologie di malware, non è possibile usare la disinfezione perché il file rilevato è interamente dannoso. In questi casi, il file infetto è eliminato dal disco.

- **Azione predefinita per i file sospetti.** I file vengono rilevati come sospetti dall'analisi euristica e da altre tecnologie di Bitdefender. Queste forniscono un tasso di rilevazione elevato, ma in alcuni casi gli utenti devono fare attenzione a determinati falsi positivi (file puliti rilevati come sospetti). I file sospetti non possono essere disinfettati, perché non è disponibile alcuna routine di disinfezione.

  Le attività di scansione sono configurate in modo predefinito per ignorare i file sospetti. Potresti volere modificare l'azione predefinita in modo da mettere i file sospetti in quarantena. I file in quarantena vengono inviati regolarmente ai laboratori di Bitdefender per un'ulteriore analisi. Se viene confermata la presenza di malware, viene rilasciata una firma per consentirne la rimozione.

- **Azione predefinita per i rootkit.** I rootkit sono software specializzati che vengono usati per nascondere file al sistema operativo. Anche se non dannosi di natura, i rootkit sono spesso utilizzati per nascondere malware o celare la presenza di un intruso nel sistema.

  I rootkit rilevati e i file nascosti vengono ignorati per impostazione predefinita.

Anche se non consigliato, puoi modificare le azioni predefinite. Puoi specificare una seconda azione da intraprendere se la prima dovesse fallire, oltre a diverse azioni per ciascuna categoria. Scegli dai menu corrispondenti la prima e la seconda azione da intraprendere su ciascun tipo di file rilevato. Sono disponibili le seguenti opzioni:

Non fare nulla
Nessuna azione verrà intrapresa sui file rilevati. Questi file appariranno solo nel registro della scansione.

Disinfetta
Rimuovi il codice malware dai file infetti. Si consiglia di impostarla sempre come prima azione da intraprendere sui file infetti.

Elimina
Elimina i file rilevati dal disco, senza alcun avviso. È consigliabile evitare di usare questa azione.

Sposta i file in quarantena
Sposta i file rilevati dalla loro posizione originale alla cartella di quarantena. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Puoi gestire i file in quarantena dalla pagina Quarantena della console.

- **Obiettivi scansione.** Aggiungi all'elenco tutte le posizioni che vuoi che siano esaminate sui computer di destinazione.

  Per aggiungere un nuovo file o cartella da esaminare:

  1. Scegli una posizione predefinita dal menu a discesa o inserisci i **Percorsi specifici** che vuoi esaminare.
  2. Specifica il percorso dell'oggetto da esaminare nel campo di modifica.
     - Se hai scelto una posizione predefinita, completa il percorso come necessario. Per esempio, per esaminare l'intera cartella `Programmi`, è sufficiente selezionare la posizione predefinita e corrispondente dal menu a discesa. Per esaminare una determinata cartella in `Programmi`, devi completare il percorso aggiunto un backslash (\) e il nome della cartella.
     - Se hai scelto **Percorsi specifici**, inserisci il percorso completo per l'oggetto da esaminare. È consigliabile utilizzare variabili di sistema (laddove appropriato) per assicurarsi che il percorso sia valido su tutti i computer di destinazione.
  3. Clicca sul pulsante ⊕ **Aggiungi** corrispondente.

  Per modificare una posizione esistente, cliccaci sopra. Per rimuovere una posizione dall'elenco, sposta il cursore su di essa e clicca sul pulsante ⊖ **Elimina**.

- Per le attività di scansione della rete, devi inserire le credenziali di un account utente con permessi di lettura/scrittura sulle unità di rete obiettivo, in modo che l'agente di sicurezza possa accedere e intraprendere azioni su queste unità di rete.

- **Eccezioni.** Puoi utilizzare le eccezioni definite nella sezione **Antimalware > Eccezioni** della policy attuale oppure definire eccezioni personalizzate per l'attività di scansione attuale. Per maggiori dettagli sulle eccezioni, fai riferimento a «Eccezioni» (p. 180).

Scansione dispositivo

Puoi configurare l'agente di sicurezza per rilevare ed esaminare automaticamente dispositivi di memorizzazione esterni quando vengono collegati all'endpoint. I dispositivi rilevati rientrano in una di queste categorie:

- CD/DVD
- Dispositivi di archiviazione USB, ad esempio chiavette e dischi rigidi esterni
- I dispositivi con più di una determinata quantità di dati memorizzati.

La scansione dei dispositivi cerca di disinfettare automaticamente i file rilevati come infetti o di spostarli in quarantena, se la pulizia non è possibile. Ricordati che alcuni dispositivi come CD/DVD sono di sola lettura. Non è possibile intraprendere alcuna azione sui file infetti presenti su tali supporti di archiviazione.

Nota
Durante la scansione di un dispositivo, l'utente può accedere a qualsiasi dato dal dispositivo.

Se i pop-up di avviso sono stati attivati nella sezione **Generali > Notifiche**, all'utente sarà chiesto se esaminare oppure no il dispositivo rilevato, invece di avviare la scansione automaticamente.

Quando viene avviata la scansione di un dispositivo:

- Un pop-up di notifica informa l'utente sulla scansione del dispositivo, fatto salvo che i pop-up di notifica siano stati attivati nella sezione **Generali > Notifiche**.

Una volta completata la scansione, l'utente deve verificare le minacce rilevate, se ve ne sono.

Seleziona l'opzione **Scansione dispositivo** per attivare il rilevamento automatico e la scansione dei dispositivi di memorizzazione. Per configurare la scansione del dispositivo individualmente per ciascun tipo di dispositivo, utilizza le seguenti opzioni:

- **Supporti CD/DVD**
- **Dispositivi di archiviazione USB**

- **Non esaminare dispositivi con dati memorizzati superiori a (MB)**. Usa questa opzione per saltare automaticamente la scansione di un dispositivo rilevato se la quantità di dati memorizzati supera la dimensione indicata. Inserisci il limite di dimensione (in megabyte) nel campo corrispondente. Zero significa che non viene applicata alcuna limitazione alle dimensioni.

HyperDetect

Nota
Questo modulo è disponibile per:

- Windows for workstations
- Windows for servers
- Linux

HyperDetect aggiunge un ulteriore livello di sicurezza sulle tecnologie di scansione esistenti (Scansione all'accesso, a richiesta e del traffico), per combattere contro la nuova generazione di attacchi informatici, incluso le minacce persistenti avanzate. HyperDetect migliora i moduli di protezione Antimalware e Controllo contenuti con la sua potente euristica basata su intelligenza artificiale e apprendimento automatico.

Con la sua capacità di prevedere attacchi mirati e rilevare i malware più sofisticati in fase di pre-esecuzione, HyperDetect espone le minacce molto più velocemente delle tecnologie basate su firme o scansione comportamentale.

Per configurare HyperDetect:

1. Usa la casella **HyperDetect** per attivare o disattivare il modulo.
2. Seleziona il tipo di minaccia da cui vuoi proteggere la tua rete. Di norma, la protezione viene attivata per tutti i tipi di minaccia: attacchi mirati, file sospetti e traffico di rete, exploit, ransomware o grayware.

   Nota
   L'euristica per il traffico di rete richiede che **Controllo contenuti > Scansione traffico** siano attivati.

3. Personalizza il livello di protezione dalle minacce dei tipi selezionati.

   Usa l'interruttore principale nella parte superiore dell'elenco delle minacce per selezionare un livello unico di protezione per tutti i tipi di minacce, oppure seleziona livelli individuali per una protezione personalizzata.

Impostando il modulo a un determinato livello, comporterà una serie di azioni intraprese fino a quel livello. Per esempio, se impostato su **Normale**, il modulo rileva e limita le minacce che attivano le soglie **Permissivo** e **Normale**, ma non quello **Aggressivo**.

La protezione aumenta da **Permissivo** ad **Aggressivo**.

Ricordati che una rilevazione aggressiva potrebbe comportare falsi positivi, mentre una permissiva potrebbe esporre la tua rete ad alcune minacce. Prima si consiglia di impostare il livello di protezione al massimo e poi abbassarlo in caso di molti falsi positivi, finché non si ottieni l'equilibrio ottimale.

Nota
Ogni volta che si attiva la protezione per un certo tipo di minaccia, la rilevazione viene impostata automaticamente sul valore predefinito (livello **Normale**).

4. Nella sezione **Azioni**, configura come HyperDetect dovrebbe reagire alle rilevazioni. Usa le opzioni del menu a discesa per impostare l'azione da intraprendere sulle minacce:
   - Per i file: nega accesso, disinfetta, elimina, metti in quarantena o solo segnala il file.
   - Per il traffico di rete: blocca o solo segnala il traffico sospetto.
5. Seleziona la casella **Estendi la segnalazione ai livelli superiori** accanto al menu a discesa, se desideri visualizzare le minacce rilevate a livelli di protezione superiori rispetto a quello impostato.

Se sei incerto sulla configurazione attuale, puoi facilmente ripristinare le impostazioni iniziali, cliccando sul pulsante **Predefinito** nel lato inferiore della pagina.

Anti-exploit avanzato

Nota
Questo modulo è disponibile per:
- Windows for workstations

L'anti-exploit avanzato è una tecnologia proattiva che rileva gli exploit in tempo reale. Basato sull'apprendimento automatico, protegge da una serie di exploit noti e sconosciuti, inclusi gli attacchi privi di file relativi alla memoria.

Per attivare la protezione contro gli exploit, seleziona la casella **Anti-exploit avanzato**.

L'Anti-exploit avanzato è configurato in modo da essere eseguito con le impostazioni consigliate. Puoi regolare la protezione in modo diverso, se necessario. Per ripristinare le impostazioni iniziali, clicca sul link **Ripristina predefiniti** a destra dell'intestazione della sezione.

Le impostazioni dell'anti-exploit di GravityZone sono suddivise in tre sezioni:

- **Rilevamenti a livello di sistema**

  Le tecniche anti-exploit di questa sezione monitorano i processi del sistema che sono bersaglio di exploit.

  Per maggiori informazioni sulle tecniche disponibili e su come configurarne le impostazioni, fai riferimento a «Configurare la mitigazione a livello di sistema» (p. 175).

- **Applicazioni predefinite**

  Il modulo Anti-exploit avanzato è preconfigurato con un elenco di applicazioni comuni maggiormente esposte agli exploit, come Microsoft Office, Adobe Reader o Flash Player.

  Per maggiori informazioni sulle tecniche disponibili e su come configurarne le impostazioni, fai riferimento a «Configurare tecniche specifiche in base all'applicazione» (p. 176).

- **Applicazioni aggiuntive**

  In questa sezione puoi aggiungere e configurare la protezione per tutte le altre applicazioni che desideri.

  Per maggiori informazioni sulle tecniche disponibili e su come configurarne le impostazioni, fai riferimento a «Configurare tecniche specifiche in base all'applicazione» (p. 176).

Puoi espandere o comprimere ciascuna sezione cliccandone l'intestazione. In questo modo puoi raggiungere rapidamente le impostazioni che vuoi configurare.

Configurare la mitigazione a livello di sistema

In questa sezione sono incluse le seguenti sezioni:

Tecnica	Descrizione
Escalation dei privilegi	Impedisce ai processi di ottenere privilegi non autorizzati e di accedere alle risorse. Azione predefinita: Termina processo
Protezione processo LSASS	Protegge il processo LSASS da fughe di dati segreti come gli hash delle password e le impostazioni di sicurezza. Azione predefinita: Blocca processo

Queste tecniche anti-exploit sono abilitate per impostazione predefinita. Per disabilitare un'opzione, deseleziona la relativa casella.

Facoltativamente, puoi modificare l'azione che viene eseguita automaticamente in seguito al rilevamento. Scegli una delle azioni disponibili dal relativo menu:

- **Termina processo**: termina immediatamente il processo interessato dall'exploit.
- **Blocca processo**: impedisce al processo dannoso di accedere a risorse non autorizzate.
- **Solo segnalazione**: GravityZone segnala l'evento senza intraprendere alcuna azione di mitigazione. Puoi visualizzare i dettagli dell'evento nella notifica di **Anti-exploit avanzato** e nei rapporti Applicazioni bloccate e Verifica sicurezza.

Configurare tecniche specifiche in base all'applicazione

Sia le applicazioni predefinite che quelle aggiuntive condividono la stessa serie di tecniche anti-exploit. Li trovi descritti nel presente documento:

Tecnica	Descrizione
Emulazione ROP	Rileva i tentativi di rendere eseguibili pagine di memoria per i dati, usando la tecnica ROP (Return-Oriented Programming). Azione predefinita: Termina processo
Stack Pivot ROP	Rileva i tentativi di assunzione del controllo del flusso di dati tramite la tecnica ROP, validando la posizione dello stack. Azione predefinita: Termina processo

Tecnica	Descrizione
Chiamata non valida ROP	Rileva i tentativi di assunzione del controllo del flusso di dati tramite la tecnica ROP, validando i chiamanti di funzionalità sensibili del sistema. Azione predefinita: Termina processo
Stack ROP non allineato	Rileva i tentativi di corruzione dello stack tramite la tecnica ROP, validando l'allineamento degli indirizzi dello stack. Azione predefinita: Termina processo
ROP Return To Stack	Rileva i tentativi di esecuzione di codice direttamente dallo stack tramite la tecnica ROP, validando l'intervallo di indirizzi dei mittenti. Azione predefinita: Termina processo
ROP Make Stack Executable	Rileva i tentativi di corruzione dello stack tramite la tecnica ROP, validando la protezione della pagina dello stack. Azione predefinita: Termina processo
Flash generico	Rileva i tentativi di exploit di Flash Player. Azione predefinita: Termina processo
Payload Flash	Rileva i tentativi di esecuzione di codice dannoso in Flash Player, scansionando gli oggetti Flash nella memoria. Azione predefinita: Termina processo
VBScript Generic	Rileva i tentativi di exploit di VBScript. Azione predefinita: Termina processo
Esecuzione shellcode	Rileva i tentativi di creazione di nuovi processi o di download di file, tramite shellcode. Azione predefinita: Termina processo
Shellcode LoadLibrary	Rileva i tentativi di esecuzione di codice tramite percorsi di rete, usando shellcode. Azione predefinita: Termina processo
Anti-Detour	Rileva i tentativi di ignorare i controlli di sicurezza per la creazione di nuovi processi. Azione predefinita: Termina processo

Tecnica	Descrizione
Shellcode EAF (Export Address Filtering)	Rileva i tentativi di accesso a funzionalità sensibili del sistema da parte di codice dannoso da esportazioni DLL. Azione predefinita: Termina processo
Thread shellcode	Rileva i tentativi di inserimento di codice malevolo, validando thread di nuova creazione. Azione predefinita: Termina processo
Anti-Meterpreter	Rileva i tentativi di creazione di una reverse shell, tramite la scansione di pagine di memoria eseguibili. Azione predefinita: Termina processo
Creazione processi obsoleti	Rileva i tentativi di creazione di nuovi processi tramite tecniche obsolete. Azione predefinita: Termina processo
Creazione processi figlio	Blocca la creazione di qualsiasi processo figlio. Azione predefinita: Termina processo
Applica DEP Windows	Impone a Protezione esecuzione programmi di bloccare l'esecuzione di codice da pagine dati. Impostazione predefinita: disattivata
Applica trasferimento modulo (ASLR)	Impedisce il caricamento di codice in posizioni prevedibili, tramite la rilocazione di moduli di memoria. Impostazione predefinita: attivata
Emerging Exploits	Protegge da ogni minaccia emergente o exploit. Per questa categoria vengono usati aggiornamenti rapidi, prima che possano essere effettuate modifiche più consistenti. Impostazione predefinita: attivata

Per monitorare altre applicazioni rispetto a quelle predefinite, clicca su pulsante **Aggiungi applicazione** disponibile nella parte superiore e in quella inferiore della pagina.

Per configurare le impostazioni anti-exploit per un'applicazione:

1. Per le applicazioni già presenti, clicca sul nome dell'applicazione. Per le nuove applicazioni, clicca sul pulsante **Aggiungi**.

Verrà aperta una nuova pagina che mostra tutte le tecniche e le relative impostazioni per l'applicazione selezionata.

Importante
Fai attenzione quando aggiungi nuove applicazioni da monitorare. Bitdefender non può garantire la compatibilità con tutte le applicazioni. Pertanto consigliamo di provare la funzionalità su alcuni endpoint non critici, prima di implementarla nella rete.

2. Quando aggiungi una nuova applicazione, inserisci il nome dell'applicazione e il nome dei suoi processi nei campi dedicati. Usa il punto e virgola (;) per separare i nomi dei processi.
3. Per controllare rapidamente la descrizione di una tecnica, clicca sulla freccia accanto al suo nome.
4. Seleziona o deseleziona le caselle di controllo delle tecniche di exploit, come necessario.

   Per selezionare tutte le tecniche, usa l'opzione **Tutto**.
5. Se necessario, modifica l'azione automatica eseguita in seguito al rilevamento. Scegli una delle azioni disponibili dal relativo menu:
   - **Termina processo**: termina immediatamente il processo interessato dall'exploit.
   - **Solo segnalazione**: GravityZone segnala l'evento senza intraprendere alcuna azione di mitigazione. Puoi vedere i dettagli dell'evento nella notifica e nei rapporti di **Anti-exploit avanzato**.

   Per impostazione predefinita, tutte le tecniche per le applicazioni predefinite sono configurate in modo da mitigare il problema. Le tecniche per le applicazioni aggiuntive sono invece configurate in modo da segnalare solamente l'evento.

   Per modificare rapidamente e in una sola volta l'azione da intraprendere per tutte le tecniche, seleziona l'azione dal menu associato con l'opzione **Tutto**.

Per ritornare alle impostazioni generali anti-exploit, clicca sul pulsante **Indietro** nella parte superiore della pagina.

Impostazioni

In questa sezione, puoi configurare le impostazioni della quarantena e le regole di eccezione della scansione.

- Configurazione delle impostazioni di quarantena
- Configurare le eccezioni della scansione

Quarantena

Puoi configurare le seguenti opzioni per i file messi in quarantena dagli endpoint di destinazione:

- **Elimina i file più vecchi di (giorni).** Di norma, i file in quarantena più vecchi di 30 giorni sono eliminati automaticamente. Se vuoi modificare questo intervallo, scegli un'opzione diversa dal menu.
- **Invia file messi in quarantena a Bitdefender Labs ogni (ore).** Di norma, i file messi in quarantena vengono inviati automaticamente ai laboratori di Bitdefender ogni ora. Puoi modificare l'intervallo di tempo tra i file che vengono messi in quarantena (di norma è un'ora). I file campioni saranno analizzati dai ricercatori antimalware di Bitdefender. Se viene confermata la presenza di malware, viene rilasciata una firma per consentirne la rimozione.
- **Riesamina la quarantena dopo gli aggiornamenti del contenuto di sicurezza**. Mantieni questa opzione selezionata per esaminare manualmente i file in quarantena dopo ogni aggiornamento del contenuto di sicurezza. I file puliti vengono spostati automaticamente alla loro ubicazione originale.
- **Copia i file in quarantena prima di applicare l'azione di disinfezione**. Seleziona questa opzione per impedire perdite di dati in caso di falsi positivi e copiare ciascun file rilevato come infetto in quarantena prima di applicare l'azione di disinfezione. In seguito potrai ripristinare i file legittimi dalla pagina **Quarantena**.
- **Consenti agli utenti di intraprendere azioni sulla quarantena in locale.** Questa opzione controlla le azioni che gli utenti dell'endpoint possono intraprendere sui file locali in quarantena tramite l'interfaccia di Bitdefender Endpoint Security Tools. Di norma, gli utenti locali possono ripristinare o eliminare i file in quarantena dal proprio computer utilizzando le opzioni disponibili in Bitdefender Endpoint Security Tools. Disattivando questa opzione, gli utenti non avranno più accesso ai pulsanti d'azione per i file in quarantena nell'interfaccia di Bitdefender Endpoint Security Tools.

Eccezioni

L'agente di sicurezza di Bitdefender può escludere dalla scansione determinati tipi di elementi. Le eccezioni dell'antimalware devono essere utilizzate in circostanze

particolari o in seguito a raccomandazioni di Microsoft o Bitdefender. Per un elenco aggiornato delle eccezioni suggeriste da Microsoft, fai riferimento a questo articolo.

In questa sezione, puoi configurare l'uso di diversi tipi di eccezioni disponibili con l'agente di sicurezza di Bitdefender.

- Le **Eccezioni integrate** sono attivate per impostazione predefinita e incluso nell'agente di sicurezza di Bitdefender.

  Puoi scegliere di disattivare le eccezioni integrate, se desideri esaminare tutti i tipi di elementi, ma questa azione influenzerà notevolmente le prestazioni della macchina, aumentando anche il tempo necessario per la scansione.

- Puoi anche stabilire **eccezioni personalizzate** per applicazioni sviluppate internamente o per strumenti personalizzati, in base alle tue esigenze.

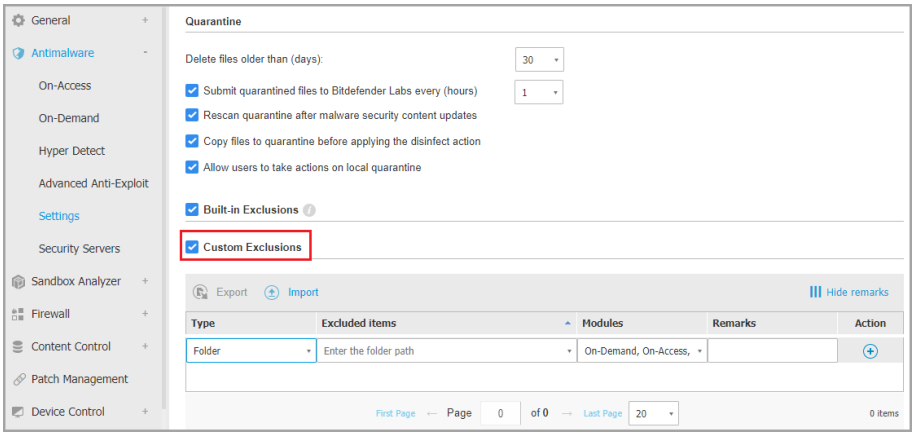
  Le eccezioni personalizzate dell'antimalware vengono applicate a uno o più dei seguenti metodi di scansione:

  - Scansione all'accesso
  - Scansione a richiesta
  - Advanced Threat Control
  - Protezione attacchi privi di file
  - Mitigazione di ransomware

  Importante

  - Se hai un file test EICAR che utilizzi periodicamente per testare la protezione antimalware, dovresti escluderlo dalla scansione all'accesso.
  - Se utilizzi VMware Horizon View 7 e App Volumes AppStacks, fai riferimento a questo documento di VMware.

  Per escludere elementi specifici dalla scansione, seleziona l'opzione **Eccezioni personalizzate**, poi aggiungi le regole nella tabella sottostante.



Policy di computer e virtual machine - Eccezioni personalizzate

Per aggiungere una regola di eccezione personalizzata:

1. Seleziona il tipo di eccezione nel menu:
   - **File**: solo il file specificato
   - **Cartella**: tutti i file e i processi all'interno della cartella specificata e di tutte le sue sottocartelle
   - **Estensione**: tutti gli elementi aventi l'estensione specificata
   - **Processo**: qualsiasi oggetto a cui il processo escluso ha accesso
   - **Hash file**: il file con l'hash specificato
   - **Hash certificato**: tutte le applicazioni sotto l'hash del certificato specificato (impronta)
   - **Nome della minaccia**: ogni elemento con il nome di rilevamento (non disponibile per i sistemi operativi Linux)
   - **Linea di comando**: la linea di comando specificata (disponibile solo per i sistemi operativi Windows)

Avvertimento
Negli ambienti VMware privi di agente integrati con vShield, puoi escludere solo cartelle ed estensioni. Installando Bitdefender Tools sulle virtual machine, puoi anche escludere file e processi.

Durante il processo di installazione, configurando il pacchetto, devi selezionare la casella **Impiega endpoint con vShield quando viene rilevato un ambiente VMware integrato con vShield**. Per maggiori informazioni, fai riferimento alla sezione **Creare pacchetti di installazione** della Guida di installazione.

2. Fornisci i dettagli specifici per il tipo di eccezione selezionato:

   File, Cartella o Processo

   Inserisci il percorso dell'elemento da escludere dalla scansione. Per scrivere il percorso, hai diverse opzioni utili a tua disposizione:

   – Indicare esplicitamente il percorso.

     Ad esempio: `C: emp`

     Per aggiungere eccezioni per percorsi UNC, usa una qualsiasi delle seguenti sintassi:

     `\\hostName\shareName\filePath`

     `\\IPaddress\shareName\filePath`

   – Usa le variabili di sistema disponibili nel menu a discesa.

     Per le esclusioni dei processi, devi anche aggiungere il nome del file eseguibile dell'applicazione.

     Per esempio:

     `%ProgramFiles%` - esclude la cartella Programmi

     `%WINDIR%\system32` – esclude la cartella system32 all'interno della cartella Windows

     Nota
     È consigliabile utilizzare variabili di sistema (laddove appropriato) per assicurarsi che il percorso sia valido su tutti i computer di destinazione.

   – Usa i caratteri jolly.

     L'asterisco (*) sostituisce lo zero o più caratteri. Il punto di domanda (?) sostituisce esattamente un carattere. Puoi utilizzare diversi punti di domanda per definire qualsiasi combinazione di un dato numero di caratteri. Per esempio, ??? sostituisce una qualsiasi combinazione formata esattamente da tre caratteri.

Per esempio:

Esclusione di file:

`C:\Test\*` – esclude tutti i file della cartella di prova

`C:\Test\*.*png` – esclude tutti i file PNG della cartella di prova

Esclusione di una cartella:

`C:\Test\*` - esclude tutte le cartelle incluse nella directory Test

Esclusione di un processo:

`C:\Program Files\WindowsApps\Microsoft.Not??.exe` – esclude i processi delle note di Microsoft.

Nota
L'esclusione dei processi non supporta i caratteri jolly nei sistemi operativi Linux.

Estensione

Inserisci una o più estensioni dei file da escludere dalla scansione, separate da un punto e virgola (;). Puoi inserire le estensioni con o senza il punto iniziale. Per esempio, inserisci txt per escludere i file di testo.

Nota
Sui sistemi basati su Linux, le estensioni dei file sono sensibili alle maiuscole e i file con lo stesso nome ma diversa estensione vengono considerati come elementi distinti. Per esempio, `file.txt` è diverso da `file.TXT`.

Hash file, Hash certificato, Nome minaccia o Linea di comando

Inserisci l'hash del file, l'impronta di certificazione (hash), il nome esatto della minaccia o la linea di comando, a seconda della regola di eccezione. Puoi usare un elemento per ciascuna eccezione.

3. Seleziona i metodi di scansione a cui applicare la regola. Alcune eccezioni possono essere rilevanti solo per la scansione all'accesso, per la scansione a richiesta o ATC/IDS, mentre altre possono essere consigliate per tutti e tre i moduli.
4. Facoltativamente, clicca il pulsante **Mostra note** per aggiungere una nota relativa alla regola nella colonna **Note**.

5. Clicca sul pulsante ⊕ **Aggiungi**.

   La nuova regola sarà aggiunta all'elenco.

Per rimuovere una regola dalla lista, clicca sul pulsante ⊗ **Elimina** corrispondente.

Importante
Ricordati che le eccezioni per la scansione a richiesta NON saranno applicate alla scansione contestuale. La scansione contestuale viene avviata cliccando con il pulsante destro del mouse su un file o una cartella e seleziona **Esamina con Bitdefender Endpoint Security Tools**.

Importare ed esportare le eccezioni

Se intendi riutilizzare le regole di eccezione in più policy, puoi scegliere di esportarle e importarle.

Per esportare le eccezioni personalizzate:

1. Clicca su **Esporta** nel lato superiore della tabella delle eccezioni.
2. Salva il file CSV sul computer. In base alle impostazioni del tuo browser, il fil potrebbe essere scaricato automaticamente oppure ti sarà chiesto di salvarlo in una determinata posizione.

Ogni riga nel file CSV corrisponde a una sola regola, con i vari campi nel seguente ordine:

```
<exclusion type>, <object to be excluded>, <modules>
```

Questi sono i valori disponibili per i campi CSV:

Tipo di eccezione:

- 1, per le eccezioni dei file
- 2, per le eccezioni delle cartelle
- 3, per le eccezioni delle estensioni
- 4, per le eccezioni dei processi
- 5, per le eccezioni hash file
- 6, per le eccezioni hash certificato

7, per le eccezioni di tipo nome minaccia

8, per le eccezioni di tipo linea di comando

Elemento da escludere:
Un percorso o un'estensione di un file

Moduli:
1, per la scansione a richiesta

2, per la scansione all'accesso

3, per tutti i moduli

4, per ATC/IDS

Per esempio, un file CSV contenente eccezioni antimalware potrebbe apparire come questo:

```
1,"d:\\temp",1
1,%WinDir%,3
4,"%WINDIR%\\system32",4
```

Nota
I percorsi di Windows devono avere la doppia barra inversa (\\). Per esempio, `%WinDir%\\System32\\LogFiles`.

Per importare le eccezioni personalizzate:

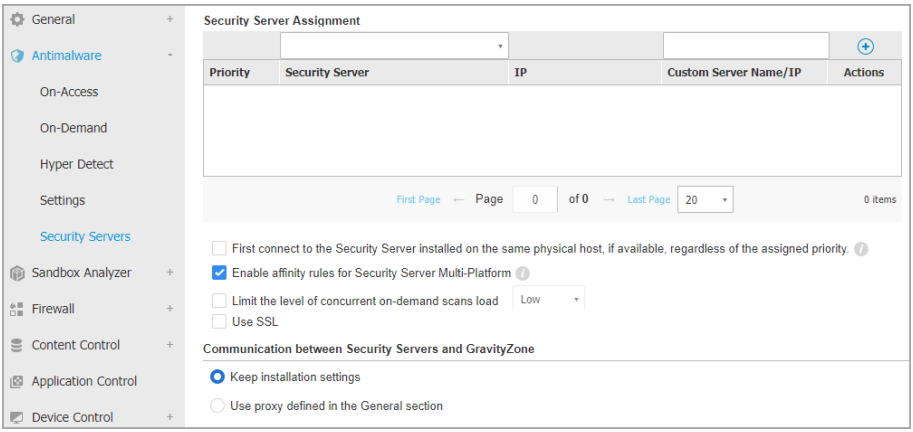
1. Clicca su **Importa**. Si aprirà la finestra **Importa eccezioni policy**.
2. Clicca su **Aggiungi** e poi seleziona il file CSV.
3. Clicca su **Salva**. La tabella viene riempita con le regole valide. Se il file CSV contiene regole non valide, un avviso ti informa dei numeri di riga corrispondenti.

Security Server

In questa sezione puoi configurare:

- Assegnazione del Security Server
- Impostazioni specifiche del Security Server

Nota
La licenza del tuo prodotto potrebbe non includere questa funzionalità.



Policy - Computer e virtual machine - Antimalware - Server di sicurezza

Assegnazione di Security Server

Puoi assegnare uno o più Security Server agli endpoint bersaglio e impostare la priorità con cui gli endpoint sceglieranno un Security Server per inviare le richieste di scansione.

Nota
Si consiglia di usare i Security Server per esaminare le virtual machine o i computer con basse risorse.

Per assegnare un Security Server agli endpoint bersaglio, aggiungi i Security Server che vuoi usare nella tabella **Assegnazione Security Server**, come segue:

1. Clicca sull'elenco a discesa **Security Server** e seleziona un Security Server.
2. Se il Security Server è in DMZ o dietro un server NAT, inserisci l'FQDN o l'IP del server NAT nel campo **Nome/IP server personale**

Importante
Assicurati che il port forwarding sia configurato correttamente sul server NAT così che il traffico dagli endpoint possa raggiungere il Security Server. Per maggiori

dettagli sulle porte, fai riferimento all'articolo della KB Porte di comunicazione di GravityZone.

3. Clicca sul pulsante ⊕ **Aggiungi** nella colonna **Azioni**.

   Il Security Server viene aggiunto all'elenco.

4. Ripeti i passaggi precedenti per aggiungere altri Security Server, se disponibile o necessario.

Per impostare la priorità dei Security Server:

1. Usa le frecce su e giù disponibili nella colonna **Azioni** per aumentare o diminuire la priorità di ogni Security Server.

   Assegnando più Security Server, quello in cima all'elenco ha la priorità maggiore e sarà selezionato per primo. Se tale Security Server non è disponibile o è sovraccaricato, sarà selezionato il prossimo Security Server. La scansione del traffico viene reindirizzata al primo Security Server disponibile e con un carico opportuno.

Per rimuovere un Security Server dall'elenco, clicca sul corrispondente pulsante ⊗ **Elimina** nella colonna **Azioni**.

Impostazioni del Security Server

Assegnando la policy ai Security Server, puoi configurare le seguenti impostazioni:

- **Limita il numero di scansioni a richiesta concomitanti**

  Eseguire più attività di scansione contemporanee su virtual machine che condividono lo stesso archivio dati può creare storm di scansione antimalware. Per impedire ciò e consentire solo un determinato numero di attività di scansione alla volta:

  1. Seleziona l'opzione **Limita il numero di scansioni a richieste contemporanee**.
  2. Seleziona il livello delle attività di scansione contemporanee nel menu a discesa. Puoi scegliere un livello predefinito o inserire un valore personale.

     La formula per trovare il limite massimo di attività di scansioni per ogni livello predefinito è: `N = a x MAX(b ; vCPU - 1)`, dove:

     – `N` = limite massimo di attività di scansione

- `a` = coefficiente di moltiplicazione con i seguenti valori: `1` - per basso; `2` - per medio; `4` - per alto
- `MAX(b;vCPU-1)` = una funzione che riporta il numero massimo di slot di scansione disponibili sul Security Server.
- `b` = Il numero predefinito di slot di scansione a richiesta, che attualmente è impostato su quattro.
- `vCPU` = numero di CPU virtuali assegnate al Security Server

Per esempio:

Per un Security Server con 12 CPU e un livello alto di scansioni contemporanee, abbiamo un limite di:

`N = 4 x MAX(4 ; 12-1) = 4 x 11 = 44` attività di scansione a richiesta contemporanee.

- **Attiva regole di affinità per Security Server Multi-Platform**

  Scegli quale comportamento il Security Server dovrebbe avere quando il suo host entra in modalità manutenzione:

  - Se attivato, il Security Server resta legato all'host e GravityZone lo spegne. Al termine della manutenzione, GravityZone riavvia automaticamente il Security Server.

    Questo è il comportamento predefinito.

  - Se disattivato, il Security Server viene spostato a un altro host e continua a operare. In questo caso, il nome del Security Server cambia in Control Center per indicare l'host precedente. Il cambio di nome persiste finché il Security Server non torna al suo host nativo.

    Se le risorse sono sufficienti, il Security Server può arrivare su un host dove è installato un altro Security Server.

- **Usa SSL**

  Attiva questa opzione se desideri cifrare la connessione fra gli endpoint di destinazione e le appliance Security Server specificate.

  Di norma, GravityZone utilizza certificati di sicurezza auto-firmati. Puoi modificarli con i tuoi certificati nella pagina **Configurazione > Certificati** di Control Center. Per maggiori informazioni, fai riferimento al capitolo "Impostazioni di configurazione di Control Center" della Guida di installazione.

- **Comunicazione tra Security Server e GravityZone**

  Scegli una delle opzioni disponibili per definire le preferenze del tuo proxy per la comunicazione tra le macchine Security Server e GravityZone:

  – **Mantieni impostazioni installazione** per utilizzare le stesse impostazioni proxy definite con il pacchetto di installazione.

  – **Usa proxy definito nella sezione General**, per usare le impostazioni proxy definite nella policy attuale, nella sezione **Generale > Impostazioni**.

  – **Non usare il proxy**, quando gli endpoint bersaglio non comunicano con determinate componenti di Bitdefender tramite proxy.

7.2.3. Sandbox Analyzer

Nota
Questo modulo è disponibile per:

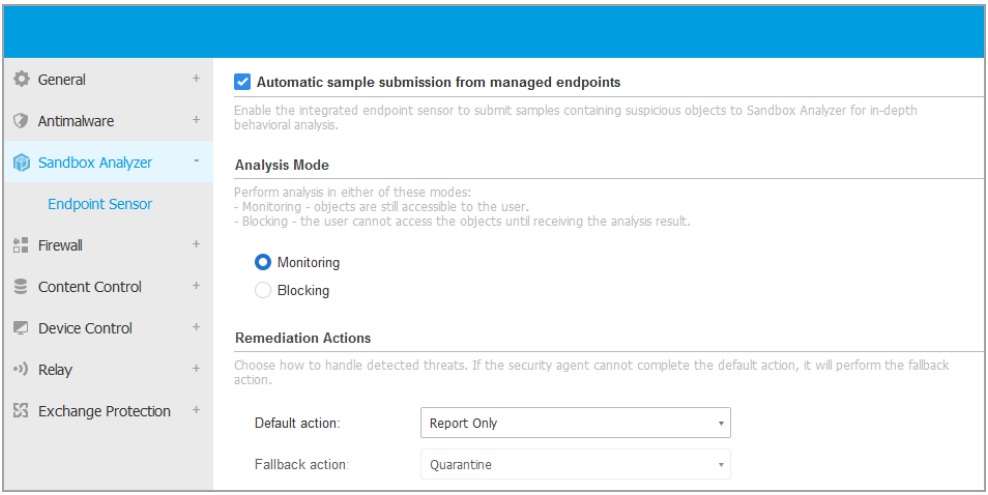
- Windows for workstations
- Windows for servers

Sandbox Analyzer fornisce un potente livello di protezione dalle minacce avanzate, eseguendo un'analisi automatica e approfondita dei file sospetti non ancora firmati dai motori antimalware di Bitdefender.

In questa sezione, puoi configurare le impostazioni di Sandbox Analyzer per l'invio automatico tramite Bitdefender Endpoint Security Tools. Per dettagli sull'invio manuale, fai riferimento a «Invio manuale» (p. 430).

Sensore endpoint

Bitdefender Endpoint Security Tools può fungere da sensore di feeding per Sandbox Analyzer dagli endpoint Windows.



Policy > Sandbox Analyzer > Sensore endpoint

Configura le impostazioni di Sandbox Analyzer per l'invio automatico:

1. **Impostazioni connessione**. Il sensore dell'endpoint è configurato in modo da inviare campioni a un'istanza predefinita di Sandbox Analyzer ospitata da Bitdefender, in base alla tua area geografica.
   - **Usa Cloud Sandbox Analyzer** - Il sensore endpoint invierà i campioni all'istanza di Sandbox Analyzer ospitata da Bitdefender, in base alla tua regione.
   - **Usa istanza locale di Sandbox Analyzer** - Il sensore endpoint invierà i campioni all'istanza di Sandbox Analyzer On-Premises. Seleziona l'istanza preferita di Sandbox Analyzer nel menu a discesa.

   Se la tua rete è dietro un server proxy o un firewall, puoi configurare un proxy per connettersi a Sandbox Analyzer, selezionando la casella **Usa configurazione proxy**.

   Devi compilare i seguenti campi:
   - **Server** - L'IP del server proxy.
   - **Porta** - La porta utilizzata per connettersi al server proxy.
   - **Nome utente** - Un nome utente riconosciuto dal proxy.

- **Password** - La password valida per l'utente indicato.

2. Seleziona la casella **Invio campione automatico da endpoint gestiti** per attivare l'invio automatico di file sospetti da Sandbox Analyzer.

   Importante

   - Sandbox Analyzer richiede la scansione all'accesso. Assicurati di aver attivato il modulo **Antimalware > Scansione all'accesso**.
   - Sandbox Analyzer utilizza gli stessi bersagli ed eccezioni, definiti in **Antimalware > Scansione all'accesso**. Rivedi attentamente le impostazioni della Scansione all'accesso quando configuri Sandbox Analyzer.
   - Per prevenire i falsi positivi (rilevamento errato di applicazioni legittime), puoi impostare le eccezioni per nome del file, estensione, dimensione del file e percorso del file. Per maggiori informazioni sulla Scansione all'accesso, fai riferimento a «Antimalware» (p. 151).
   - Il limite di invio per ogni file o archivio è 50 MB.

3. Seleziona la **Modalità Analisi**. Sono disponibili due opzioni:
   - **Monitoraggio**. L'utente può accedere al file durante l'analisi nel sandbox, ma si consiglia di non eseguirlo fin quando non saranno disponibili i risultati delle analisi.
   - **Blocco**. L'utente non può eseguire il file fin quando il risultato delle analisi non viene inviato all'endpoint dal Cluster di Sandbox Analyzer tramite il portale di Sandbox Analyzer.
4. Specifica le **Azioni di risanamento**. Queste vengono intraprese quando Sandbox Analyzer rileva una minaccia. Per ciascuna modalità di analisi, viene fornita una doppia configurazione, consistente di un'azione predefinita e una di riserva. Sandbox Analyzer esegue inizialmente l'azione predefinita e poi quella di riserva, se la precedente non può essere completata.

   Accedendo a questa sezione per la prima volta, sono disponibili le seguenti configurazioni:

   Nota
   Come migliore prassi, si consiglia di utilizzare le azioni di risanamento in questa configurazione.

- Nella modalità **Monitoraggio**, l'azione predefinita è **Solo segnalazione**, con l'azione di riserva disattivata.
- In modalità **Blocco**, l'azione predefinita è **Quarantena**, mentre l'azione di riserva è **Elimina**.

Sandbox Analyzer ti fornisce le seguenti azioni di riparazione:

- **Disinfetta**. Rimuove il codice malware dai file infetti.
- **Elimina**. Rimuove dal disco l'intero file rilevato.
- **Quarantena**. Sposta i file rilevati dalla loro posizione originale alla cartella di quarantena. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Puoi gestire i file in quarantena nella pagina **Quarantena** della Control Center.
- **Solo segnalazione**. Sandbox Analyzer segnala solo le minacce rilevate senza intraprendere alcuna azione.

Nota
In base all'azione predefinita, potrebbe non essere disponibile un'azione di riserva.

5. Entrambe le sezioni di riparazione predefinite e fallback sono impostate nella modalità **Segnala solo**.
6. In **Pre-filtro contenuti**. personalizza il livello di protezione contro le potenziali minacce. Il sensore dell'endpoint ha un meccanismo integrato di filtro dei contenuti che determina se un file sospetto deve essere detonato in Sandbox Analyzer.

   I tipi di oggetto supportati sono: applicazioni, documenti, script, archivi, e-mail. Per maggiori dettagli sui tipi di oggetto supportati, fai riferimento a «Tipi di file supportati da Pre-filtro contenuti per l'invio automatico» (p. 462).

   Usa l'interruttore principale nella parte superiore dell'elenco delle minacce per selezionare un livello unico di protezione per tutti i tipi di oggetto, oppure seleziona livelli individuali per una protezione personalizzata.

   La configurazione del modulo su un determinato livello comporta l'invio di un certo numero di campioni:

   - **Permissivo**. Il sensore dell'endpoint invia automaticamente a Sandbox Analyzer solo gli elementi con la più alta probabilità di essere dannosi, ignorando gli altri.

- **Normale**. Il sensore dell'endpoint trova un equilibrio tra gli oggetti inviati e ignorati e invia a Sandbox Analyzer gli oggetti con la probabilità più alta e più bassa di essere dannosi.
- **Aggressivo**. Il sensore dell'endpoint invia a Sandbox Analyzer quasi tutti gli elementi, indipendentemente dalla loro pericolosità potenziale.

In un campo dedicato, puoi stabilire le eccezioni per i tipi di oggetto che non vuoi inviare a Sandbox Analyzer.

Puoi anche stabilire limiti di dimensione degli oggetti inviati, selezionando la casella corrispondente e inserendo un qualsiasi valore compreso tra 1 KB e 50 MB.

Sandbox Analyzer supporta l'invio locale del file tramite endpoint con ruolo di relay, che sono in grado di connettersi agli indirizzi del Portale di Sandbox Analyzer in base alla tua regione. Per maggiori dettagli relativi alle impostazioni della configurazione del relay, fai riferimento a «Relay» (p. 231).

Nota
Un proxy configurato nelle impostazioni di connessione di Sandbox Analyzer sostituirà qualsiasi endpoint con ruolo di relay.

7.2.4. Firewall

Nota
Questo modulo è disponibile per le workstation Windows.

Il Firewall protegge l'endpoint da tentativi di connessione interne o esterne non autorizzate.

La funzionalità del Firewall si basa sui profili di rete. I profili si basano sui livelli di fiducia, che devono essere definiti per ogni rete.

Il Firewall rileva ogni nuova connessione, confronta le informazioni dell'adattatore per quella connessione con le informazioni dei profili esistenti e applica il profilo corretto. Per maggiori informazioni su come vengono applicati i profili, fai riferimento a «Impostazioni della rete» (p. 197).

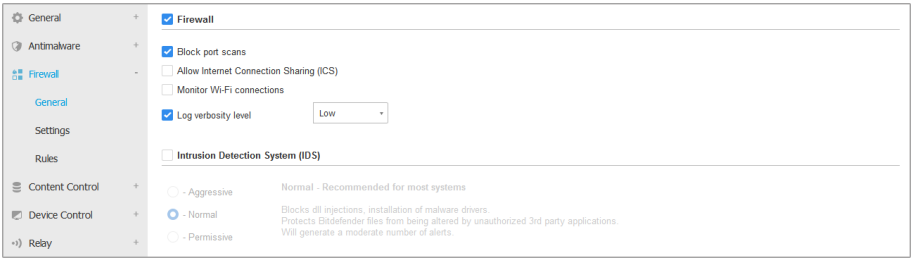
Importante
Il modulo Firewall è disponibile solo per le workstation Windows supportate.

Le impostazioni sono organizzate nelle seguenti sezioni:

- Generale
- Impostazioni
- Regole

Generale

In questa sezione, puoi attivare o disattivare il Firewall di Bitdefender e configura le impostazioni generali.



Policy - Impostazioni generali del Firewall

- **Firewall.** Usa la casella per attivare o disattivare il Firewall.

  Avvertimento
  Disattivando la protezione del Firewall, i computer saranno vulnerabili a eventuali attacchi alla rete o Internet.

- **Blocca port scan.** I port scan sono spesso usati dagli hacker per scoprire quali porte sono aperte su un computer. Potrebbero quindi violare il computer, se trovassero una porta meno sicura o vulnerabile.
- **Consenti Internet Connection Sharing (ICS).** Seleziona questa opzione per impostare il Firewall per consentire il traffico della condivisione della connessione a Internet.

  Nota
  Questa opzione non attiva automaticamente le ICS sul sistema dell'utente.

- **Monitora connessioni Wi-Fi.** L'agente di sicurezza di Bitdefender può informare gli utenti connessi alla rete Wi-Fi quando un nuovo computer entra nella rete. Per mostrare tali notifiche sullo schermo dell'utente, seleziona questa opzione.

- **Livello verbosità del registro.** L'agente di sicurezza di Bitdefender conserva un registro di eventi riguardanti l'utilizzo del modulo Firewall (attivare/disattivare il firewall, bloccare il traffico, modificare le impostazioni) o generati dalle attività rilevate da questo modulo (scansione delle porte, blocco di tentativi di connessione o del traffico secondo le regole). Seleziona un'opzione dal **Livello verbosità del registro** per indicare quante informazioni il registro dovrebbe includere.
- **Sistema di rilevazione intrusioni.** L'Intrusion Detection System monitora il sistema in cerca di attività sospette (per esempio, tentativi non autorizzati per alterare i file di Bitdefender, inserimenti di DLL, tentativi di keylogging, ecc.).

  Nota
  Le impostazioni della policy Intrusion Detection System (IDS) si applica solo a Endpoint Security (agente di sicurezza datato). L'agente di Bitdefender Endpoint Security Tools integra le capacità dell'Host-Based Intrusion Detection System nel suo modulo Advanced Threat Control (ATC).

  Per configurare l'Intrusion Detection System:

  1. Usa la casella per attivare o disattivare l'Intrusion Detection System.
  2. Clicca sul livello di sicurezza che si adatta meglio alle tue esigenze (Aggressivo, Normale o Permissivo). Usa la descrizione sul lato destro dell'indicatore per scegliere.

  Per prevenire a un'applicazione legittima di essere rilevato dall'Intrusion Detection System, aggiungi una **regola di esclusione dei processi ATC/IDS** per quell'applicazione nella sezione **Antimalware > Impostazioni > Eccezioni personalizzate**.

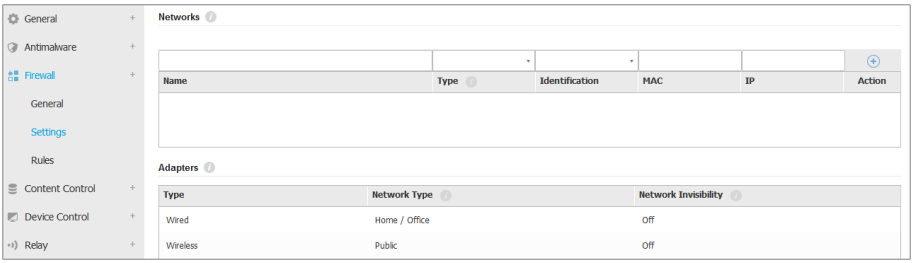
Importante
L'Intrusion Detection System è disponibile solo per i client di Endpoint Security.

Impostazioni

Il firewall applica automaticamente un profilo basato sul livello di fiducia. Puoi avere diversi livelli di fiducia per le connessioni di rete, in base all'architettura della rete o al tipo di adattatore utilizzato per stabilire la connessione di rete. Per esempio, se all'interno della rete aziendale hai delle sottoreti, puoi impostare un livello di fiducia per ciascuna sottorete.

Le impostazioni sono organizzate nelle seguenti tabelle:

- Reti
- Adattatori



Policy - Impostazioni del firewall

Impostazioni della rete

Se vuoi che il Firewall applichi diversi profili ai vari segmenti di rete nella società, devi specificare le reti gestite nella tabella **Reti**. Compila i campi nella tabella **Reti**, come descritto di seguito:

- **Nome.** Inserisci il nome tramite cui puoi riconoscere la rete nell'elenco.
- **Tipo.** Seleziona nel menu il tipo di profilo assegnato alla rete.

  L'agente di sicurezza di Bitdefender applica automaticamente uno dei quattro profili di rete per ciascuna connessione di rete rilevata sull'endpoint, per definire le opzioni basilari di filtraggio del traffico. I tipi di profilo sono:

  - Rete **affidabile**. Disattiva il firewall per i relativi adattatori.
  - Rete **Casa/Ufficio**. Consente l'intero traffico verso e dai computer nella rete locale mentre l'altro traffico viene filtrato.
  - Rete **pubblica**. Tutto il traffico viene filtrato.
  - Rete **non affidabile**. Blocca completamente la rete e il traffico Internet attraverso i relativi adattatori.
- **Identificazione.** Seleziona dal menu il metodo tramite cui la rete sarà identificata dall'agente di sicurezza di Bitdefender. Le reti possono essere identificate con tre metodi: **DNS**, **Gateway** e **Rete**.
  - **DNS**: identifica tutti gli endpoint che utilizzando un determinato DNS.
  - **Gateway**: identifica tutti gli endpoint che comunicano tramite il gateway indicato.

- **Rete**: identifica tutti gli endpoint del segmento di rete indicato, definito dal suo indirizzo di rete.

- **MAC**. Usa questo campo per specificare l'indirizzo MAC di un server DNS o di un gateway che delimita la rete, in base al metodo di identificazione selezionato.

  Devi inserire l'indirizzo MAA in formato esadecimale, separato da trattini (-) o due punti (:). Per esempio, sia `00-50-56-84-32-2b` e `00:50:56:84:32:2b` sono indirizzi validi.

- **IP.** Utilizza questo campo per definire gli indirizzi IP specifici in una rete. Il formato dell'IP dipende dal metodo di identificazione, come qui indicato:
  - **Rete.** Inserisci il numero di rete nel formato CIDR. Per esempio, `192.168.1.0/24`, dove `192.168.1.0` è l'indirizzo di rete e `/24` è la maschera di rete.
  - **Gateway.** Inserisci l'indirizzo IP del gateway.
  - **DNS.** Inserisci l'indirizzo IP del server DNS.

Dopo aver definito una rete, clicca sul pulsante **Aggiungi** nel lato destro della tabella e aggiungila all'elenco.

Impostazioni adattatori

Se viene rilevata una rete che non è definita nella tabella **Reti**, l'agente di sicurezza di Bitdefender rileva il tipo di adattatore di rete e applica un profilo corrispondente alla connessione.

I campi della tabella **Adattatori** sono decritti nel seguente modo:

- **Tipo.** Mostra il tipo di adattatori di rete. L'agente di sicurezza di Bitdefender può rilevare tre tipi di adattatori predefiniti: **Cablato**, **Wireless** e **Virtuale** (Virtual Private Network).

- **Tipo di rete.** Descrive il profilo di rete assegnato a un determinato tipo di adattatore. I profili di rete sono descritti nella sezione impostazioni di rete. Cliccando sul campo tipo di rete puoi modificare tale impostazione.

  Se selezioni **Consenti a Windows di decidere**, per una qualsiasi nuova connessione di rete rilevata dopo l'applicazione della policy, l'agente di sicurezza di Bitdefender applica un profilo per il firewall basato sulla classificazione di rete in Windows, ignorando le impostazioni della tabella **Adattatori**.

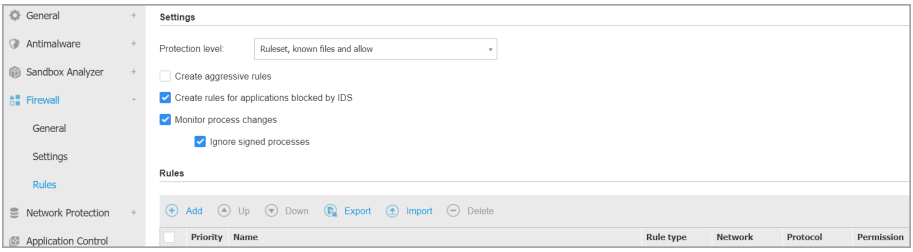
Se la rilevazione basata su Windows Network Manager fallisce, viene tentata una rilevazione di base. Viene utilizzato un profilo generico, in cui il profilo di rete viene considerato **Pubblico** e le impostazioni furtive vengono impostate su **Attiva**.

Quando l'endpoint in Active Directory si connette al dominio, il profilo del firewall viene impostato automaticamente in **Casa/Ufficio** e le impostazioni furtive vengono impostate in **Remoto**. Se il computer non è in un dominio, tale condizione non è applicabile.

- **Network Discovery.** Nasconde il computer da software dannoso e hacker nella rete o su Internet. Configura la visibilità del computer nella rete in base alla necessità, per ciascun tipo di adattatore, selezionando una delle seguenti opzioni:
  - **Sì.** Chiunque nella rete locale o in Internet può pingare e rilevare il computer.
  - **No.** Il computer è invisibile sia nella rete locale che su Internet.
  - **Remoto.** Il computer non può essere rilevato da Internet. Chiunque nella rete locale può pingare e rilevare il computer.

Regole

In questa sezione, puoi configurare l'accesso alla rete dell'applicazione e le regole di traffico dei dati applicate dal firewall. Nota che le impostazioni disponibili si applicano solo ai profili **Casa/Ufficio** e **Pubblico**.



Policy - Impostazioni regole del firewall

Impostazioni

Puoi configurare le seguenti impostazioni:

- **Livello di protezione.** Il livello di protezione selezionato definisce la logica decisionale del firewall quando le applicazioni richiedono l'accesso alla rete e ai servizi Internet. Sono disponibili le seguenti opzioni:

  Set di regole e consentire
  Applica le regole del firewall esistenti e consenti automaticamente tutti gli altri tentativi di connessione. Per ogni nuovo tentativo di connessione, viene creata una regola, che viene poi aggiunta al set delle regole.

  Set di regole e chiedere
  Applica le regole del firewall esistenti e chiedi all'utente quale azione intraprendere per tutti gli altri tentativi di connessione. Sullo schermo dell'utente viene visualizzata una finestra di avviso con informazioni dettagliate sul tentativo di connessione sconosciuto. Per ogni nuovo tentativo di connessione, viene creata una regola, che viene poi aggiunta al set delle regole.

  Set di regole e negare
  Applica le regole del firewall esistenti e nega automaticamente tutti gli altri tentativi di connessione. Per ogni nuovo tentativo di connessione, viene creata una regola, che viene poi aggiunta al set delle regole.

  Set di regole, file noti e consentire
  Applica le regole del firewall esistenti, consenti automaticamente tutti gli altri tentativi di connessione da parte di applicazioni note e consenti anche automaticamente tutti gli altri tentativi di connessione sconosciuti. Per ogni nuovo tentativo di connessione, viene creata una regola, che viene poi aggiunta al set delle regole.

  Set di regole, file noti e chiedere
  Applica le regole del firewall esistenti, consenti automaticamente tutti gli altri tentativi di connessione da parte di applicazioni note e chiedi all'utente quali azioni intraprendere per tutti gli altri tentativi di connessione sconosciuti. Sullo schermo dell'utente viene visualizzata una finestra di avviso con informazioni dettagliate sul tentativo di connessione sconosciuto. Per ogni nuovo tentativo di connessione, viene creata una regola, che viene poi aggiunta al set delle regole.

  Set di regole, file noti e negare
  Applica le regole del firewall esistenti, consenti automaticamente tutti gli altri tentativi di connessione da parte di applicazioni note e nega automaticamente tutti gli altri tentativi di connessione sconosciuti. Per

ogni nuovo tentativo di connessione, viene creata una regola, che viene poi aggiunta al set delle regole.

Nota
I file noti rappresentano una grande raccolta di applicazioni sicure e affidabili, che viene creata e costantemente gestita da Bitdefender.

- **Crea regole aggressive.** Con questa opzione selezionata, il firewall creerà regole per ogni processo che apra l'applicazione che richieda l'accesso alla rete o a Internet.
- **Crea regole per applicazioni bloccate da IDS.** Con questa opzione selezionata, il firewall creerà automaticamente una regola **Nega** ogni volta che l'Intrusion Detection System blocca un'applicazione.
- **Monitora modifiche processo.** Seleziona questa opzione se desideri verificare ogni applicazione che tenta di connettersi a Internet, se è stata modificata dall'aggiunta della regola che controlla il suo accesso a Internet. Se l'applicazione è stata modificata, sarà creata una nuova regola in base al livello di protezione esistente.

  Nota
  Normalmente, le applicazioni vengono modificate dagli aggiornamenti. Ma c'è il rischio che possano essere modificate dalle applicazioni malware allo scopo di infettare il computer locale e gli altri computer nella rete.

  Le applicazioni segnalate si suppone che siano di fiducia e che abbiano un più alto grado di sicurezza. Puoi selezionare **Ignora processi firmati** per consentire automaticamente alle applicazioni modificate e firmate di connettersi a Internet.

Regole

La tabella Regola elenca le regole del firewall esistenti, fornendo alcune informazioni importanti su ciascuna di esse:

- Nome della regola o applicazione a cui fa riferimento.
- Il protocollo a cui si applica la regola.
- Azione della regola (consenti o nega pacchetti).
- Azioni che puoi intraprendere sulla regola.
- Priorità della regola.

Nota

Queste sono le regole del firewall applicate esplicitamente dalla policy. Le regole aggiuntive possono essere configurate su computer come risultato dell'applicazione delle impostazioni del firewall.

Un numero di regole del firewall predefinite che ti aiutano a gestire o negare facilmente i tipi di traffico più popolari. Seleziona l'opzione desiderata dal menu **Permessi**.

ICMP / ICMPv6 in ingresso
Consenti o blocca i messaggi ICMP / ICMPv6. I messaggi ICMP sono spesso usati dagli hacker per eseguire attacchi contro le reti informatiche. Di norma, questo tipo di traffico è consentito.

Connessioni desktop remote in ingresso
Consenti o blocca l'accesso ad altri computer alle connessioni desktop remote. Di norma, questo tipo di traffico è consentito.

Inviare e-mail
Consenti o nega l'invio di e-mail via SMTP. Di norma, questo tipo di traffico è consentito.

Navigazione web HTTP
Consenti o blocca la navigazione web HTTP. Di norma, questo tipo di traffico è consentito.

Stampa di rete
Consenti o nega l'accesso alle stampanti in un'altra area di rete locale. Di norma, questo tipo di traffico è negato.

Traffico Windows Explorer su HTTP / FTP
Consenti o blocca il traffico HTTP e FTP da Windows Explorer. Di norma, questo tipo di traffico è negato.

Oltre alle regole standard, puoi creare regole del firewall aggiuntive per altre applicazioni installate sugli endpoint. Tuttavia questa configurazione è riservata agli amministratori con notevoli abilità di rete.

Per creare e configurare una nuova regola, clicca sul pulsante ⊕ **Aggiungi** nel lato superiore della tabella. Fai riferimento al seguente articolo per maggiori informazioni.

Per rimuovere una regola dall'elenco, selezionala e clicca sul pulsante ⊖ **Elimina** nel lato superiore della tabella.

Nota
Non è possibile né eliminare né modificare le regole del firewall predefinite.

Configurare le regole personali

Puoi configurare due tipi di regole del firewall:

- **Regole basate sulle applicazioni.** Tali regole si applicazioni a determinati software trovati sui computer client.
- **Regole basate sulla connessione.** Tali regole si applicano a qualsiasi applicazione o servizio che utilizza una determinata connessione.

Per creare e configurare una nuova regola, clicca sul pulsante ⊕ **Aggiungi** nel lato superiore della tabella e seleziona il tipo di regola desiderato nel menu. Per modificare una regola esistente, clicca sul nome della regola.

Possono essere configurate le seguenti impostazioni:

- **Nome regola.** Inserisci il nome sotto alla regola che sarà indicata nella tabella delle regole (per esempio, il nome dell'applicazione a cui si applica la regola).
- **Percorso dell'applicazione** (solo per le regole basate sulle applicazioni). Devi indicare il percorso del file eseguibile dell'applicazione sui computer di destinazione.
  - Seleziona nel menu una posizione predefinita e completa il percorso come necessario. Per esempio, per un'applicazione installata nella cartella `Program Files`, seleziona `%ProgramFiles%` e completa il percorso aggiungendo una barra inversa (\) e il nome della cartella dell'applicazione.
  - Inserisci il percorso completo nel campo di modifica. È consigliabile utilizzare variabili di sistema (laddove appropriato) per assicurarsi che il percorso sia valido su tutti i computer di destinazione.
- **Linea di comando** (solo per regole basate sulle applicazioni). Se desideri che la regola venga applicata solo quando l'applicazione indicata sia aperta con un comando specifico nell'interfaccia linea di comando di Windows, digita il comando corrispondente nel campo di modifica. Altrimenti, lascia il campo in bianco.
- **MD5 applicazione** (solo per regole basate sulle applicazioni). Se desideri che la regola per controllare l'integrità dei dati del file dell'applicazione sia basata sul suo codice hash MD5, inseriscilo nel campo di modifica. Altrimenti, lascia il campo in bianco.

- **Indirizzo locale.** Specifica l'indirizzo IP locale e la porta sui quali sarà applicata la regola. Se hai più di un adattatore di rete, puoi deselezionare la casella **Qualsiasi** e digitare un indirizzo IP specifico. Altrimenti, per filtrare le connessioni su una determinata porta o range di porte, deseleziona la casella **Qualsiasi** e inserisci la porta desiderata o il range di porte nel campo corrispondente.
- **Indirizzo remoto.** Specifica l'indirizzo IP remoto e la porta sui quali sarà applicata la regola. Per filtrare il traffico per e da un determinato computer, deseleziona la casella **Qualsiasi** e digita il suo indirizzo IP.
- **Applica la regola solo per computer connessi direttamente.** Puoi filtrare l'accesso basato sull'indirizzo Mac.
- **Protocollo.** Seleziona il protocollo IP a cui sarà applicata la regola.
  - Se desideri che la regola venga applicata a tutti i protocolli, seleziona **Qualsiasi**.
  - Se desideri che la regola venga applicata a TCP, seleziona **TCP**.
  - Se desideri che la regola venga applicata a UDP, seleziona **UDP**.
  - Se desideri che la regola venga applicata a un protocollo specifico, selezionalo nel menu **Altro**.

    Nota

    I numeri dei protocolli IP vengono assegnati dalla Internet Assigned Numbers Authority (IANA). Puoi trovare l'elenco completo dei numeri di protocolli IP assegnati su http://www.iana.org/assignments/protocol-numbers.

- **Direzione.** Seleziona la direzione del traffico a cui applicare la regola.

Direzione	Descrizione
In uscita	La regola sarà applicata solo per il traffico in uscita.
In entrata	La regola sarà applicata solo per il traffico in entrata.
Entrambi	La regola sarà applicata in entrambe le direzioni.

- **Versione IP.** Seleziona la versione dell'IP (IPv4, IPv6 o altro) a cui applicare la regola.
- **Rete.** Seleziona il tipo di rete a cui si applica la regola.

- **Autorizzazione.** Seleziona uno dei permessi disponibili:

Autorizzazione	Descrizione
Consenti	L'accesso alla rete / Internet dell'applicazione sarà autorizzato quando si verifichino le circostanze specificate.
Nega	L'accesso alla rete / Internet dell'applicazione sarà negato nelle circostanze specificate.

Clicca su **Salva** per aggiungere la regola.

Per le regole che hai creato, usa le frecce nel lato destro della tabella per impostare la priorità di ciascuna regola. La regola con la priorità maggiore è quella in posizione più elevata nell'elenco.

Importare ed esportare le regole

Puoi esportare e importare le regole del firewall per usarle in altre policy o aziende. Per esportare le regole:

1. Clicca su **Esporta** nel lato superiore della tabella delle regole.
2. Salva il file CSV sul computer. In base alle impostazioni del tuo browser, il fil potrebbe essere scaricato automaticamente oppure ti sarà chiesto di salvarlo in una determinata posizione.

Importante

- Ogni riga nel file CSV corrisponde a una sola regola e ha più campi.
- La posizione delle regole del firewall nel file CSV determina la loro priorità. Puoi modificare la priorità di una regola spostando l'intera riga.

Per il set predefinito di regole, puoi modificare solo i seguenti elementi:

- **Priorità**: imposta la priorità della regola in qualsiasi ordine desideri spostando la riga CSV.
- **Permesso**: modifica il campo `set.Permission` usando i permessi disponibili:
  - 1 per **Consenti**
  - 2 per **Nega**

Qualsiasi altra regolazione viene scartata all'importazione.

Per le regole personalizzate del firewall, tutti i valori del campo sono configurabili nel seguente modo:

Campo	Nome e valore
`ruleType`	**Tipo di regola**: 1 per **Applicazione regola** 2 per **Regola di connessione**
`tipo`	Il valore di questo campo è opzionale.
`details.name`	**Nome regola**
`details.applictionPath`	**Percorso dell'applicazione** (solo per le regole basate sulle applicazioni)
`details.commandLine`	**Linea di comando** (solo per regole basate sulle applicazioni)
`details.applicationMd5`	**MD5 applicazione** (solo per regole basate sulle applicazioni)
`settings.protocol`	**Protocollo** 1 per **Qualsiasi** 2 per **TCP** 3 per **UDP** 4 per **Altro**
`settings.customProtocol`	Richiesto solo se il **Protocollo** viene impostato su **Altro**. Per valori specifici, considera questa pagina. I valori 0, 4, 6, 41, 61, 63, 68, 99, 114, 124, 34-37, 141-143 non sono supportati.
`settings.direction`	**Direzione**: 1 per **Entrambi** 2 per **In entrata** 3 per **In uscita**

Campo	Nome e valore
`settings.ipVersion`	**Versione IP**: 1 per **Qualsiasi** 2 per **IPv4** 3 per **IPv6**
`settings.localAddress.any`	L'**indirizzo locale** è impostato su **Qualsiasi**: 1 per True 0 o vuoto per False
`settings.localAddress.ipMask`	L'**Indirizzo locale** è impostato su **IP o IP/Mask**
`settings.remoteAddress.portRange`	L'**Indirizzo remoto** è impostato su **porta o range della porta**
`settings.directlyConnected.enable`	**Applica la regola solo per computer connessi direttamente**: 1 per attivato 0 per vuoto o disattivato
`settings.directlyConnected.remoteMac`	**Applica la regola solo per computer direttamente connessi** con il filtro **MAC address**.
`permission.home`	La **rete** a cui applicare la regola è **Casa/Ufficio**: 1 per True 0 per vuoto o False
`permission.public`	La **Rete** a cui si applica la regola è **Pubblica**: 1 per True 0 per vuoto o False
`permission.setPermission`	Permessi disponibili:

Campo	Nome e valore
	1 per **Consenti** 2 per **Nega**

Per importare le regole:

1. Clicca su **Importa** nel lato superiore della tabella delle regole.
2. Nella nuova finestra, clicca su **Aggiungi** e seleziona il file CSV.
3. Clicca su **Salva**. La tabella viene riempita con le regole valide.

7.2.5. Protezione rete

Usa la sezione Protezione di rete per configurare le tue preferenze relative al filtraggio dei contenuti, la protezione dei dati per le attività dell'utente, tra cui navigazione web, e-mail e applicazioni software, e il rilevamento di tecniche di attacco alla rete che cercano di ottenere accesso a determinati endpoint. Puoi limitare o consentire l'accesso al web e l'utilizzo delle applicazioni, configurare la scansione del traffico, l'antiphishing e le regole di protezione dei dati.

Ricordati che le impostazioni della Protezione rete si applicheranno a tutti gli utenti che accedono ai computer bersaglio.

Le impostazioni sono organizzate nelle seguenti sezioni:

- Generale
- Controllo contenuti
- Protezione web
- Attacchi alla rete

Nota

- Il modulo Controllo contenuti è disponibile per:
  - Windows for workstations
  - macOS
- Il modulo Network Attack Defense è disponibile per:
  - Windows for workstations

Importante

Per macOS, Controllo contenuti si basa su un'estensione del kernel. Su macOS High Sierra (10.13) e versioni successive, l'installazione di un'estensione del kernel richiede

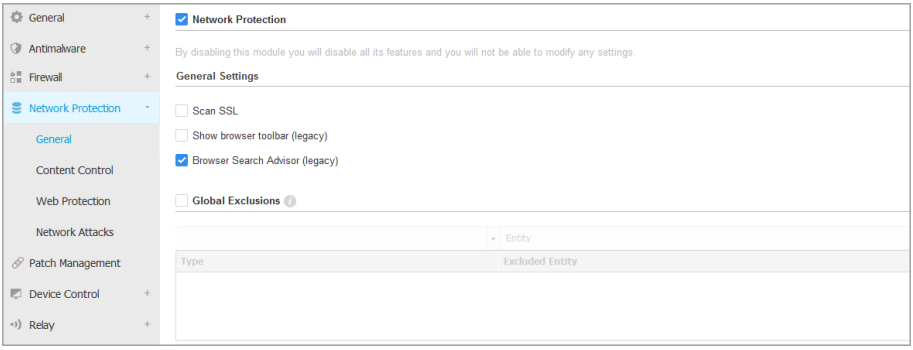
la tua approvazione. Il sistema comunica all'utente che è stata bloccata un'estensione di sistema da Bitdefender. L'utente può autorizzarla dalle preferenze in **Protezione & Privacy**. Fin quando l'utente non approva l'estensione di sistema di Bitdefender, questo modulo non funzionerà e l'interfaccia utente di Endpoint Security for Mac mostrerà un problema critico, chiedendo l'approvazione.
Per eliminare l'intervento dell'utente, puoi pre-approvare l'estensione del kernel di Bitdefender inserendola nella whitelist usando uno strumento di Mobile Device Management. Per maggiori dettagli sulle estensioni del kernel Bitdefender, fai riferimento a questo articolo della KB.

Generale

In questa pagina, puoi configurare opzioni come l'attivazione o la disattivazione delle funzionalità, oltre a configurare le eccezioni.

Le impostazioni sono organizzate nelle seguenti sezioni:

- Impostazioni generali
- Eccezioni globali



Policy - Protezione rete - Generali

Impostazioni generali

- **Controlla SSL**. Seleziona questa opzione se vuoi che il traffico web Secure Sockets Layer (SSL) sia ispezionato dai moduli di protezione dell'agente di sicurezza di Bitdefender.
- **Mostra barra degli strumenti del browser (datata)**. La barra degli strumenti di Bitdefender informa gli utenti sulla valutazione delle pagine web che stai visualizzando. La barra degli strumenti di Bitdefender non è la tipica barra degli

strumenti del browser. L'unica cosa che aggiunge al browser è una piccola linguetta  nella parte superiore di ogni pagina web. Cliccando sulla linguetta, apri la barra degli strumenti.

In base a come Bitdefender classifica la pagina web, una delle seguenti valutazioni sarà mostrata nel lato sinistro della barra degli strumenti:

- Il messaggio "Questa pagina non è sicura" compare su uno sfondo rosso.
- Il messaggio "Si consiglia cautela" su uno sfondo arancione.
- Il messaggio "Questa pagina è sicura" compare su uno sfondo verde.

Nota

- Questa opzione non è disponibile per macOS.
- Questa opzione è stata rimossa dall'avvio di Windows con le installazioni di Bitdefender Endpoint Security Tools in versione 6.6.5.82.

- **Ricerca sicura browser (datata).** Ricerca sicura classifica i risultati delle ricerche tramite Google, Bing e Yahoo! oltre ai link di Facebook e Twitter, posizionando un'icona accanto a ogni risultato. Le icone utilizzate e il loro significato:

  Non dovresti visitare questa pagina web.
  Questa pagina web può contenere contenuti pericolosi. Se decidi di visitarlo, usa la massima cautela.
  Questa è una pagina sicura da visitare.

Nota

- Questa opzione non è disponibile per macOS.
- Questa opzione è stata rimossa dall'avvio di Windows con le installazioni di Bitdefender Endpoint Security Tools in versione 6.6.5.82.

Eccezioni globali

Puoi scegliere di saltare la scansione antimalware di parte del traffico mentre le opzioni di **Protezione rete** sono attivate.

Nota

Queste eccezioni si applicano a **Scansione traffico** e **Antiphishing** nella sezione **Protezione web** e **Network Attack Defense** nella sezione **Attacchi di rete**. Le eccezioni di **Protezione dati** sono configurabili separatamente nella sezione **Controllo contenuti**.

Per definire un'eccezione:

1. Seleziona il tipo di eccezione nel menu.
2. In base al tipo di eccezione, definisci la quantità del traffico da escludere dalla scansione, come segue:
   - **IP/mask**. Inserisci l'indirizzo IP o l'IP della maschera per cui non vuoi esaminare il traffico in entrata e uscita, che include le tecniche di attacco alla rete.
   - **URL**. Escludi dalla scansione gli indirizzi web indicati. Considera che le eccezioni della scansione basate su URL si applicano in modo diverso per le connessioni HTTP e HTTPS, come spiegato di seguito.

     Puoi definire un'eccezione della scansione basata su URL come segue:

     – Inserisci un determinato URL, come `www.example.com/example.html`
       - Nel caso di connessioni HTTP, solo l'URL specifico viene escluso dalla scansione.
       - Per le connessioni HTTPS, l'aggiunta di uno specifico URL esclude l'intero dominio e i relativi sottodomini. Inoltre, in questo caso, puoi specificare direttamente il dominio da escludere dalla scansione.

     – Usa i caratteri jolly per definire gli schemi degli indirizzi web (solo per le connessioni HTTP).

       Importante
       Le eccezioni con caratteri jolly non funzionano per le connessioni HTTPS.

       Puoi usare i seguenti caratteri jolly:
       - L'asterisco (*) sostituisce lo zero o più caratteri.
       - Il punto di domanda (`?`) sostituisce esattamente un carattere. Puoi utilizzare diversi punti di domanda per definire qualsiasi combinazione di un dato numero di caratteri. Per esempio, `???` sostituisce una qualsiasi combinazione formata esattamente da tre caratteri.

       Nella seguente tabella, puoi trovare diversi errori di sintassi per indicare gli indirizzi web specifici (URL).

Sintassi	Applicabilità delle eccezioni
`www.example*`	Ogni URL che inizia con `www.example` (indipendentemente dall'estensione del dominio). L'eccezione non si applicherà ai sottodomini del sito web indicato, come `subdomain.example.com`.
`*example.com`	Ogni URL che termina con `example.com`, tra cui relativi sottodomini.
`*example.com*`	Ogni URL che contiene la stringa indicata.
`*.com`	Ogni sito web con l'estensione del dominio `.com`, incluso i relativi sottodomini. Usa la sintassi per escludere dalla scansione interi domini di livello superiore.
`www.example?.com`	Ogni indirizzo web che inizia con `www.example?.com`, dove `?` può essere sostituito con un singolo carattere. Tali siti web potrebbero includere: `www.example1.com` o `www.exampleA.com`.

Nota
Puoi utilizzare URL relativi al protocollo.

- **Applicazione**. Esclude dalla scansione il processo o l'applicazione selezionata. Per definire un'eccezione di scansione delle applicazioni:
  - Inserisci il percorso completo dell'applicazione. Per esempio, `C:\Program Files\Internet Explorer\iexplore.exe`
  - Usa le variabili ambientali per specificare il percorso dell'applicazione. Per esempio: `%programfiles%\Internet Explorer\iexplore.exe`
  - Usa i caratteri jolly per indicare qualsiasi applicazione che corrisponda a un determinato modello di nome. Per esempio:
    - `c*.exe` corrisponde a tutte le applicazioni che iniziano con "c" (chrome.exe).

- `??????.exe` corrisponde a tutte le applicazioni con un nome che contiene sei caratteri (chrome.exe, safari.exe, etc.).
- `[^c]*.exe` corrisponde a tutte le applicazioni tranne quelle che iniziano con "c".
- `[^ci]*.exe` corrisponde a tutte le applicazioni tranne quelle che iniziano con "c" o "i".

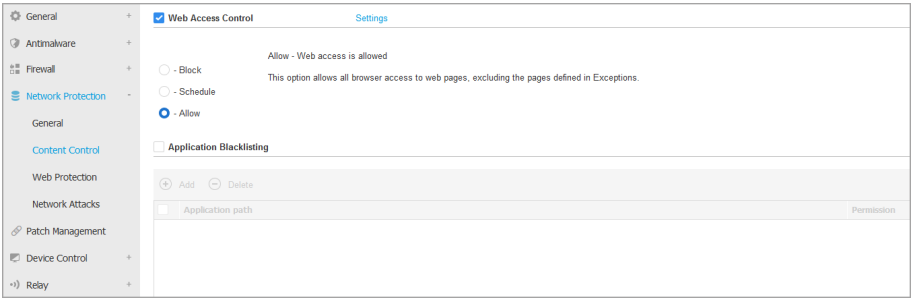
3. Clicca sul pulsante ⊕**Aggiungi** nel lato destro della tabella.

Per rimuovere un'entità dall'elenco, clicca sul corrispondente pulsante ⊗ **Elimina**.

Controllo contenuti

Le impostazioni del Controllo contenuti sono organizzate nelle seguenti sezioni:

- Controllo siti web
- Blacklist applicazioni
- Protezione dati



Controllo siti web

Il Controllo siti web ti aiuta a consentire o bloccare l'accesso al web per utenti o applicazioni durante determinati intervalli di tempo.

Le pagine web bloccate dal Controllo siti web non vengono mostrate nel browser. Al loro posto, viene mostrata una pagina web predefinita che informa l'utente che la pagina web richiesta è stata bloccata dal Controllo siti web.

Usa l'interruttore per attivare o disattivare il **Controllo siti web**.

Hai tre opzioni di configurazione:

- Seleziona **Consenti** per garantire sempre l'accesso al web.

- Seleziona **Blocca** per bloccare sempre l'accesso al web.
- Seleziona **Programma** per attivare eventuali limitazioni di tempo per l'accesso al web in base a un determinato programma.

Che tu scelga di consentire o bloccare l'accesso al web, puoi definire delle eccezioni a tali azioni per le tutte le categorie del web o solo per gli indirizzi web specificati. Clicca su **Impostazioni** per configurare il tuo programma di accesso al web e le eccezioni, come segue:

Programmazione

Per limitare l'accesso a Internet in determinati orari della giornata, su base settimanale:

1. Seleziona dalla griglia gli intervalli di tempo durante i quali bloccare l'accesso a Internet.

   Puoi cliccare sulle singole caselle oppure puoi cliccare e trascinare per coprire periodi più lunghi. Clicca di nuovo nella casella per invertire la selezione.

   Per avviare una nuova selezione, clicca su **Consenti tutto** o **Blocca tutto**, in base al tipo di limitazione che desideri implementare.

2. Clicca su **Salva**.

Nota
L'agente di sicurezza di Bitdefender eseguirà gli aggiornamenti ogni ora, anche se l'accesso web fosse bloccato.

Categorie

Il filtro categorie web filtra dinamicamente l'accesso ai siti web in base ai loro contenuti. Puoi utilizzare il filtro categorie web per definire le eccezioni all'azione del Controllo siti web selezionata (Consenti o Blocca) per tutte le categorie web (come giochi, contenuti per adulti o reti online).

Per configurare il filtro categorie web:

1. Attiva il **filtro categorie web**.
2. Per una configurazione rapida, clicca su uno dei profili predefiniti (**Aggressivo**, **Normale** o **Permissivo**). Usa la descrizione sul lato destro dell'indicatore per scegliere. Puoi visualizzare le azioni predefinite per le categorie web disponibili espandendo la sezione **Regole web** posizionata in basso.

3. Se non sei soddisfatto delle impostazioni predefinite, puoi definire un filtro personalizzato:
   a. Seleziona **Personalizzato**.
   b. Clicca su **Regole web** per espandere la sezione corrispondente.
   c. Trova la categoria che desideri nell'elenco e seleziona l'azione desiderata dal menu. Per maggiori informazioni sulle categorie di siti web disponibili, fai riferimento a questo articolo della KB.
4. Seleziona l'opzione **Imposta categorie web come eccezioni per Accesso al web** se vuoi ignorare le impostazioni esistenti di accesso al web e applicare solo il filtro categorie web.
5. Il messaggio predefinito mostrato all'utente che accede a siti web limitati contiene anche la categoria a cui il contenuto del sito web corrisponde. Deseleziona l'opzione **Mostra avvisi dettagliati sul client** se vuoi che gli utenti non vedano queste informazioni.

   Nota
   Questa opzione non è disponibile per macOS.

6. Clicca su **Salva**.

Nota

- Il permesso **Consenti** per determinate categorie web è anche preso in considerazione durante gli intervalli di tempo quando l'accesso al web viene bloccato dal Controllo siti web.
- I permessi **Consenti** funzionano solo quando l'accesso al web è bloccato dal Controllo siti web, mentre i permessi **Blocca** funzionano solo quando l'accesso al web è consentito dal Controllo siti web.
- Puoi ignorare il permesso della categoria per singoli indirizzi web aggiungendoli al permesso opposto in **Controllo siti web > Impostazioni > Eccezioni**. Per esempio, se un indirizzo web è bloccato dal filtro categorie web, aggiungi una regola web per quell'indirizzo con il permesso impostato su **Consenti**.

Eccezioni

Puoi anche definire regole web per bloccare o consentire esplicitamente determinati indirizzi web, ignorando le impostazioni del Controllo siti web

esistenti. Gli utenti potranno, per esempio, accedere a una determinata pagina web anche quando la navigazione web è bloccata dal Controllo siti web.

Per creare una regola web:

1. Attiva l'opzione **Usa eccezioni**.
2. Inserisci l'indirizzo che vuoi consentire o bloccare nel campo **Indirizzo web**.
3. Seleziona **Consenti** o **Blocca** nel menu **Permesso**.
4. Clicca sul pulsante ⊕ **Aggiungi** nel lato destro della tabella per aggiungere l'indirizzo all'elenco delle eccezioni.
5. Clicca su **Salva**.

Per modificare una regola web:

1. Clicca sull'indirizzo web che vuoi modificare.
2. Modifica l'URL esistente.
3. Clicca su **Salva**.

Per rimuovere una regola web, cliccare sul pulsante ⊗ **Elimina** corrispondente.

Blacklist applicazioni

In questa sezione, puoi configurare l'inserimento nella blacklist delle applicazioni, che ti aiuterà a bloccare completamente o limitare l'accesso degli utenti alle applicazioni nei loro computer. Giochi, contenuti multimediali e messaggi software, oltre ad altre categorie di software e malware che in questo modo possono essere bloccati.

Per configurare la blacklist delle applicazioni:

1. Attiva l'opzione **Blacklist applicazioni**.
2. Specifica le applicazioni a cui vuoi limitare l'accesso. Per limitare l'accesso a un'applicazione:
   a. Clicca sul pulsante ⊕**Aggiungi** nel lato superiore della tabella. Apparirà una finestra di configurazione.
   b. Devi indicare il percorso del file eseguibile dell'applicazione sui computer di destinazione. Ci sono due modi per farlo:
      - Seleziona nel menu una posizione predefinita e completa il percorso come necessario nel campo di modifica. Per esempio, per un'applicazione installata nella cartella `Program Files`, seleziona `%ProgramFiles%`

e completa il percorso aggiungendo una barra inversa (\) e il nome della cartella dell'applicazione.
- Inserisci il percorso completo nel campo di modifica. È consigliabile utilizzare variabili di sistema (laddove appropriato) per assicurarsi che il percorso sia valido su tutti i computer di destinazione.

c. **Programmazione accesso**. Programma l'accesso all'applicazione durante determinati orari della giornata su base settimanale:
- Seleziona dalla griglia gli intervalli di tempo durante i quali vuoi bloccare l'accesso all'applicazione. Puoi cliccare sulle singole caselle oppure puoi cliccare e trascinare per coprire periodi più lunghi. Clicca di nuovo nella casella per invertire la selezione.
- Per avviare una nuova selezione, clicca su **Consenti tutto** o **Blocca tutto**, in base al tipo di limitazione che desideri implementare.
- Clicca su **Salva**. La nuova regola sarà aggiunta all'elenco.

Per rimuovere una regola dall'elenco, selezionala e clicca sul pulsante ⊗ **Elimina** nel lato superiore della tabella. Per modificare una regola esistente, cliccaci sopra per aprire la sua finestra di configurazione.

Protezione dati

La protezione dei dati impedisce la divulgazione non autorizzata di dati sensibili in base a regole definite dall'amministratore.

Nota
Questa funzionalità non è disponibile per macOS.

Puoi creare regole per proteggere qualsiasi tipo di informazione personale o confidenziale, come:

- Informazioni personali del cliente
- Nomi e dettagli importanti di prodotti e tecnologie in sviluppo
- Informazioni per contattare i dirigenti aziendali

Le informazioni protette potrebbero includere nomi, numeri di telefono, carte di credito e conti bancari, indirizzi e-mail e così via.

In base alle regole di protezione dei dati che hai creato, Bitdefender Endpoint Security Tools esamina il web e il traffico e-mail in uscita per cercare determinate stringhe di caratteri (ad esempio, un numero di carta di credito). In caso di corrispondenza, la rispettiva pagina web o messaggio e-mail viene bloccato per

impedire di inviare i dati protetti. L'utente viene informato immediatamente sull'azione intrapresa da Bitdefender Endpoint Security Tools tramite una pagina di avviso web o e-mail.

Per configurare la protezione dei dati:

1. Usa la casella per attivare la protezione dei dati.
2. Crea regole di protezione dei dati per tutte i dati sensibili che vuoi proteggere. Per creare una regola:
   a. Clicca sul pulsante **Aggiungi** nel lato superiore della tabella. Apparirà una finestra di configurazione.
   b. Inserisci il nome sotto il quale la regola sarà elencata nella tabella delle regole. Seleziona un nome suggestivo in modo che tu o un altro amministratore possa facilmente identificare di quale regola si tratti.
   c. Scegli il tipo di dati che desideri proteggere
   d. Inserisci i dati che vuoi proteggere (per esempio, il numero di telefono di un dirigente aziendale o il nome interno di un nuovo prodotto a cui l'azienda sta lavorando). È accettata qualsiasi combinazione di parole, numeri o stringhe consistente in caratteri alfanumerici e speciali (come @, # o $).

      Assicurati di inserire almeno cinque caratteri per evitare il blocco erroneo di messaggi e-mail e pagine web.

      Importante

      I dati forniti vengono memorizzati in forma cifrata sugli endpoint protetti, ma possono essere visualizzati sull'account della Control Center. Per una sicurezza maggiore, non inserire tutti i dati che desideri proteggere. In questo caso, devi annullare l'opzione **Solo parola esatta**.

   e. Configura le opzioni di scansione del traffico come necessario.
      - **Scansione web (traffico HTTP)** - controlla il traffico HTTP (web) e blocca i dati in uscita corrispondenti ai dati della regola.
      - **Esamina e-mail (traffico SMTP)** - Esamina il traffico SMTP (posta) e blocca le mail in uscita contenenti i dati della regola.

      Puoi scegliere di applicare la regola solo se i dati della regola corrispondono completamente oppure se le maiuscole/minuscole corrispondono.
   f. Clicca su **Salva**. La nuova regola sarà aggiunta all'elenco.

3. Configura le esclusioni per le regole di protezione dei dati in modo che gli utenti possano ancora inviare dati protetti a siti web e destinatari autorizzati. Le eccezioni possono essere applicate globalmente (a tutte le regole) o solo a determinate regole. Per aggiungere un'eccezione:
   a. Clicca sul pulsante **Aggiungi** nel lato superiore della tabella. Apparirà una finestra di configurazione.
   b. Inserisci gli indirizzi web o e-mail di cui gli utenti sono autorizzati a divulgare dati protetti.
   c. Seleziona il tipo di eccezione (indirizzo web o e-mail).
   d. Nella tabella **Regole**, seleziona la o le regole di protezione dei dati a cui applicare tale eccezione.
   e. Clicca su **Salva**. La nuova regola di eccezione sarà aggiunta all'elenco.

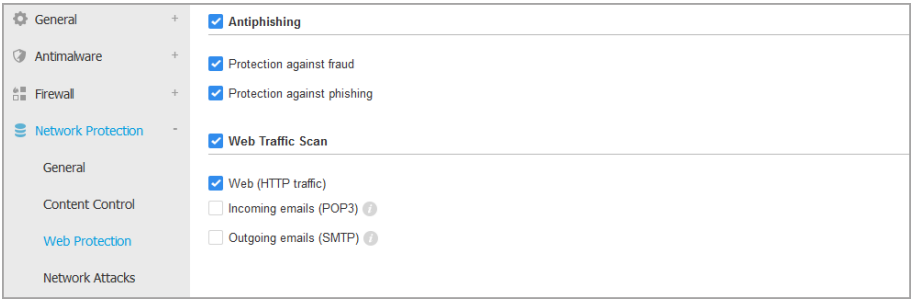
Nota
Se un'e-mail contenente dati bloccati viene indirizzata a più destinatari, quelli per cui sono stati definite delle eccezioni la riceveranno.

Per eliminare una regola o un'eccezione dall'elenco, clicca sul corrispondente pulsante **Elimina** nel lato destro della tabella.

Protezione web

In questa pagina, le impostazioni sono organizzate nelle seguenti sezioni:

- Antiphishing
- Scansione del traffico web



Policy - Protezione rete - Protezione web

Antiphishing

La protezione antiphishing blocca automaticamente le pagine phishing note per impedire agli utenti di divulgare inavvertitamente informazioni private o confidenziali a eventuali truffatori online. Al posto di una pagina web phishing, viene mostrata una speciale pagina di avvertimento nel browser per informare l'utente che la pagina web richiesta è pericolosa.

Seleziona **Antiphishing** per attivare la protezione antiphishing. Puoi modificare ulteriormente l'Antiphishing configurando le seguenti impostazioni:

- **Protezione dalle frodi**. Seleziona questa opzione se vuoi estendere la protezione ad altri tipi di truffe oltre al phishing. Per esempio, i siti web rappresentanti false società, che non possono richiedere direttamente informazioni private, ma invece cercano di comportarsi come attività legittime per fare un profitto ingannando le persone a fare affari con loro.
- **Protezione da phishing**. Mantieni questa opzione selezionata per proteggere gli utenti dai tentativi di phishing.

Se una pagina web legittima viene rilevata in maniera errata come phishing e bloccata, puoi aggiungerla alla whitelist per consentire agli utenti di accedervi. L'elenco dovrebbe contenere solo siti web di cui ti fidi completamente.

Per gestire le eccezioni dell'antiphishing:

1. Vai alle impostazioni **Generali** e clicca su **Eccezioni globali**.
2. Inserisci l'indirizzo web e clicca sul pulsante ⊕ **Aggiungi**.

   Se vuoi escludere un intero sito web, scrivi il nome del dominio, come `http://www.website.com`, mentre se desideri escludere solo una pagina web, scrivi l'indirizzo web esatto di tale pagina.

   Nota
   I caratteri jolly non sono accettati per creare URL.

3. Per rimuovere un'eccezione dall'elenco, clicca sul corrispondente pulsante ⊗ **Elimina**.
4. Clicca su **Salva**.

Scansione del traffico web

Le e-mail in entrata (POP3) e il traffico web sono esaminati in tempo reale per impedire di scaricare malware sull'endpoint. Le e-mail in uscita (SMTP) sono esaminate per impedire ai malware di infettare altri endpoint. Controllare il traffico web potrebbe rallentare leggermente la navigazione web, ma impedirà l'accesso a ogni malware tramite Internet o i download.

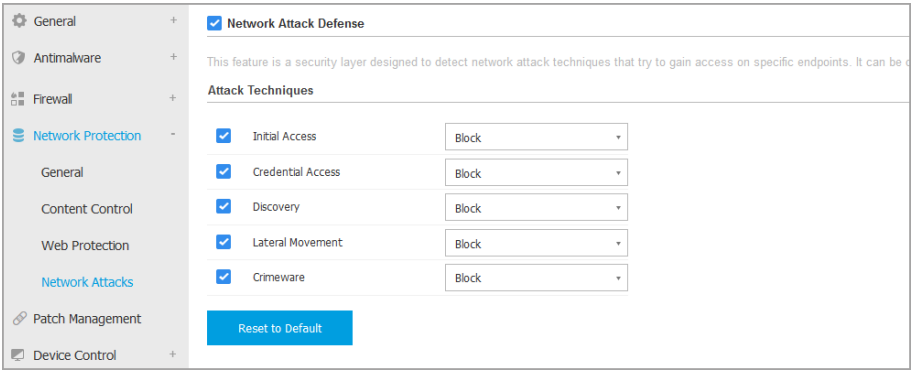
Quando un'e-mail viene rilevata come infetta, viene sostituita automaticamente con un'e-mail standard che informa il destinatario dell'e-mail infetta originale. Se una pagina web contiene o distribuisce malware, viene bloccata automaticamente. Invece viene mostrata una speciale pagina di avviso per informare l'utente che la pagina web richiesta è pericolosa.

Sebbene non consigliabile, per aumentare le prestazioni del sistema, puoi disattivare la scansione di e-mail e traffico web. Questa non è una grave minaccia finché rimane attiva la scansione all'accesso dei file.

Nota
Le opzioni **E-mail in arrivo** e **E-mail in uscita** non sono disponibili per macOS.

Attacchi alla rete

Network Attack Defense offre un livello di sicurezza basato su una tecnologia di Bitdefender che rileva e intraprende azioni contro gli attacchi alla rete progettati per ottenere accesso agli endpoint attraverso tecniche specifiche, come attacchi di forza bruta, exploit di rete e furti di password.



Policy - Protezione rete - Attacchi alla rete

Per configurare Network Attack Defense:

1. Seleziona la casella **Network Attack Defense** per attivare il modulo.
2. Seleziona le caselle corrispondenti per attivare la protezione da ogni categoria di attacco alla rete. Le tecniche di attacco alla rete vengono raggruppate in base alle conoscenze della MITRE ATT&CK come segue:
   - **Accesso iniziale** - L'aggressore riesce a penetrare in una rete tramite diversi mezzi, tra cui vulnerabilità di server destinati al pubblico. Per esempio: exploit di divulgazione delle informazioni, exploit di inserimento SQL, vettori di inserimento download drive-by.
   - **Credenziali di accesso** - L'aggressore ruba le credenziali, come nomi utente e password, per ottenere accesso ai sistemi. Per esempio: attacchi di forza bruta, exploit di autenticazione non autorizzati, furti di password.
   - **Discovery** - L'aggressore, una volta penetrato, cerca di ottenere informazioni sui sistemi e la rete interna, prima di decidere la propria mossa. Per esempio, exploit di attraversamento directory o exploit di attraverso directory HTTP.
   - **Movimento laterale** - L'aggressore esplora la rete, spesso spostandosi tra più sistemi, per trovare il bersaglio principale. L'aggressore potrebbe usare strumenti specifici per realizzare tale obiettivo. Per esempio: exploit di inserimento comandi, exploit di Shellshock o exploit di doppia estensione.
   - **Crimeware** - Questa categoria include tecniche progettate per automatizzare i crimini informatici. Per esempio, le tecniche di Crimeware sono: exploit Nuclear, oltre diversi software malware come Trojan e bot.
3. Seleziona le azioni che vuoi intraprendere contro ciascuna categoria di tecniche di attacco alla rete dalle seguenti opzioni:
   a. **Blocca** - Network Attack Defense blocca i tentativi di attacco, una volta rilevati.
   b. **Segnala solo** - Network Attack Defense ti informa sul tentativo di attacco rilevato, ma non cercherà di fermarlo.

Puoi facilmente ripristinare le impostazioni iniziali, cliccando sul pulsante **Torna a predefinite** nel lato inferiore della pagina.

I dettagli sui tentativi di attacco alla rete sono disponibili nei rapporti Incidenti rete e nella notifica dell'evento Incidenti di rete.

7.2.6. Patch Management

Nota
Questo modulo è disponibile per:

- Windows for workstations
- Windows for servers

Il modulo Gestione patch ti libera dal peso di dover mantenere aggiornati gli endpoint con tutte le ultime patch disponibili per i vari software, distribuendo e installando le patch automaticamente per una vasta gamma di prodotti.

Nota
Puoi controllare l'elenco di fornitori e prodotti supportati in questo articolo della KB.

Questa sezione della policy include le impostazioni per un impiego automatico delle patch. Per prima cosa, configurerai come le patch vengono scaricate sugli endpoint e poi sceglierai quali patch installare e quando.

Configurare le impostazioni di download delle patch

Il processo di diffusione delle patch utilizza Patch Caching Server per ottimizzare il traffico di rete. Gli endpoint si collegano a questi server e scaricano le patch tramite la rete locale. Per una maggiore disponibilità delle patch, si consiglia di usare più di un server.

Per assegnare i Patch Caching Server agli endpoint bersaglio:

1. Nella sezione **Impostazioni download patch**, clicca sul campo nel lato superiore del tavolo. Viene mostrato l'elenco dei Patch Caching Server rilevati.

   Se l'elenco è vuoto, allora devi installare il ruolo Patch Caching Server sui Relay nella tua rete. Per maggiori informazioni, fai riferimento alla Guida di installazione.

2. Seleziona il server che desideri nell'elenco.
3. Clicca sul pulsante ⊕ **Aggiungi**.
4. Ripeti i passaggi precedenti per aggiungere più server, se necessario.
5. Usa le frecce su e giù nel lato destro della tabella per stabilire la priorità del server. La priorità diminuisce dall'alto verso il basso dell'elenco.

Un endpoint richiede una patch dai server assegnati in ordine di priorità. L'endpoint scarica la patch dal server in cui la trova prima. Un server che manca di una patch necessaria la scaricherà automaticamente dal fornitore, rendendola disponibile per le richieste future.

Per eliminare i server non più necessari, clicca sul pulsante ⊖ Elimina corrispondente nel lato destro della tabella.

Seleziona l'opzione **Usa i siti web dei fornitori come posizione di riserva per scaricare le patch** per assicurarti che i tuoi endpoint ricevano le patch dei software nel caso in cui i Patch Caching Server non siano disponibili.

Configurare la scansione e l'installazione delle patch

GravityZone esegue l'impiego delle patch in due fasi indipendenti:

1. Valutazione. Se richiesto tramite la console di gestione, gli endpoint eseguono una scansione per le patch mancanti, segnalandole.
2. Installazione. La console invia agli agenti un elenco di patch che vuoi installare. L'endpoint scarica le patch dal Patch Caching Server e poi le installa.

La policy fornisce le impostazioni per automatizzare questi processi, parzialmente o interamente, in modo che vengano eseguiti periodicamente, in base al programma preferito.

Per impostare la scansione automatica delle patch:

1. Seleziona la casella **Scansione automatica patch**.
2. Usa le opzioni di programmazione per configurare la ricorrenza della scansione. Puoi impostare la scansione per essere eseguita giornalmente o in determinati giorni della settimana, in un dato momento.
3. Seleziona **Esegui una scansione intelligente in caso di installazione di una nuova app/programma** per rilevare ogni volta che una nuova applicazione viene installata sull'endpoint e quali patch sono disponibili per essa.

Per configurare l'installazione automatica delle patch:

1. Seleziona la casella **Installa patch automaticamente dopo la scansione**.
2. Seleziona quali tipi di patch installare: sicurezza, altre o entrambe.
3. Usa le opzioni di programmazione per configurare quando eseguire le attività di installazione. Puoi impostare la scansione per essere eseguita immediatamente dopo il termine della scansione delle patch, giornalmente o

in determinati giorni della settimana, in un dato momento. Consigliamo di installare immediatamente le patch di sicurezza che sono state trovate.

4. Di norma, tutti i prodotti sono idonei per l'applicazione delle patch. Se vuoi solo aggiornare automaticamente un set di prodotti, che consideri essenziali per la tua attività, segui questi passaggi:
   a. Seleziona la casella **Specifica fornitore e prodotto**.
   b. Clicca sul campo **Fornitore** nel lato superiore della tabella. Viene mostrato un elenco con tutti i fornitori supportati.
   c. Scorri l'elenco e seleziona un fornitore per i prodotti a cui vuoi installare una patch.
   d. Clicca sul campo **Prodotti** nel lato superiore della tabella. Viene mostrato un elenco con tutti i prodotti del fornitore selezionato.
   e. Seleziona tutti i prodotti a cui vuoi applicare la patch.
   f. Clicca sul pulsante ⊕ **Aggiungi**.
   g. Ripeti i passaggi precedenti per i restanti fornitori e prodotti.

      Se hai dimenticato di aggiungere un prodotto o vuoi rimuoverne uno, trova il fornitore nella tabella, clicca due volte sul campo **Prodotti** e seleziona o deseleziona il prodotto nell'elenco.

   Per rimuovere un fornitore con tutti i suoi prodotti, trovalo nella tabella e clicca sul pulsante ⊖ **Elimina** corrispondente nel lato destro della tabella.
5. Per vari motivi, un endpoint potrebbe essere offline quando viene pianificata l'installazione di una patch. Seleziona l'opzione **Se mancante, eseguila il prima possibile** per installare immediatamente le patch una volta che l'endpoint è tornato online.
6. Alcune patch potrebbero richiedere un riavvio di sistema per completare l'installazione. Se desideri farlo manualmente, seleziona l'opzione **Posticipa riavvio**.

Importante
Affinché valutazione e installazione abbiano successo su endpoint Windows, devi assicurarti che vengano soddisfatti i seguenti requisiti:

- **Trusted Root Certification Authorities** conserva il certificato **DigiCert Assured ID Root CA**.

- **Intermediate Certification Authorities** include il **DigiCert SHA2 Assured ID Code Signing CA**.
- Gli endpoint devono aver installato le patch per Windows 7 e Windows Server 2008 R2 indicate in questo articolo di Microsoft: Microsoft Security Advisory 3033929

7.2.7. Controllo dispositivi

Nota
Questo modulo è disponibile per:

- Windows for workstations
- Windows for servers
- macOS

Il modulo Controllo dispositivi consente di prevenire la sottrazione di dati sensibili e le infezioni di malware tramite dispositivi esterni collegati agli endpoint, applicando regole ed eccezioni di blocco tramite una policy a una vasta gamma di tipi di dispositivi.

Importante
Per macOS, Controllo dispositivi si basa su un'estensione del kernel. Su macOS High Sierra (10.13.x) e versioni superiori, l'installazione di un'estensione del kernel richiede l'approvazione dell'utente. Il sistema comunica all'utente che è stata bloccata un'estensione di sistema da Bitdefender. L'utente può autorizzarla dalle preferenze in **Protezione & Privacy**. Fin quando l'utente non approva l'estensione di sistema di Bitdefender, questo modulo non funzionerà e l'interfaccia utente di Endpoint Security for Mac mostrerà un problema critico, chiedendo l'approvazione.
Per eliminare l'intervento dell'utente, puoi pre-approvare l'estensione del kernel di Bitdefender inserendola nella whitelist usando uno strumento di Mobile Device Management. Per maggiori dettagli sulle estensioni del kernel Bitdefender, fai riferimento a questo articolo della KB.

Per utilizzare il modulo Controllo dispositivi, devi prima includerlo nell'agente di sicurezza installato sui target di riferimento, poi attivare l'opzione **Controllo dispositivi** nella policy applicata a questi endpoint. In seguito, ogni volta che un dispositivo viene connesso a un endpoint gestito, l'agente di sicurezza invierà informazioni relative a questo evento alla Control Center, tra cui il nome del dispositivo, la classe, l'ID e l'ora e la data di connessione.

Nella tabella seguente puoi trovare i tipi di dispositivi supportati da Controllo dispositivi su sistemi Windows e macOS:

Tipo di dispositivo	Windows	macOS
Adattatori di Bluetooth	x	x
Unità CD-ROM	x	x
Unità floppy disk	x	N/A
IEEE 1284.4	x	
IEEE 1394	x	
Unità di imaging	x	x
Modem	x	Gestito sotto adattatori di rete
Unità a nastri	x	N/A
Windows Portable	x	x
Porte COM/LPT	x	Porte LPT/seriali supportate
SCSI Raid	x	
Stampanti	x	Supporta solo stampanti collegate in locale
Adattatore di rete	x	x (inclusi adattatori Wi-Fi)
Adattatori di rete wireless	x	x
Archivio interno	x	
Archivio esterno	x	x

Nota

- Su macOS, se il permesso **Personale** viene selezionato per una determinata classe di dispositivi, sarà applicato solo il permesso configurato per la sottocategoria **Altro**.
- Su Windows e macOS, Controllo dispositivi autorizza o nega l'accesso all'intero adattatore Bluetooth a livello di sistema, in base alla policy. Non c'è alcuna possibilità di impostare le eccezioni granulari per i dispositivi abbinati.

Controllo dispositivi consente di gestire i permessi dei dispositivi come segue:

- Definire le regole di permesso

- Definire le eccezioni di permesso

Regole

La sezione **Regole** consente di definire i permessi per i dispositivi connessi agli endpoint di destinazione.

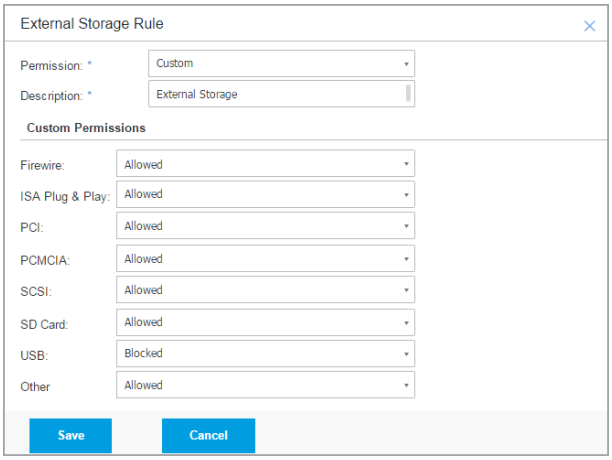
Per impostare i permessi per il tipo di dispositivo che desideri:

1. Vai a **Controllo dispositivi > Regole**.
2. Clicca sul nome del dispositivo nella tabella disponibile.
3. Seleziona un tipo di permesso dalle opzioni disponibili. Ricorda che il set di permessi disponibile potrebbe variare in base al tipo di dispositivo:
   - **Consentito**: il dispositivo può essere utilizzato sull'endpoint di destinazione.
   - **Bloccato**: il dispositivo non può essere utilizzato sull'endpoint di destinazione. In questo caso, ogni volta che il dispositivo viene connesso all'endpoint, l'agente di sicurezza invierà una notifica indicante che il dispositivo è stato bloccato.

     Importante
     I dispositivi collegati precedentemente bloccati non vengono sbloccati automaticamente cambiando l'impostazione dell'autorizzazione in **Consentito**. Per poter usare il dispositivo, l'utente deve ricollegarlo o riavviare il sistema.

   - **Solo lettura**: sul dispositivo è possibile usare solo le funzioni di lettura.
   - **Personalizzato**: definisci diversi permessi per ogni tipo di porta dello stesso dispositivo, come Firewire, ISA Plug & Play, PCI, PCMCIA, USB, ecc. In questo caso, viene mostrato l'elenco di componenti disponibili per il dispositivo selezionato ed è impossibile impostare i permessi che desideri per ogni componente.

     Per esempio, per dispositivi di archiviazione esterni, puoi bloccare solo la porta USB, consentendo l'utilizzo di tutte le altre porte.



Policy - Controllo dispositivi - Regole

Eccezioni

Dopo aver impostato le regole dei permessi per i diversi tipi di dispositivo, potresti voler escludere determinati dispositivi o tipi di prodotto da tali regole.

Puoi definire le eccezioni dei dispositivi:

- Tramite l'ID del dispositivo (o l'ID dell'hardware) per designare singoli dispositivi che desideri escludere.
- Tramite l'ID del prodotto (o PID), per designare una gamma di dispositivi prodotti dallo stesso produttore.

Per definire le eccezioni alle regole per dispositivi:

1. Vai a **Controllo dispositivi > Eccezioni**.
2. Attiva l'opzione **Eccezioni**.
3. Clicca sul pulsante ⊕**Aggiungi** nel lato superiore della tabella.
4. Seleziona il metodo che vuoi utilizzare per aggiungere le eccezioni:
   - **Manualmente**. In questo caso, devi inserire ciascun ID dispositivo o ID prodotto che vuoi escludere, a patto di avere a portata di mano l'elenco degli ID appropriati:
     a. Seleziona il tipo di eccezione (tramite ID prodotto o ID dispositivo).

b. Nel campo **Eccezioni**, inserisci gli ID che vuoi escludere.
c. Nel campo **Descrizione**, inserisci un nome che ti aiuterà a identificare il dispositivo o la gamma di dispositivi.
d. Seleziona il tipo di permesso per i dispositivi indicati (**Consentito** o **Bloccato**).
e. Clicca su **Salva**.

Nota
Puoi configurare manualmente eccezioni con caratteri jolly in base all'ID del dispositivo, usando la sintassi `wildcards:deviceID`. Usa il punto interrogativo (?) per sostituire un carattere e l'asterisco per sostituire un qualsiasi numero di caratteri in `deviceID`. Ad esempio, con `wildcards:PCI\VEN_8086*`, verranno esclusi dalla regola della policy tutti i dispositivi che contengono la stringa `PCI\VEN_8086` nel proprio ID.

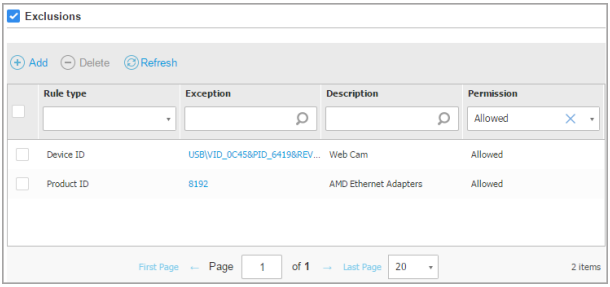
- **Dai dispositivi scoperti**. In questo caso, puoi selezionare gli ID dispositivo o ID prodotto per escluderli da un elenco di tutti i dispositivi scoperti nella tua rete (relativi solo agli endpoint gestiti):
  a. Seleziona il tipo di eccezione (tramite ID prodotto o ID dispositivo).
  b. Nella tabella **Eccezioni**, seleziona gli ID che vuoi escludere:
     – Per gli ID dispositivo, seleziona ciascun dispositivo per escluderlo dall'elenco.
     – Per gli ID prodotto, selezionando un dispositivo, escluderai tutti i dispositivi aventi lo stesso ID prodotto.
  c. Nel campo **Descrizione**, inserisci un nome che ti aiuterà a identificare il dispositivo o la gamma di dispositivi.
  d. Seleziona il tipo di permesso per i dispositivi indicati (**Consentito** o **Bloccato**).
  e. Clicca su **Salva**.

Importante
- I dispositivi già connessi agli endpoint all'installazione di Bitdefender Endpoint Security Tools saranno scoperti solo dopo aver riavviato gli endpoint corrispondenti.
- I dispositivi collegati precedentemente bloccati non vengono sbloccati automaticamente impostando un'eccezione con autorizzazione **Consentito**. Per poter usare il dispositivo, l'utente deve ricollegarlo o riavviare il sistema.

Tutte le eccezioni dei dispositivi compariranno nella tabella **Eccezioni**.

Per rimuovere un'eccezione:

1. Selezionala nella tabella.
2. Clicca sul pulsante ⊕ **Elimina** nel lato superiore della tabella.



Policy - Controllo dispositivi - Eccezioni

7.2.8. Relay

Nota
Questo modulo è disponibile per:

- Windows for workstations
- Windows for servers
- Linux

Questa sezione ti consente di definire le impostazioni di comunicazione e aggiornamento per gli endpoint di destinazione assegnati con ruolo di relay.

Le impostazioni sono organizzate nelle seguenti sezioni:

- Comunicazione
- Aggiornamento

Comunicazione

La tabella **Comunicazione** contiene le preferenze di proxy per la comunicazione tra gli endpoint relay e i componenti di GravityZone.

Se necessario, puoi configurare in maniera indipendente la comunicazione tra gli endpoint relay e i servizi cloud di Bitdefender / GravityZone, utilizzando le seguenti impostazioni:

- **Mantieni impostazioni installazione** per utilizzare le stesse impostazioni proxy definite con il pacchetto di installazione.
- **Usa proxy definito nella sezione General**, per usare le impostazioni proxy definite nella policy attuale, nella sezione **Generale > Impostazioni**.
- **Non usarla**, quando gli endpoint di destinazione non comunicano con determinate componenti di Bitdefender tramite proxy.

Aggiornamento

Questa sezione ti consente di definire le impostazioni di aggiornamento per gli endpoint bersaglio con ruolo di relay:

- Nella sezione **Aggiornamento**, puoi configurare le seguenti impostazioni:
  - L'intervallo di tempo quando gli endpoint relay cercano gli aggiornamenti.
  - La cartella localizzata sull'endpoint relay in cui vengono scaricati e anche replicati gli aggiornamenti delle firme e del prodotto. Se vuoi definire una determinata cartella di download, inserisci il suo percorso completo nel campo corrispondente.

    Importante
    Si consiglia di definire una cartella dedicata per gli aggiornamenti del prodotto e delle firme. Evita di selezionare una cartella contenente file di sistema o personali.

- La posizione di aggiornamento predefinita per gli agenti relay è http://upgrade.bitdefender.com. Puoi specificare altri percorsi inserendo l'indirizzo IP o l'hostname locale di una o più macchine relay nella tua rete, poi configurare la loro priorità utilizzando i tasti su e giù mostrati passandoci sopra con il mouse. Se il primo percorso di aggiornamento non è disponibile, viene utilizzato il successivo e così via.

  Per definire un percorso di aggiornamento predefinito:

  1. Attiva l'opzione **Definisci percorso aggiornamento personalizzato**.
  2. Inserisci l'indirizzo del nuovo server di aggiornamento nel campo **Aggiungi percorso**. Usa una di queste sintassi:
     - `update_server_ip:port`
     - `update_server_name:port`

La porta standard è 7074.

3. Se l'endpoint relay comunica con il server di aggiornamento locale tramite un server proxy, seleziona **Usa proxy**. Saranno considerate le impostazioni proxy definite nella sezione **Generale > Impostazioni**.
4. Clicca sul pulsante **Aggiungi** nel lato destro della tabella.
5. Utilizza le frecce Su / Giù nella colonna **Azione** per impostare la priorità dei percorsi di aggiornamento definiti. Se il primo percorso di aggiornamento non è disponibile, viene considerato il successivo e così via.

Per rimuovere una posizione dalla lista, clicca sul pulsante **Elimina** corrispondente. Sebbene tu possa rimuovere il percorso di aggiornamento predefinito, non è consigliabile farlo.

7.2.9. Exchange Protection

Nota
Questo modulo è disponibile per Windows for servers.

Security for Exchange viene fornito con impostazioni altamente configurabili, che proteggono i Server di Microsoft Exchange da minacce come malware, spam e phishing. Con la Protezione Exchange installata sul tuo server mail, puoi anche filtrare le e-mail contenenti allegati o contenuti considerati pericolosi in base alle policy di sicurezza della tua azienda.

Per mantenere le prestazioni del server a livelli normali, il traffico e-mail viene elaborato dai filtri Security for Exchange nel seguente ordine:

1. Filtro antispam
2. Controllo contenuti > Filtro contenuti
3. Controllo contenuti > Filtro allegati
4. Filtro antimalware

Le impostazioni di Security for Exchange sono organizzate nelle seguenti sezioni:

- Generale
- Antimalware
- Antispam
- Controllo contenuti

Generale

In questa sezione, puoi creare e gestire gruppi di account e-mail, definire l'età degli elementi in quarantena ed escludere determinati mittenti.

Gruppi di utenti

La Control Center consente di creare gruppi utente per applicare diverse policy di scansione e filtraggio a diverse categorie di utenti. Per esempio, puoi creare policy appropriate per il dipartimento IT, per il team vendite o per i dirigenti dell'azienda.

I gruppi utente sono disponibili a livello aziendale, indipendentemente dalla policy o l'utente che li ha creati.

Pr creare un gruppo utente:

1. Clicca sul pulsante ⊕**Aggiungi** nel lato superiore della tabella. Viene mostrata la finestra dei dettagli.
2. Inserisci il nome del gruppo, la descrizione e gli indirizzi e-mail degli utenti.

   Nota
   - Per un grande elenco di indirizzi e-mail, puoi copiare e incollare l'elenco da un file di testo.
   - Separatori accettati nell'elenco: spazio, virgola, punto e virgola e Invio.

3. Clicca su **Salva**.

I gruppi personalizzati sono modificabili. Clicca sul nome del gruppo per aprire la finestra di configurazione, dove puoi modificare i dettagli del gruppo o l'elenco degli utenti.

Per rimuovere un gruppo personalizzato dall'elenco, seleziona il gruppo e clicca sul pulsante ⊖ **Elimina** nel lato superiore della tabella.

Impostazioni

- **Elimina i file in quarantena più vecchi di (giorni).** Di norma, i file in quarantena più vecchi di 15 giorni sono eliminati automaticamente. Se vuoi modificare questo intervallo, inserisci un altro valore nel campo corrispondente.
- **Connessione con Blacklist.** Con questa opzione attivata, il Server Exchange rifiuta tutte le e-mail dai mittenti inseriti nella blacklist.

  Per creare una blacklist:
  1. Clicca sul link **Modifica gli elementi nella blacklist**.

2. Inserisci gli indirizzi e-mail che vuoi bloccare. Modificando l'elenco, puoi anche utilizzare i seguenti caratteri jolly per definire un intero dominio e-mail o un modello per gli indirizzi e-mail:
   - Asterisco (*), per sostituire lo zero, uno o più caratteri.
   - Punto di domanda (?), sostituendo un singolo carattere.

   Per esempio, inserendo `*@boohouse.com`, saranno bloccati tutti gli indirizzi e-mail da `boohouse.com`.
3. Clicca su **Salva**.

Controllo IP dominio (anticamuffamento)

Usa questo filtro per impedire agli spammer di mascherare l'indirizzo e-mail del mittente e far sembrare che il messaggio sia stato inviato da un contatto di fiducia. Puoi specificare l'indirizzo IP autorizzato a inviare e-mail per i tuoi domini e-mail e, se necessario, per altri domini e-mail noti. Se un'e-mail sembra provenire da un dominio nell'elenco, ma l'indirizzo IP non corrisponde a uno di quelli indicati, l'e-mail viene rifiutata.

Avvertimento
Non utilizzare questo filtro se stai usando uno smarthost, un servizio di filtraggio e-mail hosted o una soluzione gateway di filtraggio delle e-mail con i tuoi server Exchange.

Importante

- Il filtro controlla solo le connessioni e-mail non autenticate.
- Pratiche consigliate:
  - Si consiglia di utilizzare questo filtro solo su Exchange Server che sono connessi direttamente a Internet. Per esempio, se hai entrambi i server Edge Transport e Hub Transport, configura questo filtro solo sui server Edge.
  - Aggiungi all'elenco di domini tutti gli indirizzi IP interni consentiti per inviare e-mail tramite connessioni SMTP non autenticate. Ciò potrebbe includere sistemi di notifica automatica, equipaggiamenti di rete, come stampanti, ecc.
  - In una configurazione di Exchange che utilizza i gruppi di disponibilità del database, aggiungi anche all'elenco dei domini gli indirizzi IP di tutti i server di Hub Transport e Mailbox.
  - Procedi con cautela se vuoi configurare gli indirizzi IP autorizzati per determinati domini e-mail esterni che non sono sotto la tua gestione. Se non

riesci a mantenere aggiornato l'elenco degli indirizzi IP, i messaggi e-mail di questi domini saranno rifiutati. Se stai utilizzando un backup MX, devi aggiungere a tutti i domini e-mail configurati gli indirizzi IP da cui il backup MX inoltra i messaggi e-mail al tuo server mail primario.

Per configurare il filtro anticamuffamento, segui questi passaggi:

1. Seleziona la casella **Controllo IP dominio (anticamuffamento)** per attivare il filtro.
2. Clicca sul pulsante **Aggiungi** nel lato superiore della tabella. Apparirà la finestra di configurazione.
3. Inserisci il dominio e-mail nel campo corrispondente.
4. Fornisci la gamma di indirizzi IP autorizzati da usare con il dominio indicato in precedenza, utilizzando il formato CIDR (maschera IP/Rete).
5. Clicca sul pulsante **Aggiungi** nel lato destro della tabella. Gli indirizzi IP vengono aggiunti alla tabella.
6. Per eliminare una gamma di IP dall'elenco, clicca sul corrispondente pulsante **Elimina** sul lato destro della tabella.
7. Clicca su **Salva**. Il dominio viene aggiunto al filtro.

Per eliminare un dominio e-mail dal filtro, selezionalo nella tabella Anticamuffamento e clicca sul pulsante **Elimina** nel lato superiore della tabella.

Antimalware

Il modulo antimalware protegge i server mail Exchange da ogni tipo di minaccia malware (virus, Trojan, spyware, rootkit, adware, ecc.), rilevando elementi infetti o sospetti, e tentando di disinfettarli o isolare l'infezione, in base alle azioni indicate.

La scansione antimalware viene eseguita a due livelli:

- Livello di Trasporto
- Store Exchange

Scansione a livello di Trasporto

Bitdefender Endpoint Security Tools si integra con gli agenti mail di trasporto per esaminare tutto il traffico e-mail.

Di norma, la scansione a livello di trasporto è attivata. Bitdefender Endpoint Security Tools filtra il traffico e-mail e, se richiesto, informa gli utenti delle azioni intraprese aggiungendo un testo nel corpo dell'e-mail.

Usa la casella **Filtro antimalware** per disattivare o riattivare questa funzionalità.

Per configurare un testo di notifica, clicca sul link **Impostazioni**. Sono disponibili le seguenti opzioni:

- **Aggiungi piè di pagina a e-mail esaminate.** Seleziona questa casella per aggiungere una frase nella parte inferiore delle e-mail esaminate. Per modificare il testo predefinito, inserisci il tuo messaggio nella casella di testo sottostante.
- **Testo sostitutivo.** Per e-mail i cui allegati sono stati eliminati o messi in quarantena, può essere allegato un file di notifica. Per modificare i testi di notifica predefiniti, inserisci il tuo messaggio nelle caselle di testo corrispondenti.

Il filtro antimalware si basa sulle regole. Ogni e-mail che raggiunge il server mail viene controllato in base alle regole del filtro antimalware, per ordine di priorità, finché non corrisponde una regola. Poi l'e-mail viene elaborata in base alle opzioni specificate da quella regola.

Gestire le regole di filtraggio

Puoi visualizzare tutte le regole esistenti indicate nella tabella, insieme alle informazioni sulla loro priorità, stato ed estensione. Le regole sono ordinate in base alla priorità con la prima regola che la massima priorità.

Ogni policy antimalware ha un ruolo predefinito che diventa attivo una volta che il filtro antimalware viene attivato. Che cosa devi sapere sul ruolo predefinito:

- Non puoi copiare, disattivare o eliminare la regola.
- Puoi modificare solo le azioni e le impostazioni di scansione.
- La regola predefinita è sempre la più bassa.

Creare Regole

Hai due alternative per creare le regole del filtro:

- Inizia dalle impostazioni predefinite, seguendo questi passaggi:
  1. Clicca sul pulsante ⊕ **Aggiungi** nel lato superiore della tabella per aprire la finestra di configurazione.
  2. Configura le impostazioni della regola. Per maggiori dettagli relativi alle opzioni, fai riferimento a Opzioni regola.
  3. Clicca su **Salva**. La regola viene elencata per prima nella tabella.

- Usa un clone di una regola personale come modello, seguendo questi passaggi:
  1. Seleziona la regola che desideri dalla tabella.
  2. Clicca sul pulsante **Clona** nel lato superiore della tabella per aprire la finestra di configurazione.
  3. Imposta le opzioni della regola in base alle tue esigenze.
  4. Clicca su **Salva**. La regola viene elencata per prima nella tabella.

Modificare delle Regole

Per modificare una regola esistente:

1. Clicca sul nome della regola per aprire la finestra di configurazione.
2. Inserisci i nuovi valori per le opzioni che desideri modificare.
3. Clicca su **Salva**. Le modifiche avranno effetto una volta che la policy viene salvata.

Impostare la priorità della regola

Per modificare la priorità di una regola:

1. Seleziona la regola da spostare.
2. Usa i pulsanti **Su** o **Giù** nel lato superiore della tabella per aumentare o ridurre la priorità della regola.

Eliminare delle Regole

Puoi eliminare una o più regole personali alla volta. Tutto ciò che ti serve è:

1. Seleziona la casella delle regole da eliminare.
2. Clicca sul pulsante **Elimina** nel lato superiore della tabella. Una volta eliminata una regola, non potrai più ripristinarla.

Opzioni della regola

Sono disponibili le seguenti opzioni:

- **Generale.** In questa sezione devi impostare un nome per la regola, diversamente non potrai salvarla. Seleziona la casella **Attiva** se vuoi che la regola sia efficace una volta salvata la policy.
- **Estensione della regola** Puoi limitare la regola a un sottoinsieme di e-mail, impostando le seguenti opzioni di estensione cumulative:
  - **Applica a (direzione).** Seleziona la direzione del traffico e-mail alla quale sarà applicata la regola.
  - **Mittenti.**Z Puoi decidere se applicare la regola a ogni mittente o solo a determinati mittenti. Per limitare la gamma di mittenti, clicca sul pulsante **Specifica** e seleziona i gruppi desiderati dalla tabella sulla sinistra. Visualizza i gruppi selezionati nella tabella sulla destra.

- **Destinatari.** Puoi decidere se applicare la regola a ogni destinatario o solo a determinati destinatari. Per limitare la gamma di destinatari, clicca sul pulsante **Specifica** e seleziona i gruppi desiderati dalla tabella sulla sinistra. Puoi visualizzare i gruppi selezionati nella tabella sulla destra.

  La regola viene applicata ogni volta che un destinatario corrisponde alla tua selezione. Se vuoi applicare la regola solo se tutti i destinatari si trovano nei gruppi selezionati, seleziona **Abbina tutti i destinatari**.

  Nota
  Gli indirizzi nei campi **Cc** e **Bcc** sono anch'essi destinatari.

  Importante
  Le regole basate sui gruppi di utenti si applicano solo ai ruoli Mailbox e Hub Transport.

- **Opzioni.** Configura le opzioni di scansione per le e-mail che corrispondono alla regola:
  - **Tipi di file esaminati.** Usa questa opzione per specificare quali tipi di file vuoi che vengano esaminati. Puoi scegliere di esaminare tutti i file (indipendentemente dalla loro estensione), solo i file delle applicazioni o determinate estensioni che ritieni possano essere pericolose. Esaminare tutti i file ti garantisce la migliore protezione, mentre si consiglia di controllare solo le applicazioni per eseguire una scansione più veloce.

    Nota
    I file delle applicazioni sono più vulnerabili agli attacchi dei malware rispetto ad altri tipi di file. Per maggiori informazioni, fai riferimento a «Tipi di file applicazioni» (p. 458).

    Se vuoi esaminare solo i file con determinate estensioni, hai due alternative:
    - **Estensioni definite dall'utente**, dove devi fornire solo le estensioni da esaminare.
    - **Tutti i file, tranne determinate estensioni**, dove devi inserire solo le estensioni che la scansione deve ignorare.
  - **Dimensione massima allegati/corpo e-mail (MB).** Seleziona questa casella e inserisci un valore nel campo corrispondente per impostare la dimensione massima accettata di un file in allegato o del corpo dell'e-mail da esaminare.
  - **Profondità massima archivio (livelli).** Seleziona la casella e scegli la profondità massima dell'archivio nel campo corrispondente. Più il livello di

profondità è basso, maggiori saranno le prestazioni e minore il grado di protezione.
  - **Esamina applicazioni potenzialmente non desiderate (PUA).** Seleziona questa casella per eseguire una scansione per possibili applicazioni dannose o non desiderate, come adware, che potrebbero essere installate sui sistemi senza il consenso dell'utente, modificare il comportamento di diversi prodotti software e ridurre le prestazioni del sistema.
- **Azioni.** Puoi specificare diverse azioni che l'agente di sicurezza può intraprendere automaticamente sui file, in base al tipo di rilevazione.

  Il tipo di rilevazione divide i file in tre categorie:
  - **File infetti.** Bitdefender rileva i file infetti attraverso diversi meccanismi avanzati, che includono tecnologie basate su firme dei malware, apprendimento automatico e intelligenza artificiale (IA).
  - **File sospetti.** Questi file vengono rilevati come sospetti dall'analisi euristica e da altre tecnologie di Bitdefender. Queste forniscono un tasso di rilevazione elevato, ma in alcuni casi gli utenti devono fare attenzione a determinati falsi positivi (file puliti rilevati come sospetti).
  - **File non esaminabili.** Questi file non possono essere esaminati. I file esaminabili includono, ma non solo, file protetti da password, cifrati o supercompressi.

  Per ogni tipo di rilevazione, hai un'azione predefinita o principale, e un'azione alternativa in caso di fallimento della principale. Anche se non consigliato, puoi modificare queste azioni nei menu corrispondenti. Scegli l'azione da intraprendere:
  - **Disinfetta.** Rimuove il codice malware dai file infetti e ricostruisce il file originale. Per alcuni particolari tipologie di malware, non è possibile usare la disinfezione perché il file rilevato è interamente dannoso. Si consiglia di impostarla sempre come prima azione da intraprendere sui file infetti. I file sospetti non possono essere disinfettati, perché non è disponibile alcuna routine di disinfezione.
  - **Respingi/Elimina e-mail.** Sui server con ruolo di Edge Transport, l'e-mail rilevata viene respinta con un codice di errore 550 SMTP. In tutti gli altri casi, l'e-mail viene eliminata senza alcun avviso. È consigliabile evitare di usare questa azione.
  - **Elimina file.** Elimina gli allegati con problemi senza alcun avviso. È consigliabile evitare di usare questa azione.
  - **Sostituisci file.** Elimina i file con problemi e inserisci un file di testo che avvisa l'utente delle azioni intraprese.

- **Sposta file in quarantena.** Sposta i file rilevati nella cartella della quarantena e inserisce un file di testo che avvisa l'utente dell'azione intrapresa. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Puoi gestire i file in quarantena dalla pagina **Quarantena**.

  > **Nota**
  > Ti ricordiamo che la quarantena per Exchange Server richiede spazio su disco aggiuntivo nella partizione in cui l'agente di sicurezza viene installato. Lo spazio della quarantena dipende dal numero di oggetti memorizzati e dalla loro dimensione.

- **Non fare nulla.** Nessuna azione verrà intrapresa sui file rilevati. Questi file appariranno solo nel registro della scansione. Le attività di scansione sono configurate in modo predefinito per ignorare i file sospetti. Potresti volere modificare l'azione predefinita in modo da mettere i file sospetti in quarantena.
- Di norma, quando un'e-mail corrisponde all'applicazione di una regola, viene elaborata esclusivamente in conformità con la regola stessa, senza essere esaminata nuovamente per le altre regole. Se vuoi continuare il controllo in base alle altre regole, deseleziona la casella **Se le condizioni della regola vengono soddisfatte, blocca l'elaborazione di altre regole**.

Eccezioni

Se vuoi che un determinato traffico e-mail venga ignorato da ogni regola di filtro, puoi definire delle eccezioni alla scansione. Per creare un'eccezione:

1. Espandi la sezione **Eccezioni per regole antimalware**.
2. Clicca sul pulsante ⊖ **Aggiungi** da questa sezione della barra degli strumenti, che apre la finestra di configurazione.
3. Configura le impostazioni di eccezione. Per maggiori dettagli sulle opzioni, fai riferimento a Opzioni regola.
4. Clicca su **Salva**.

Scansione Store Exchange

La Protezione Exchange utilizza Exchange Web Services (EWS) di Microsoft per consentire la scansione delle mailbox Exchange e dei database di cartelle pubbliche. Puoi configurare il modulo antimalware per eseguire regolarmente attività di scansione a richiesta sui database bersaglio, in base a un tuo programma.

Nota

- La scansione a richiesta è disponibile solo per Exchange Server con il ruolo Mailbox installato.
- Ricordati che la scansione a richiesta aumenta il consumo di risorse e in base alle opzioni di scansione e al numero di elementi da esaminare, può richiedere parecchio tempo per terminare.

La scansione a richiesta richiede un account amministratore di Exchange (account di servizio) per impersonare gli utenti Exchange e recuperare gli elementi bersagli da esaminare dalle mailbox degli utenti e le cartelle pubbliche. Si consiglia di creare un account dedicato a tale scopo.

L'account amministratore di Exchange deve soddisfare i seguenti requisiti:

- Deve essere membro del gruppo di Gestione dell'organizzazione (Exchange 2016, 2013 e 2010)
- Deve essere membro del gruppo Amministratori Exchange dell'organizzazione (Exchange 2007)
- Ha una casella di posta allegata.

Attivare la scansione a richiesta

1. Nella sezione **Attività di scansione**, clicca sul link **Aggiungi credenziali**.
2. Inserisci il nome utente e la password dell'account di servizio.
3. Se l'e-mail differisce dal nome utente, devi anche fornire l'indirizzo e-mail dell'account di servizio.
4. Inserisci l'URL di Exchange Web Services (EWS), necessario quando l'Exchange Autodiscovery non funziona.

Nota

- Il nome utente deve includere il nome del dominio, nel formato `user@domain` o `domain\user`.
- Non dimenticare di aggiornare le credenziali nella Control Center, ogni volta che vengono cambiate.

Gestire le attività di scansione

La tabella delle attività di scansione mostra tutte le attività in programma e fornisce informazioni sulle loro destinazioni e la loro ricorrenza.

Per creare attività per scansioni di Exchange Store:

1. Nella sezione **Attività di scansione**, clicca sul pulsante ⊕ **Aggiungi** nel lato superiore della tabella per aprire la finestra di configurazione.
2. Configura le impostazioni dell'attività come descritto nella seguente sezione.
3. Clicca su **Salva**. L'attività viene aggiunta nell'elenco e diventa efficace una volta salvata la policy.

Puoi modificare un'attività in qualsiasi momento cliccando sul nome dell'attività.

Per rimuovere attività dall'elenco, selezionale e clicca sul pulsante ⊖ **Elimina** nel lato superiore della tabella.

Impostazioni attività di scansione

Le attività hanno una serie di impostazioni qui descritte:

- **Generale.** Inserisci un nome specifico per l'attività.

  Nota
  Puoi visualizzare il nome dell'attività nella cronologia di Bitdefender Endpoint Security Tools.

- **Programmazione.** Usa le opzioni di programmazione per configurare il programma della scansione. Puoi impostare la scansione per essere eseguita ogni tot ore, giorni o settimane, partendo da una determinata ora o data. Per i database maggiori, l'attività di scansione potrebbe richiedere molto tempo e influenzare le prestazioni del server. In tali casi, puoi configurare l'attività per fermarla dopo un certo periodo.
- **Destinazione.** Scegli i contenitori e gli elementi da esaminare. Puoi scegliere di esaminare caselle di posta, cartelle pubbliche o entrambe. Oltre alle e-mail, puoi scegliere di esaminare altri oggetti, come **Contatti**, **Attività**, **Appuntamenti** e **Elementi pubblicati**. Inoltre, puoi impostare le seguenti restrizioni ai contenuti da sottoporre a scansione:
  - Solo messaggi non letti
  - Solo elementi con allegati
  - Solo nuovi elementi, ricevuti in un determinato intervallo di tempo

  Per esempio, puoi scegliere di esaminare solo le e-mail dalle caselle di posta dell'utente, ricevuti negli ultimi sette giorni.

  Seleziona la casella **Eccezioni**, se vuoi definire delle eccezioni per la scansione. Per creare un'eccezione, usa i campi nelle intestazioni della tabella nel seguente modo:
  1. Seleziona il tipo di archivio dal menu.

2. In base al tipo di archivio, specifica l'elemento da escludere:

Tipo di archivio	Formato elemento
Casella di posta	Indirizzo e-mail
Cartella pubblica	Il percorso della cartella, a partire dalla radice
Base di dati	L'identità del database

> **Nota**
> Per ottenere l'identità del database, usa il comando shell di Exchange:
> `Get-MailboxDatabase | fl name,identity`

Puoi inserire un solo elemento alla volta. Se hai diversi elementi dello stesso tipo, devi definire tante regole quante il numero di elementi.

3. Clicca sul pulsante ⊕ **Aggiungi** nel lato superiore della tabella per salvare l'eccezione e aggiungerla all'elenco.

Per rimuovere una regola di eccezione dall'elenco, clicca sul pulsante ⊖ **Elimina** corrispondente.

- **Opzioni.** Configura le opzioni di scansione per le e-mail che corrispondono alla regola:
  - **Tipi di file esaminati.** Usa questa opzione per specificare quali tipi di file vuoi che vengano esaminati. Puoi scegliere di esaminare tutti i file (indipendentemente dalla loro estensione), solo i file delle applicazioni o determinate estensioni che ritieni possano essere pericolose. Esaminare tutti i file ti garantisce la migliore protezione, mentre si consiglia di controllare solo le applicazioni per eseguire una scansione più veloce.

    > **Nota**
    > I file delle applicazioni sono più vulnerabili agli attacchi dei malware rispetto ad altri tipi di file. Per maggiori informazioni, fai riferimento a «Tipi di file applicazioni» (p. 458).

    Se vuoi esaminare solo i file con determinate estensioni, hai due alternative:
    - **Estensioni definite dall'utente**, dove devi fornire solo le estensioni da esaminare.
    - **Tutti i file, tranne determinate estensioni**, dove devi inserire solo le estensioni che la scansione deve ignorare.

- **Dimensione massima allegati/corpo e-mail (MB).** Seleziona questa casella e inserisci un valore nel campo corrispondente per impostare la dimensione massima accettata di un file in allegato o del corpo dell'e-mail da esaminare.
- **Profondità massima archivio (livelli).** Seleziona la casella e scegli la profondità massima dell'archivio nel campo corrispondente. Più il livello di profondità è basso, maggiori saranno le prestazioni e minore il grado di protezione.
- **Esamina applicazioni potenzialmente non desiderate (PUA).** Seleziona questa casella per eseguire una scansione per possibili applicazioni dannose o non desiderate, come adware, che potrebbero essere installate sui sistemi senza il consenso dell'utente, modificare il comportamento di diversi prodotti software e ridurre le prestazioni del sistema.

- **Azioni.** Puoi specificare diverse azioni che l'agente di sicurezza può intraprendere automaticamente sui file, in base al tipo di rilevazione.

  Il tipo di rilevazione divide i file in tre categorie:
  - **File infetti.** Bitdefender rileva i file infetti attraverso diversi meccanismi avanzati, che includono tecnologie basate su firme dei malware, apprendimento automatico e intelligenza artificiale (IA).
  - **File sospetti.** Questi file vengono rilevati come sospetti dall'analisi euristica e da altre tecnologie di Bitdefender. Queste forniscono un tasso di rilevazione elevato, ma in alcuni casi gli utenti devono fare attenzione a determinati falsi positivi (file puliti rilevati come sospetti).
  - **File non esaminabili.** Questi file non possono essere esaminati. I file esaminabili includono, ma non solo, file protetti da password, cifrati o supercompressi.

  Per ogni tipo di rilevazione, hai un'azione predefinita o principale, e un'azione alternativa in caso di fallimento della principale. Anche se non consigliato, puoi modificare queste azioni nei menu corrispondenti. Scegli l'azione da intraprendere:
  - **Disinfetta.** Rimuove il codice malware dai file infetti e ricostruisce il file originale. Per alcuni particolari tipologie di malware, non è possibile usare la disinfezione perché il file rilevato è interamente dannoso. Si consiglia di impostarla sempre come prima azione da intraprendere sui file infetti. I file sospetti non possono essere disinfettati, perché non è disponibile alcuna routine di disinfezione.
  - **Respingi / Elimina e-mail.** L'e-mail viene eliminata senza alcun preavviso. È consigliabile evitare di usare questa azione.

- **Elimina file.** Elimina gli allegati con problemi senza alcun avviso. È consigliabile evitare di usare questa azione.
- **Sostituisci file.** Elimina i file con problemi e inserisci un file di testo che avvisa l'utente delle azioni intraprese.
- **Sposta file in quarantena.** Sposta i file rilevati nella cartella della quarantena e inserisce un file di testo che avvisa l'utente dell'azione intrapresa. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Puoi gestire i file in quarantena dalla pagina **Quarantena**.

  Nota
  Ti ricordiamo che la quarantena per Exchange Server richiede spazio su disco aggiuntivo nella partizione in cui l'agente di sicurezza viene installato. Lo spazio della quarantena dipende dal numero delle e-mail memorizzate e dalla loro dimensione.

- **Non fare nulla.** Nessuna azione verrà intrapresa sui file rilevati. Questi file appariranno solo nel registro della scansione. Le attività di scansione sono configurate in modo predefinito per ignorare i file sospetti. Potresti volere modificare l'azione predefinita in modo da mettere i file sospetti in quarantena.
- Di norma, quando un'e-mail corrisponde all'applicazione di una regola, viene elaborata esclusivamente in conformità con la regola stessa, senza essere esaminata nuovamente per le altre regole. Se vuoi continuare il controllo in base alle altre regole, deseleziona la casella **Se le condizioni della regola vengono soddisfatte, blocca l'elaborazione di altre regole**.

Antispam

Il modulo Antispam offre più livelli di protezione contro lo spam e il phishing usando una combinazione di diversi filtri e motori per determinare se le e-mail sono spam oppure no.

Nota

- Il filtro antispam è disponibile per:
  - Exchange Server 2016/2013 con ruolo Edge Transport o Mailbox
  - Exchange Server 2010/2007 con ruolo Edge Transport o Hub Transport
- Se hai sia il ruolo Edge e Hub nella tua organizzazione Exchange, si consiglia di attivare il filtro antispam sul server con il ruolo di Edge Transport.

Il filtro spam viene attivato automaticamente per le e-mail in entrata. Usa la casella **Filtro antimalware** per disattivare o riattivare questa funzionalità.

Filtri Antispam

Un'e-mail viene verificata in base alle regole del filtro antispam basate sui gruppi di mittenti e destinatari, per ordine di priorità, finché non corrisponde a una regola. L'e-mail viene elaborata in base alle opzioni della regola e vengono intraprese le relative azioni sullo spam rilevato.

Determinati filtri antispam sono configurabili e puoi controllare se usarli oppure no. Questo è l'elenco dei filtri opzionali:

- **Filtro caratteri.** Molte e-mail spam sono scritte in caratteri cirillici o asiatici. Il filtro caratteri rileva questo tipo di e-mail e tag come SPAM.
- **Contenuti etichettati come sessualmente espliciti.** Spam che contiene materiale sessualmente esplicito, che potrebbe includere l'avviso SESSUALMENTE ESPLICITO: nella linea dell'oggetto. Questo filtro rileva e-mail segnate come SESSUALMENTE ESPLICITO: nell'oggetto e le etichetta come spam.
- **Filtro URL.** Quasi tutte le e-mail spam includono link a diversi siti web. In genere, questi siti contengono altre pubblicità e offrono la possibilità di acquistare eventuali articoli. A volte, sono anche usati per tentativi di phishing.

  Bitdefender mantiene un database di tali link. Il filtro URL esamina ogni link URL in un'e-mail in base al suo database. Se c'è una corrispondenza, l'email viene marcata come spam.
- **Lista Blackhole in Tempo reale (RBL).** Si tratta di un filtro che consente di verificare il server mail del mittente in confronto a eventuali server RBL di terze parti. Il filtro utilizza il protocollo DNSBL e i server RBL per filtrare spam in base alla reputazione di mail server come mittenti di spam.

  L'indirizzo del mail server viene estratto dall'intestazione dell'e-mail e ne viene controllata la validità. Se l'indirizzo appartiene a una classe privata (`10.0.0.0`, `172.16.0.0` a `172.31.0.0` o `192.168.0.0` a `192.168.255.0`), viene ignorato.

  Un controllo di DNS viene eseguito sul dominio `d.c.b.a.rbl.example.com`, dove `d.c.b.a` è l'indirizzo invertito del server e `rbl.example.com` è il server RBL. Se il DNS risponde che il dominio è valido, significa che l'IP è elencato nel server RBL e viene fornito un determinato punteggio al server. Questo punteggio varia da 0 a 100, in base al livello di fiducia assegnato al server.

La query viene eseguita per ogni server RBL nell'elenco e il punteggio restituito da ognuno viene aggiunto al punteggio intermedio. Quando il punteggio ha raggiunto 100, non vengono più eseguite alcune query.

Se il punteggio del filtro RBL è 100 o superiore, l'e-mail viene considerata spam e viene intrapresa l'azione indicata. In caso contrario, un punteggio di spam viene calcolato dal punteggio del filtro RBL e aggiunto al punteggio spam globale dell'e-mail.

- **Filtro euristico.** Sviluppato da Bitdefender, il filtro euristico rileva spam nuovi e sconosciuti. Il filtro viene addestrato automaticamente su grandi volumi di email spam nel Laboratorio antispam di Bitdefender. Durante l'addestramento, impara a distinguere tra spam e messaggi legittimi, oltre a riconoscere i nuovi tipi di spam, rilevando le somiglianze, spesso davvero minime, con e-mail che ha già esaminato. Questo filtro è progettato per migliorare la rilevazione basata su firme, mantenendo il numero di falsi positivi molto basso.
- **Query cloud di Bitdefender.** Bitdefender mantiene un database in costante evoluzione di impronte di e-mail spam nel cloud. Una query contenente l'impronta dell'e-mail viene inviata ai server nel cloud per verificare direttamente se l'e-mail è spam. Anche se l'impronta digitale non viene trovata nel database, viene controllata per altre query recenti e, se si verificano determinate condizioni, viene marcata come spam.

Gestire le regole antispam

Puoi visualizzare tutte le regole esistenti indicate nella tabella, insieme alle informazioni sulla loro priorità, stato ed estensione. Le regole sono ordinate in base alla priorità con la prima regola che la massima priorità.

Ogni policy antispam ha una regola predefinita che diventa attiva una volta attivato il modulo. Che cosa devi sapere sul ruolo predefinito:

- Non puoi copiare, disattivare o eliminare la regola.
- Puoi modificare solo le impostazioni di scansione e le azioni.
- La regola predefinita è sempre la più bassa.

Creare Regole

Per creare una regola:

1. Clicca sul pulsante ⊕ **Aggiungi** nel lato superiore della tabella per aprire la finestra di configurazione.
2. Configura le impostazioni della regola. Per maggiori dettagli sulle opzioni, fai riferimento a «Opzioni regola» (p. 249).
3. Clicca su **Salva**. La regola viene elencata per prima nella tabella.

Modificare delle Regole

Per modificare una regola esistente:

1. Clicca sul nome della regola per aprire la finestra di configurazione.
2. Inserisci i nuovi valori per le opzioni che desideri modificare.
3. Clicca su **Salva**. Se la regola è attiva, le modifiche entreranno in vigore una volta salvata la policy.

Impostare la priorità della regola

Per modificare la priorità di una regola, seleziona la regola che desideri e utilizza le frecce ⊙ **Su** e ⊙ **Giù** nel lato superiore della tabella. Puoi spostare una sola regola alla volta.

Eliminare delle Regole

Se non vuoi più utilizzare una regola, seleziona la regola e clicca sul pulsante ⊙ **Elimina** nel lato superiore della tabella.

Opzioni regola

Sono disponibili le seguenti opzioni:

- **Generale.** In questa sezione devi impostare un nome per la regola, diversamente non potrai salvarla. Seleziona la casella **Attiva** se vuoi che la regola sia efficace una volta salvata la policy.
- **Estensione della regola** Puoi limitare la regola a un sottoinsieme di e-mail, impostando le seguenti opzioni di estensione cumulative:
  - **Applica a (direzione).** Seleziona la direzione del traffico e-mail alla quale sarà applicata la regola.
  - **Mittenti.**Z Puoi decidere se applicare la regola a ogni mittente o solo a determinati mittenti. Per limitare la gamma di mittenti, clicca sul pulsante **Specifica** e seleziona i gruppi desiderati dalla tabella sulla sinistra. Visualizza i gruppi selezionati nella tabella sulla destra.
  - **Destinatari.** Puoi decidere se applicare la regola a ogni destinatario o solo a determinati destinatari. Per limitare la gamma di destinatari, clicca sul pulsante **Specifica** e seleziona i gruppi desiderati dalla tabella sulla sinistra. Puoi visualizzare i gruppi selezionati nella tabella sulla destra.

    La regola viene applicata ogni volta che un destinatario corrisponde alla tua selezione. Se vuoi applicare la regola solo se tutti i destinatari si trovano nei gruppi selezionati, seleziona **Abbina tutti i destinatari**.

    Nota
    Gli indirizzi nei campi **Cc** e **Bcc** sono anch'essi destinatari.

Importante
Le regole basate sui gruppi di utenti si applicano solo ai ruoli Mailbox e Hub Transport.

- **Impostazioni.** Clicca sul livello di sicurezza che si adatta meglio alle tue esigenze (**Aggressivo**, **Normale** o **Permissivo**). Usa la descrizione sul lato destro dell'indicatore per scegliere.

  Inoltre, puoi attivare diversi filtri. Per maggiori informazioni su questi filtri, fai riferimento a «Filtri Antispam» (p. 247).

  Importante
  Il filtro RBL richiede una configurazione aggiuntiva. Puoi configurare il filtro dopo aver reato o modificato la regola. Per maggiori informazioni, fai riferimento a «Configurare il filtro RBL» (p. 251)

  Per le connessioni autenticate puoi scegliere se bypassare o no la scansione antispam.
- **Azioni.** Ci sono diverse azioni che puoi intraprendere sulle e-mail rilevate. Ogni azione ha, a sua volta, diverse possibili opzioni o azioni secondarie. Le trovi qui descritte:

  Azioni principali:
  - **Consegna e-mail.** L'e-mail spam raggiunge le caselle di posta dei destinatari.
  - **Email di quarantena.** L'e-mail viene cifrata e salvata nella cartella della quarantena dell'Exchange Server, senza essere consegnata ai destinatari. Puoi gestire le e-mail in quarantena nella pagina **Quarantena**.
  - **Reindirizza e-mail.** L'e-mail non viene consegnata al destinatario originale, ma a una casella di posta che hai indicato nel campo corrispondente.
  - **Respingi/Elimina e-mail.** Sui server con ruolo di Edge Transport, l'e-mail rilevata viene respinta con un codice di errore 550 SMTP. In tutti gli altri casi, l'e-mail viene eliminata senza alcun avviso. È consigliabile evitare di usare questa azione.

  Azioni secondarie:
  - **Integra con Exchange SCL.** Aggiunge un'intestazione all'e-mail spam, consentendo a Exchange Server o Microsoft Outlook di agire in base al meccanismo di Spam Confidence Level (SCL).

- **Contrassegna l'oggetto dell'e-mail come.** Puoi aggiungere un'etichetta all'oggetto dell'e-mail per aiutare gli utenti a filtrare le e-mail rilevate nel client e-mail.
- **Aggiungi intestazione e-mail.** Alle e-mail rilevate come spam viene aggiunta un'intestazione. Puoi modificare il nome e il valore dell'intestazione inserendo i valori desideri nei campi corrispondenti. Più avanti, puoi utilizzare quest'intestazione dell'e-mail per creare filtri aggiuntivi.
- **Salva e-mail sul disco.** Una copia dell'e-mail di spam viene salvata come un file nella cartella specificata. Fornisci il percorso completo della cartella nel campo corrispondente.

  Nota
  Questa opzione supporta solo e-mail in formato MIME.

- **Archivia nell'account.** Una copia dell'e-mail rilevata viene consegnata all'indirizzo e-mail specificato. Questa azione aggiunge l'indirizzo e-mail specificato all'elenco di e-mail Bcc.

- Di norma, quando un'e-mail corrisponde all'applicazione di una regola, viene elaborata esclusivamente in conformità con la regola stessa, senza essere esaminata nuovamente per le altre regole. Se vuoi continuare il controllo in base alle altre regole, deseleziona la casella **Se le condizioni della regola vengono soddisfatte, blocca l'elaborazione di altre regole**.

Configurare il filtro RBL

Se vuoi utilizzare il filtro RBL, devi fornire un elenco di server RBL.

Per configurare il filtro:

1. Nella pagina **Antispam**, clicca sul link **Impostazioni** per aprire la finestra di configurazione.
2. Fornisci l'indirizzo IP del server DNS per la query e l'intervallo di timeout della query nei campi corrispondenti. Se non è stato configurato alcun indirizzo del server DNS, o se il server DNS non è disponibile, il filtro RBL utilizza i server DNS del sistema.
3. Per ciascun server RBL:
   a. Inserisci l'hostname o l'indirizzo IP del server, e il livello di confidenza che hai assegnato al server nei campi dell'intestazione della tabella.
   b. Clicca sul pulsante ⊕**Aggiungi** nel lato superiore della tabella.
4. Clicca su **Salva**.

Configurare la whitelist dei mittenti

Per mittenti noti di e-mail, puoi prevenire un consumo di risorse del server non necessario, includendoli negli elenchi come mittenti affidabili o non affidabili. Perciò, il server mail accetterà o rifiuterà le email in arrivo da questi mittenti. Per esempio, hai un'intensa comunicazione e-mail con un partner commerciale e per assicurarti di ricevere tutte le e-mail, puoi aggiungere il partner alla whitelist.

Per creare una whitelist di mittenti affidabili:

1. Clicca sul link **Whitelist** per aprire la finestra di configurazione.
2. Seleziona la casella **Whitelist mittenti**.
3. Inserisci gli indirizzi e-mail nel campo corrispondente. Modificando l'elenco, puoi anche utilizzare i seguenti caratteri jolly per definire un intero dominio e-mail o un modello per gli indirizzi e-mail:
   - Asterisco (*), per sostituire lo zero, uno o più caratteri.
   - Punto di domanda (?), sostituendo un singolo carattere.

   Per esempio, inserendo `*.gov`, tutte le e-mail provenienti dal dominio `.gov` saranno accettate.
4. Clicca su **Salva**.

Nota
Per inserire nella blacklist alcuni mittenti noti di spam, usa l'opzione **Connessione con Blacklist** nella sezione **Protezione Exchange > Generale > Impostazioni**

Controllo contenuti

Usa il Controllo contenuti per migliorare la protezione delle e-mail filtrando tutto il traffico e-mail non conforme con le policy aziendali (contenuti non desiderati o potenzialmente sensibili).

Per un controllo generale dei contenuti delle e-mail, questo modulo comprende due opzioni di filtro:

- Filtraggio del Contenuto
- Filtraggio allegati

Nota
Il Filtro contenuti e il Filtro allegati sono disponibili per:

- Exchange Server 2016/2013 con ruolo Edge Transport o Mailbox
- Exchange Server 2010/2007 con ruolo Edge Transport o Hub Transport

Gestire le regole di filtraggio

I filtri di Controllo contenuti si basano sulle regole. Puoi definire varie regole per diversi utenti e gruppi di utenti. Ogni e-mail che raggiunge il server mail viene controllata in base alle regole del filtro, per ordine di priorità, finché non corrisponde a una regola. Poi l'e-mail viene elaborata in base alle opzioni specificate da quella regola.

Le regole di filtro contenuti precedono le regole del filtro allegati.

Le regole di filtro contenuti e allegati sono elencate nelle tabelle corrispondenti in ordine di priorità, con la prima regola che la maggiore priorità. Per ciascuna regola, sono fornite le seguenti informazioni:

- Priorità
- Nome
- Direzione traffico
- Gruppi di mittenti e destinatari

Creare Regole

Hai due alternative per creare le regole del filtro:

- Inizia dalle impostazioni predefinite, seguendo questi passaggi:
  1. Clicca sul pulsante ⊕ **Aggiungi** nel lato superiore della tabella per aprire la finestra di configurazione.
  2. Configura le impostazioni della regola. Per maggiori dettagli su determinate opzioni di filtro contenuti e allegati, fai riferimento a:
     - Opzioni regola filtro contenuti
     - Opzioni regola filtro allegati.
  3. Clicca su **Salva**. La regola viene elencata per prima nella tabella.
- Usa un clone di una regola personale come modello, seguendo questi passaggi:
  1. Seleziona la regola desiderata nella tabella.
  2. Clicca sul pulsante ⧉ **Clona** nel lato superiore della tabella per aprire la finestra di configurazione.
  3. Imposta le opzioni della regola in base alle tue esigenze.
  4. Clicca su **Salva**. La regola viene elencata per prima nella tabella.

Modificare delle Regole

Per modificare una regola esistente:

1. Clicca sul nome della regola per aprire la finestra di configurazione.
2. Inserisci i nuovi valori per le opzioni che desideri modificare.

3. Clicca su **Salva**. Le modifiche avranno effetto una volta che la policy viene salvata.

Impostare la priorità della regola

Per modificare la priorità di una regola:

1. Seleziona la regola da spostare.
2. Usa i pulsanti **Su** o **Giù** nel lato superiore della tabella per aumentare o ridurre la priorità della regola.

Eliminare delle Regole

Puoi eliminare una o più regole personali. Tutto ciò che ti serve è:

1. Seleziona le regole da eliminare.
2. Clicca sul pulsante **Elimina** nel lato superiore della tabella. Una volta eliminata una regola, non potrai più ripristinarla.

Filtro contenuti

Il Filtro contenuti ti aiuta a filtrare il traffico e-mail in base alle stringhe di caratteri che hai definito in precedenza. Queste stringhe sono comparate con l'oggetto della e-mail o con il contenuto testuale del corpo del messaggio. Utilizzando il Filtro contenuti, puoi ottenere i seguenti obiettivi:

- Impedire a contenuti di e-mail indesiderate di accedere alle caselle di posta di Exchange Server.
- Bloccare e-mail in uscita contenenti dati confidenziali.
- Archiviare e-mail che soddisfano determinate condizioni in un altro account e-mail o sul disco. Per esempio, puoi salvare le e-mail inviate agli indirizzi e-mail del supporto della tua azienda in una cartella sul disco locale.

Attivare il Filtro contenuti

Se desideri utilizzare il filtro dei contenuti, seleziona la casella **Filtro contenuti**.

Per creare e gestire regole del filtro contenuti, fai riferimento a «Gestire le regole di filtraggio» (p. 253).

Opzioni della regola

- **Generale.** In questa sezione devi impostare un nome per la regola, diversamente non potrai salvarla. Seleziona la casella **Attiva** se vuoi che la regola sia efficace una volta salvata la policy.
- **Estensione della regola** Puoi limitare la regola a un sottoinsieme di e-mail, impostando le seguenti opzioni di estensione cumulative:

- **Applica a (direzione).** Seleziona la direzione del traffico e-mail alla quale sarà applicata la regola.
- **Mittenti.**Z Puoi decidere se applicare la regola a ogni mittente o solo a determinati mittenti. Per limitare la gamma di mittenti, clicca sul pulsante **Specifica** e seleziona i gruppi desiderati dalla tabella sulla sinistra. Visualizza i gruppi selezionati nella tabella sulla destra.
- **Destinatari.** Puoi decidere se applicare la regola a ogni destinatario o solo a determinati destinatari. Per limitare la gamma di destinatari, clicca sul pulsante **Specifica** e seleziona i gruppi desiderati dalla tabella sulla sinistra. Puoi visualizzare i gruppi selezionati nella tabella sulla destra.

  La regola viene applicata ogni volta che un destinatario corrisponde alla tua selezione. Se vuoi applicare la regola solo se tutti i destinatari si trovano nei gruppi selezionati, seleziona **Abbina tutti i destinatari**.

  Nota
  Gli indirizzi nei campi **Cc** e **Bcc** sono anch'essi destinatari.

  Importante
  Le regole basate sui gruppi di utenti si applicano solo ai ruoli Mailbox e Hub Transport.

- **Impostazioni.** Configura le espressioni da cercare nelle e-mail, come descritto di seguito:
  1. Seleziona la parte dell'e-mail da verificare:
     - L'oggetto dell'e-mail, selezionando la casella **Filtra per oggetto**. Tutte le e-mail il cui soggetto contiene una delle espressioni inserite nella tabella corrispondente saranno filtrate.
     - Il contenuto del corpo, selezionando la casella **Filtra per contenuto corpo**. Saranno filtrate tutte le e-mail che contengono nel proprio testo una qualsiasi delle espressioni.
     - Sia l'oggetto che il contenuto del corpo, selezionando entrambe le caselle. Tutte le e-mail il cui l'oggetto corrisponde a una regola della prima tabella e il corpo contiene una qualsiasi espressione della seconda tabella, vengono filtrate. Per esempio:

       La prima tabella contiene le espressioni: `newsletter` e `settimanale`. La seconda tabella contiene le espressioni: `shopping`, `prezzo` e `offerta`.

Un'e-mail con l'oggetto "**Newsletter** mensile del tuo fornitore di orologi preferito" e il corpo con la frase "Abbiamo il piacere di presentarti la nostra ultima **offerta** per alcuni orologi sensazionali a prezzi **incredibili**." corrisponderà a una regola e sarà filtrata. Se l'oggetto è "Notizie dal tuo fornitore di orologi", l'e-mail non viene filtrata.

2. Crea le liste di condizioni, usando i campi nelle intestazioni della tabella. Per ciascuna condizione, segui questi passaggi:
   a. Seleziona il tipo di espressione usato nelle ricerche. Puoi scegliere di inserire l'espressione di testo esatta o creare modelli di testo con l'uso di espressioni comuni.

      Nota
      La sintassi delle espressioni normali viene verificata a livello grammaticale da ECMAScript.

   b. Inserisci la stringa di ricerca nel campo **Espressione**.

      Per esempio:

      i. L'espressione `5[1-5]\d{2}([\s\-]?\d{4}){3}` corrisponde alle carte bancarie con numeri che iniziano da 51 a 55, hanno 16 cifre in gruppi di quattro, e i gruppi possono essere separati da uno spazio o un trattino. Inoltre, ogni e-mail contenente il numero della carta in uno dei seguenti formati, `5257-4938-3957-3948`, `5257 4938 3957 3948` o `5257493839573948`, sarà filtrata.

      ii. Questa espressione rileva e-mail con i termini `lotteria`, `denaro` e `premio`, in questo stesso ordine:

      ```
      (lottery)((.|\n|\r)*)( cash)((.|\n|\r)*)( prize)
      ```

      Per rilevare le e-mail che includono tutti e tre i termini indipendentemente dal loro ordine, aggiungi tre espressioni regolari con un ordine di parole diverse.

      iii. Questa espressione rileva le e-mail che includono tre o più casi della parola `premio`:

      ```
      (prize)((.|\n|\r)*)( prize)((.|\n|\r)*)( prize)
      ```

c. Se vuoi differenziare le lettere maiuscolo dalle minuscole nei confronti del testo, seleziona la casella **Maiuscole/Minuscole**. Per esempio, con la casella selezionata, `Newsletter` non è la stessa cosa di `newsletter`.

d. Se non vuoi che l'espressione non faccia parte di altre parole, seleziona la casella **Tutta la parola**. Per esempio, con la casella selezionata, l'espressione `stipendio di Anna` non corrisponde a `stipendio di MariAnna`.

e. Clicca sul pulsante ⊕ **Aggiungi** nell'intestazione della colonna **Azione** per aggiungere la condizione all'elenco.

- **Azioni.** Ci sono diverse azioni che puoi intraprendere sulle e-mail. Ogni azione ha, a sua volta, diverse possibili opzioni o azioni secondarie. Le trovi qui descritte:

  Azioni principali:
  - **Consegna e-mail.** L'e-mail rilevata raggiunge le caselle di posta dei destinatari.
  - **Quarantena.** L'e-mail viene cifrata e salvata nella cartella della quarantena dell'Exchange Server, senza essere consegnata ai destinatari. Puoi gestire le e-mail in quarantena nella pagina **Quarantena**.
  - **Reindirizza a.** L'e-mail non viene consegnata al destinatario originale, ma a una casella di posta che hai indicato nel campo corrispondente.
  - **Respingi/Elimina e-mail.** Sui server con ruolo di Edge Transport, l'e-mail rilevata viene respinta con un codice di errore 550 SMTP. In tutti gli altri casi, l'e-mail viene eliminata senza alcun avviso. È consigliabile evitare di usare questa azione.

  Azioni secondarie:
  - **Contrassegna l'oggetto dell'e-mail come.** Puoi aggiungere un'etichetta all'oggetto dell'e-mail rilevata per aiutare gli utenti a filtrare le e-mail nel client e-mail.
  - **Aggiungi un'intestazione ai messaggi e-mail.** Puoi aggiungere un nome dell'intestazione e un valore alle intestazioni delle e-mail rilevate, inserendo i valori desiderati nei campi corrispondenti.
  - **Salva e-mail sul disco.** Una copia dell'e-mail rilevata viene salvata come un file nella cartella indicata sull'Exchange Server. Se la cartella non esiste, sarà creata. Devi fornire il percorso completo della cartella nel campo corrispondente.

Nota
Questa opzione supporta solo e-mail in formato MIME.

- **Archivia nell'account.** Una copia dell'e-mail rilevata viene consegnata all'indirizzo e-mail specificato. Questa azione aggiunge l'indirizzo e-mail specificato all'elenco di e-mail Bcc.

- Di norma, quando un'e-mail corrisponde alle condizioni di una regola, non viene più controllata per ogni altra regola. Se vuoi continuare a elaborare altre regole, deseleziona la casella **Se le condizioni della regola vengono soddisfatte, blocca l'elaborazione di altre regole**.

Eccezioni

Se vuoi che il traffico e-mail per determinati mittenti o destinatari venga recapitato indipendentemente da qualsiasi regola di filtro dei contenuti, puoi definire delle eccezioni per il filtro.

Per creare un'eccezione:

1. Clicca sul link **Eccezioni** accanto alla casella **Filtro contenuti**. Questa azione apre la finestra di configurazione.
2. Inserisci gli indirizzi e-mail dei mittenti e/o dei destinatari affidabili nei campi corrispondenti. Ogni e-mail proveniente da un mittente affidabile o destinata a un destinatario affidabile viene esclusa dal filtraggio. Modificando l'elenco, puoi anche utilizzare i seguenti caratteri jolly per definire un intero dominio e-mail o un modello per gli indirizzi e-mail:
   - Asterisco (*), per sostituire lo zero, uno o più caratteri.
   - Punto di domanda (?), sostituendo un singolo carattere.

   Per esempio, inserendo `*.gov`, tutte le e-mail provenienti dal dominio `.gov` saranno accettate.
3. Per le e-mail con più destinatari, puoi selezionare la casella **Escludi e-mail dal filtro solo se tutti i destinatari sono affidabili** per applicare l'eccezione solo se tutti i destinatari dell'e-mail sono presenti nell'elenco dei destinatari affidabili.
4. Clicca su **Salva**.

Filtro allegati

Il modulo Filtro allegati offre funzionalità di filtro per gli allegati e-mail. Può rilevare allegati con determinati modelli di nome o di un certo tipo. Utilizzando il Filtro allegati, puoi:

- Blocca allegati potenzialmente pericolosi, come file `.vbs` o `.exe`, o le e-mail che li contengono.
- Blocca allegati con nomi offensivi o le e-mail che li contengono.

Attivare il Filtro allegati

Se desideri usare il Filtro allegati, seleziona la casella **Filtro allegati**.

Per creare e gestire le regole del filtro allegati, fai riferimento a «Gestire le regole di filtraggio» (p. 253).

Opzioni della regola

- **Generale.** In questa sezione devi impostare un nome per la regola, diversamente non potrai salvarla. Seleziona la casella **Attiva** se vuoi che la regola sia efficace una volta salvata la policy.
- **Estensione della regola** Puoi limitare la regola a un sottoinsieme di e-mail, impostando le seguenti opzioni di estensione cumulative:
  - **Applica a (direzione).** Seleziona la direzione del traffico e-mail alla quale sarà applicata la regola.
  - **Mittenti.**Z Puoi decidere se applicare la regola a ogni mittente o solo a determinati mittenti. Per limitare la gamma di mittenti, clicca sul pulsante **Specifica** e seleziona i gruppi desiderati dalla tabella sulla sinistra. Visualizza i gruppi selezionati nella tabella sulla destra.
  - **Destinatari.** Puoi decidere se applicare la regola a ogni destinatario o solo a determinati destinatari. Per limitare la gamma di destinatari, clicca sul pulsante **Specifica** e seleziona i gruppi desiderati dalla tabella sulla sinistra. Puoi visualizzare i gruppi selezionati nella tabella sulla destra.

    La regola viene applicata ogni volta che un destinatario corrisponde alla tua selezione. Se vuoi applicare la regola solo se tutti i destinatari si trovano nei gruppi selezionati, seleziona **Abbina tutti i destinatari**.

    Nota
    Gli indirizzi nei campi **Cc** e **Bcc** sono anch'essi destinatari.

    Importante
    Le regole basate sui gruppi di utenti si applicano solo ai ruoli Mailbox e Hub Transport.

- **Impostazioni.** Specifica i file consentiti o bloccati negli allegati delle e-mail.

  Puoi filtrare gli allegati delle e-mail per tipo o nome del file.

Per filtrare gli allegati per tipo di file, segui questi passaggi:

1. Seleziona la casella **Rileva per tipo di contenuto**.
2. Seleziona l'opzione di rilevamento più adatta alle tue esigenze:
   - **Solo le seguenti categorie**, quando hai un elenco limitato di categorie di tipi di file vietati.
   - **Tutte tranne le seguenti categorie**, quando hai un elenco limitato di categorie di tipi di file consentiti.
3. Seleziona le categorie dei tipi di file di tuo interesse dall'elenco disponibile. Per maggiori dettagli sulle estensioni di ciascuna categoria, fai riferimento a «Tipi di file filtro allegati» (p. 459).

   Se sei interessato solo ad alcuni tipi specifici di file, seleziona la casella **Estensioni personalizzate** e inserisci l'elenco delle estensioni nel campo corrispondente.
4. Seleziona la casella **Attiva rilevazione tipo di file reale** per verificare le intestazioni del file e identificare correttamente il tipo di allegato quando si esegue una scansione per estensioni limitate. Ciò significa che un'estensione non può essere semplicemente rinominata bypassando le policy di filtro degli allegati.

   Nota
   La rilevazione del tipo reale può richiedere molte risorse.

Per filtrare gli allegati per nome, seleziona la casella **Rileva per nome del file** e inserisci i nomi dei file che vuoi filtrare, nei campi corrispondenti. Modificando l'elenco, puoi anche utilizzare i seguenti caratteri jolly per definire i modelli:

- Asterisco (*), per sostituire lo zero, uno o più caratteri.
- Punto di domanda (?), sostituendo un singolo carattere.

Per esempio, inserendo `database.*`, tutti i file chiamati `database`, indipendentemente dalla loro estensione, saranno rilevati.

Nota
Se attivi sia le rilevazioni per tipo di contenuto e nome del file (senza la rilevazione del tipo reale), il file deve soddisfare contemporaneamente le condizioni per entrambi i tipi di rilevazione. Per esempio, hai selezionato la categoria **Multimedia** e inserito il nome del file `test.pdf`. In questo caso, ogni e-mail supera la regola perché il file PDF non è un file multimediale.

Seleziona la casella **Scansiona all'interno degli archivi** per impedire che i file bloccati vengano nascosti in archivi apparentemente innocui, bypassando quindi la regola di filtro.

La scansione è ricorrente negli archivi e di norma va fino al quarto livello di profondità dell'archivio. Puoi ottimizzare la scansione come descritto di seguito:

1. Seleziona la casella **Profondità massima archivio (livelli)**.
2. Scegli un valore diverso nel menu corrispondente. Per le migliori prestazioni, scegli il valore inferiore, mentre per la massima protezione, seleziona il valore maggiore.

Nota
Se hai selezionato di esaminare gli archivi, l'opzione **Scansiona all'interno degli archivi** viene disattivata e vengono esaminati tutti gli archivi.

- **Azioni.** Ci sono diverse azioni che puoi intraprendere sugli allegati rilevato o sulle e-mail che li contengono. Ogni azione ha, a sua volta, diverse possibili opzioni o azioni secondarie. Le trovi qui descritte:

  Azioni principali:
  - **Sostituisci file.** Elimina i file rilevati e inserisci un file di testo che avvisa l'utente delle azioni intraprese.

    Per configurare il testo di notifica:
    1. Clicca sul link **Impostazioni** accanto alla casella **Filtro allegati**.
    2. Inserisci il testo di notifica nel campo corrispondente.
    3. Clicca su **Salva**.
  - **Elimina file.** Elimina i file rilevati senza alcun avviso. È consigliabile evitare di usare questa azione.
  - **Respingi/Elimina e-mail.** Sui server con ruolo di Edge Transport, l'e-mail rilevata viene respinta con un codice di errore 550 SMTP. In tutti gli altri casi, l'e-mail viene eliminata senza alcun avviso. È consigliabile evitare di usare questa azione.
  - **Email di quarantena.** L'e-mail viene cifrata e salvata nella cartella della quarantena dell'Exchange Server, senza essere consegnata ai destinatari. Puoi gestire le e-mail in quarantena nella pagina **Quarantena**.
  - **Reindirizza e-mail a.** L'e-mail non viene consegnata al destinatario originale, ma a un indirizzo e-mail che hai indicato nel campo corrispondente.
  - **Consegna e-mail.** Consente all'e-mail di passare.

Azioni secondarie:

- **Contrassegna l'oggetto dell'e-mail come.** Puoi aggiungere un'etichetta all'oggetto dell'e-mail rilevata per aiutare gli utenti a filtrare le e-mail nel client e-mail.
- **Aggiungi intestazione e-mail.** Puoi aggiungere un nome dell'intestazione e un valore alle intestazioni delle e-mail rilevate, inserendo i valori desiderati nei campi corrispondenti.
- **Salva e-mail sul disco.** Una copia dell'e-mail rilevata viene salvata come un file nella cartella indicata sull'Exchange Server. Se la cartella non esiste, sarà creata. Devi fornire il percorso completo della cartella nel campo corrispondente.

  Nota
  Questa opzione supporta solo e-mail in formato MIME.

- **Archivia nell'account.** Una copia dell'e-mail rilevata viene consegnata all'indirizzo e-mail specificato. Questa azione aggiunge l'indirizzo e-mail specificato all'elenco di e-mail Bcc.

- Di norma, quando un'e-mail corrisponde all'applicazione di una regola, viene elaborata esclusivamente in conformità con la regola stessa, senza essere esaminata nuovamente per le altre regole. Se vuoi continuare il controllo in base alle altre regole, deseleziona la casella **Se le condizioni della regola vengono soddisfatte, blocca l'elaborazione di altre regole**.

Eccezioni

Se vuoi che il traffico e-mail per determinati mittenti o destinatari venga recapitato indipendentemente da qualsiasi regola di filtro degli allegati, puoi definire delle eccezioni per il filtro.

Per creare un'eccezione:

1. Clicca sul link **Eccezioni** accanto alla casella **Filtro allegati**. Questa azione apre la finestra di configurazione.
2. Inserisci gli indirizzi e-mail dei mittenti e/o dei destinatari affidabili nei campi corrispondenti. Ogni e-mail proveniente da un mittente affidabile o destinata a un destinatario affidabile viene esclusa dal filtraggio. Modificando l'elenco, puoi anche utilizzare i seguenti caratteri jolly per definire un intero dominio e-mail o un modello per gli indirizzi e-mail:
   - Asterisco (*), per sostituire lo zero, uno o più caratteri.
   - Punto di domanda (?), sostituendo un singolo carattere.

Per esempio, inserendo `*.gov`, tutte le e-mail provenienti dal dominio `.gov` saranno accettate.

3. Per le e-mail con più destinatari, puoi selezionare la casella **Escludi e-mail dal filtro solo se tutti i destinatari sono affidabili** per applicare l'eccezione solo se tutti i destinatari dell'e-mail sono presenti nell'elenco dei destinatari affidabili.
4. Clicca su **Salva**.

7.2.10. Cifratura

Nota
Questo modulo è disponibile per:

- Windows for workstations
- Windows for servers
- macOS

Il modulo Cifratura gestisce la cifratura completa del disco sugli endpoint sfruttando rispettivamente BitLocker su Windows e FileVault e l'utility con linea di comando diskutil su macOS.

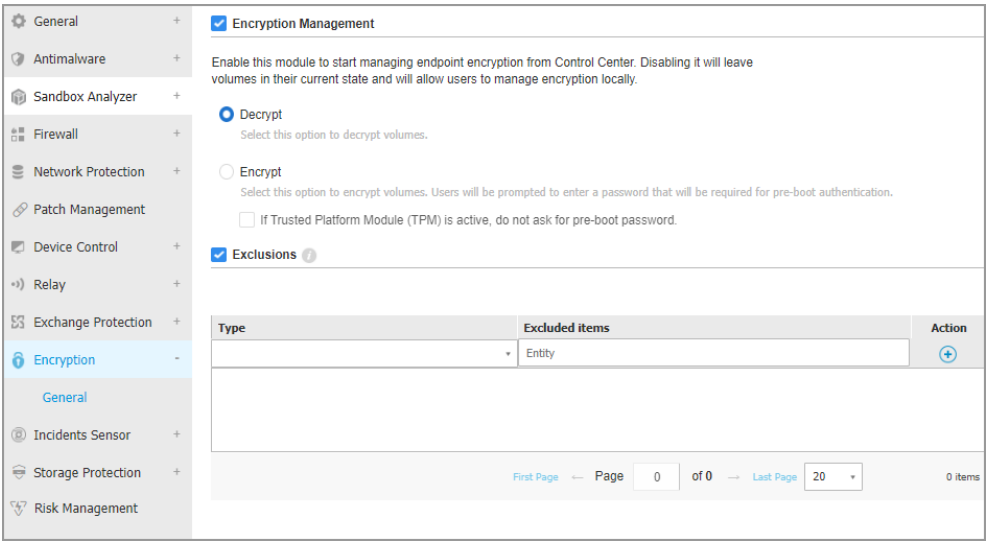
Con questo approccio, GravityZone è in grado di fornire alcuni importanti vantaggi:

- Dati protetti in caso di dispositivi smarriti o rubati.
- Ampia protezione per le piattaforme informatiche più popolari al mondo usando gli standard di cifratura suggeriti con pieno supporto di Microsoft e Apple.
- Impatto minimo sulle prestazioni degli endpoint grazie agli strumenti di cifratura nativi.

Il modulo Cifratura funziona con le seguenti soluzioni:

- BitLocker versione 1.2 e successive, su endpoint Windows con un Trusted Platform Module (TPM), per volumi di avvio e non-avvio.
- BitLocker versione 1.2 e successive, su endpoint Windows senza un TPM, per volumi di avvio e non-avvio.
- FileVault su endpoint macOS, per volumi di avvio.
- diskutil su endpoint macOS, per volumi di non-avvio.

Per l'elenco dei sistemi operativi supportati dal modulo Cifratura, fai riferimento alla Guida di installazione di GravityZone.



La pagina Cifratura

Per iniziare a gestire la cifratura dell'endpoint da Control Center, seleziona la casella **Gestione cifratura**. Finché questa impostazione è attivata, gli utenti dell'endpoint non possono gestire la cifratura a livello locale e tutte le loro azioni saranno annullate o riportate allo stato originale. Disattivando questa impostazione lascerai i volumi dell'endpoint nel loro stato attuale (cifrato o non cifrato) e gli utenti potranno gestire la cifratura sulle proprie macchine.

Per gestire i processi di cifratura e decifratura, sono disponibili tre opzioni:

- **Decifra** - Decifra i volumi e li mantiene tali quando la policy è attiva sugli endpoint.
- **Cifra** - Cifra i volumi e li mantiene tali quando la policy è attiva sugli endpoint.

  Nell'opzione Cifra, puoi selezionare la casella **Se il Trusted Platform Module (TPM) è attivo, non chiedere la password di cifratura**. Questa impostazione fornisce una cifratura su endpoint Windows con TPM, senza richiedere una password di cifratura dagli utenti. Per maggiori dettagli, fai riferimento a «Volumi di cifratura» (p. 265).
- **Eccezioni**

GravityZone supporta il metodo Advanced Encryption Standard (AES) con codici a 128 e 256 bit su Windows e macOS. L'algoritmo di cifratura attuale usato dipende dalla configurazione di ciascun sistema operativo.

Nota
GravityZone rileva e gestisce i volumi cifrati manualmente con BitLocker, FileVault e diskutil. Per iniziare a gestire questi volumi, l'agente di sicurezza chiederà agli utenti degli endpoint di modificare i propri codici di recupero. In caso di altre soluzioni di cifratura, i volumi devono essere cifrati prima di applicare una policy di GravityZone.

Volumi di cifratura

Per cifrare i volumi:

1. Seleziona la casella **Gestione cifratura**.
2. Seleziona l'opzione **Cifra**.

Il processo di cifratura inizia subito dopo l'attivazione della policy sugli endpoint, con alcune particolarità su Windows e Mac.

Su Windows

Di norma, l'agente di sicurezza chiederà agli utenti di configurare una password per iniziare la cifratura. Se la macchina ha un TPM funzionale, l'agente di sicurezza chiederà agli utenti di configurare un numero di identificazione personale (PIN) per iniziare la cifratura. Gli utenti devono inserire la password o il PIN configurati durante questa fase ad ogni avvio dell'endpoint, in una schermata di autenticazione precedente all'avvio.

Nota
L'agente di sicurezza ti permette di configurare i requisiti di complessità del PIN e i privilegi degli utenti per la modifica del proprio PIN, tramite le impostazioni della policy di gruppo di BitLocker (GPO).

Per avviare la cifratura senza richiedere una password agli utenti dell'endpoint, attiva la casella **Se Trusted Platform Module (TPM) è attivo, non chiedere alcuna password di pre-avvio**. Questa impostazione è compatibile con gli endpoint Windows che hanno TPM e UEFI.

Quando la casella **Se il Trusted Platform Module (TPM) è attivo, non chiedere la password di pre-cifratura** è attivata:

- Sugli endpoint non cifrati:
  - La cifratura continua senza richiedere una password.

  - La schermata di autenticazione pre-avvio non compare quando si avvia la macchina.
- Su endpoint cifrati con password:
  - La password viene rimossa.
  - I volumi restano cifrati.
- Su endpoint cifrati o non cifrati senza TPM o con TPM non rilevato o non funzionale:
  - All'utente viene chiesto di inserire una password per la cifratura.
  - Quando si avvia la macchina, compare la schermata di autenticazione pre-avvio.

Quando la casella **Se il Trusted Platform Module (TPM) è attivo, non chiedere la password di pre-cifratura** è disattivata:

- L'utente deve inserire una password per la cifratura.
- I volumi restano cifrati.

Su Mac

Per avviare la cifratura sui volumi di avvio, l'agente di sicurezza chiederà agli utenti di inserire le credenziali del proprio sistema. Solo gli utenti con account locale dotati di privilegi di amministratore possono consentire la cifratura.

Per avviare la cifratura sui volumi di non-avvio, l'agente di sicurezza chiederà agli utenti di impostare una password di cifratura. Questa password sarà necessaria per sbloccare il volume di non-avvio ad ogni avvio del computer. Se il computer ha più di un volume di non-avvio, gli utenti dovranno impostare una password di cifratura per ciascuno di loro.

Decifrare i volumi

Per decifrare i volumi sugli endpoint:

1. Seleziona la casella **Gestione cifratura**.
2. Seleziona l'opzione **Decifra**.

Il processo di decifratura inizia subito dopo l'attivazione della policy sugli endpoint, con alcune particolarità su Windows e Mac.

Su Windows

I volumi sono stati decifrati senza alcuna interazione degli utenti.

Su Mac

Per i volumi di avvio, gli utenti devono inserire le proprie credenziali del sistema. Per i volumi di non-avvio, gli utenti devono inserire la password impostata durante il processo di cifratura.

Nel caso in cui gli utenti dell'endpoint dimentichino le proprie password di cifratura, avranno bisogno dei codici di recupero per sbloccare le proprie macchine. Per maggiori dettagli su come recuperare i codici di ripristino, fai riferimento a «» (p. 111).

Escludere le partizioni

Puoi creare un elenco di eccezioni alla cifratura aggiungendo le lettere di determinate unità, etichette e nomi di partizioni e GUID delle partizioni. Per creare una regola per escludere le partizioni dalla cifratura:

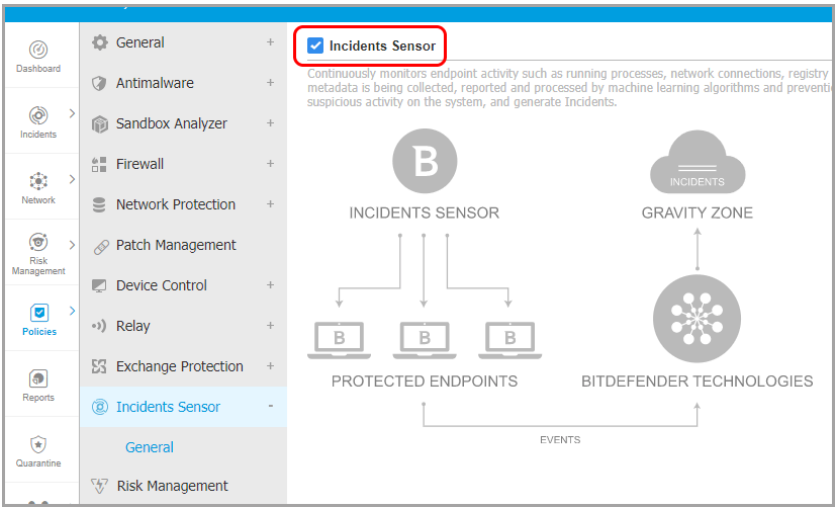
1. Seleziona la casella **Eccezioni**.
2. Clicca su **Tipo** e seleziona una tipologia di unità dal menu a discesa.
3. Inserisci un valore di un'unità nel campo **Elementi esclusi** e considera le seguenti condizioni:
   - In **Lettera dell'unità**, inserisci `D:` o la lettera della tua unità seguita da due punti.
   - Per **Etichetta/Nome** puoi inserire qualsiasi etichetta, come `Lavoro`.
   - Per una partizione **GUID**, inserisci un valore come segue: `\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\`.
4. Clicca su **Aggiungi** ⊕ per aggiungere l'eccezione all'elenco.

Per eliminare un'eccezione, scegli un elemento e clicca su **Elimina** ⊗.

7.2.11. Sensore incidenti

Il Sensore incidenti monitora costantemente le attività degli endpoint come processi in esecuzione, connessioni di rete, modifiche al registro e comportamento dell'utente. Questi metadati vengono raccolti, segnalati ed elaborati da algoritmi di apprendimento automatico e tecnologie di prevenzione, che rilevano attività sospette sul sistema, generando incidenti.

Seleziona la casella del Sensore incidenti per attivare questo modulo.



Sensore incidenti

7.2.12. Gestione rischi

Nota
Questo modulo è disponibile per:

- Windows for workstations
- Windows for servers

Il modulo Endpoint Risk Analytics ti aiuta a identificare e a correggere un vasto numero di rischi riguardanti la rete e il sistema operativo a livello di endpoint, attraverso attività di scansione dei rischi che possono essere configurate nella policy in modo da essere eseguite in modo ricorrente sugli endpoint bersaglio.

Puoi scegliere da un ampio elenco di indicatori di rischio con cui sottoporre a scansione i tuoi endpoint e determinare se sono vulnerabili. Per maggiori informazioni sugli indicatori di rischio di GravityZone, fai riferimento a questo articolo della KB.

Per configurare l'ERA:

- Seleziona la casella per attivare le funzionalità di **Gestione rischi** e avviare le policy di configurazione che definiscono come eseguire l'attività di **Scansione dei rischi**.
- **Programmazione**: stabilisce il programma di scansione dei rischi per gli endpoint bersaglio:
  1. Specifica la data e l'ora di inizio della scansione programmata dei rischi.
  2. Scegli il tipo di ricorrenza della scansione:
     - Periodica, in base a un numero specificato di ore/giorni/settimane.
     - In base al giorno della settimana.

     Importante
     Gli endpoint devono essere accesi al momento pianificato. Una scansione programmata non sarà eseguita se la macchina è spenta, in stato di ibernazione o in modalità riposo. In tali situazioni, la scansione sarà rinviata alla volta successiva.
     La scansione programmata sarà eseguita nell'ora locale dell'endpoint di destinazione. Per esempio, se la scansione programmata è impostata per avviarsi alle 18:00 e l'endpoint si trova in un fuso orario diverso della Control Center, la scansione inizierà alle 18:00 (ora dell'endpoint).

  3. Facoltativamente, puoi specificare cosa succede quando l'attività di scansione non riesce ad avviarsi al momento pianificato (endpoint offline o spento).

     Usa l'opzione **Se il periodo di esecuzione pianificato salta, esegui l'attività il prima possibile** in base alle tue esigenze:

     - Se lasci l'opzione deselezionata, verrà effettuato un nuovo tentativo di esecuzione dell'attività di scansione al momento programmato successivo.
     - Se selezioni l'opzione, forzerai l'esecuzione della scansione il prima possibile. Per impostare il momento migliore per la scansione ed evitare di disturbare l'utente durante l'orario di lavoro, seleziona **Salta se la prossima scansione pianificata inizia tra meno di**, quindi specifica l'intervallo desiderato.

Le attività di scansione dei rischi sono eseguite con tutti gli indicatori di rischio attivati per impostazione predefinita.

Una volta completata l'attività di scansione dei rischi, puoi andare alla scheda Configurazioni errate della pagina **Rischi sicurezza**, analizzarli e scegliere quali indicatori ignorare, se necessario.

Il punteggio di rischio globale dell'azienda sarà ricalcolato in base agli indicatori di rischio ignorati.

Nota
Per visualizzare l'elenco completo degli indicatori e la relativa descrizione, fai riferimento a questo articolo della KB.

8. INTERFACCIA DI MONITORAGGIO

Una corretta analisi della sicurezza della rete richiede l'accessibilità e la correlazione dei dati. Avere informazioni di sicurezza centralizzate consente di monitorare e garantire la conformità con le politiche di sicurezza dell'organizzazione, identificare rapidamente i problemi, e analizzare minacce e vulnerabilità.

La sezione di monitoraggio di GravityZone consiste in:

- **Dashboard**
- **Sintesi**

8.1. Dashboard

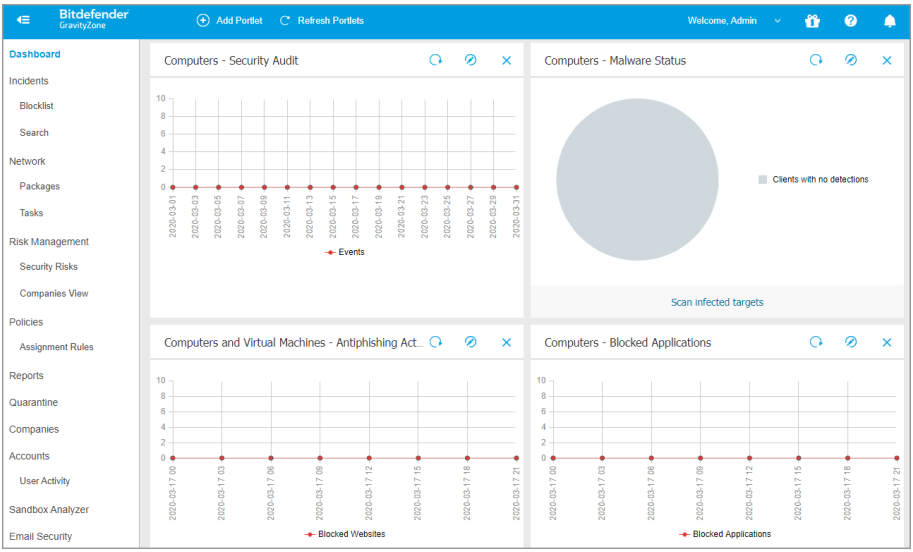
La dashboard di Control Center è una schermata personalizzabile che offre una rapida panoramica di tutti gli endpoint protetti e dello stato della rete.

Ci sono due sezioni:

- Barra della dashboard stato della rete
- Portlet dashboard

La barra di stato della rete nella dashboard ti aggiorna sul numero di incidenti aperti o in corso, le risorse minacciate (endpoint) e le minacce rilevate nella propria rete. Usa queste informazioni per scoprire eventuali elementi di rete non risolti. Clicca su **Vedi** per accedere alla pagina **Incidenti**. Per maggiori informazioni, fai riferimento a «Indagare sugli incidenti» (p. 279).

I portlet della dashboard mostrano diverse informazioni sulla sicurezza in tempo reale, utilizzando diagrammi facilmente consultabili per identificare rapidamente ogni problema che potrebbe richiedere la tua attenzione.



L'interfaccia

Ecco quello che devi sapere sui portlet della dashboard:

- Control Center ha diversi portlet predefiniti nella dashboard.
- Ogni portlet della dashboard include un rapporto dettagliato in background, accessibile con un semplice click sul diagramma.
- Ci sono diversi tipi di portlet che includono varie informazioni sulla protezione dell'endpoint, come stato di aggiornamento, stato dei malware e attività del firewall.

> **Nota**
> Di norma, i portlet recuperano i dati per il giorno attuale e, a differenza dei rapporti, non possono essere impostati per intervalli superiore a un mese.

- Le informazioni mostrate tramite portlet fanno riferimento a endpoint solo nel tuo account. Puoi personalizzare il bersaglio e le preferenze di ciascun portlet utilizzando il comando **Modifica portlet**.
- Clicca sulle voci della legenda del diagramma, se disponibili, per nascondere o mostrare la variabile corrispondente sul grafico.
- I portlet vengono mostrati in gruppi di quattro. Usa la barra di scorrimento verticale o i tasti freccia su e giù per sfogliare i diversi gruppi di portlet.

- Per gli utenti nelle aziende partner sono disponibili portlet specifici (**Stato licenza**, **Panoramica stato cliente** e **Top 10 aziende infettate**).
- Per diverse tipologie di rapporto, hai la possibilità di avviare istantaneamente determinate attività sugli endpoint di destinazione, senza dover andare alla pagina **Rete** per eseguire tale attività (per esempio, una scansione degli endpoint infetti o un aggiornamento per gli endpoint). Usa il pulsante nel lato inferiore del portlet per eseguire l'azione disponibile.

La dashboard è facile da configurare, basandosi sulle preferenze individuali. Puoi modificare le impostazioni del portlet, aggiungere altri portlet, rimuovere o riorganizzare i portlet esistenti.

8.1.1. Aggiornare i dati del portlet

Per assicurarti che il portlet mostri le informazioni più recenti, clicca sul pulsante **Aggiorna** sulla sua barra del titolo.

Per aggiornare le informazioni per tutti i portlet contemporaneamente, clicca sul pulsante **Aggiorna portlet** in cime alla dashboard.

8.1.2. Modificare le impostazioni del portlet

Alcuni portlet offrono informazioni sullo stato, mentre altri segnalano gli eventi di sicurezza avvenuti nell'ultimo periodo. Puoi controllare e configurare il periodo di segnalazione di un portlet, cliccando sull'icona **Modifica portlet** nella sua barra del titolo.

8.1.3. Aggiungere un nuovo portlet

Puoi aggiungere altri portlet per ottenere le informazioni di cui necessiti.

Per aggiungere un nuovo portlet:

1. Vai alla pagina **Dashboard**.
2. Clicca sul pulsante **Aggiungi portlet** nel lato superiore della console. Viene mostrata la finestra di configurazione.
3. Nella scheda **Dettagli**, configura i dettagli del portlet:
   - Tipo di rapporto in background
   - Nome indicativo del portlet
   - L'intervallo di tempo per gli eventi da segnalare

   Per maggiori informazioni sui tipi di rapporto disponibili, fai riferimento a «Tipo di rapporto» (p. 388).

4. Nella scheda **Bersagli**, seleziona gli elementi e i gruppi della rete da includere.
5. Clicca su **Salva**.

8.1.4. Rimuovere un portlet

Puoi rimuovere facilmente ogni portlet cliccando sull'icona ⊗ **Rimuovi** nella sua barra del titolo. Una volta rimosso un portlet, non puoi più ripristinarlo. Tuttavia, puoi creare un altro portlet con le stesse impostazioni.

8.1.5. Riorganizzare i portlet

Puoi riorganizzare i portlet della dashboard per adattarsi meglio alle tue esigenze. Per riorganizzare i portlet:

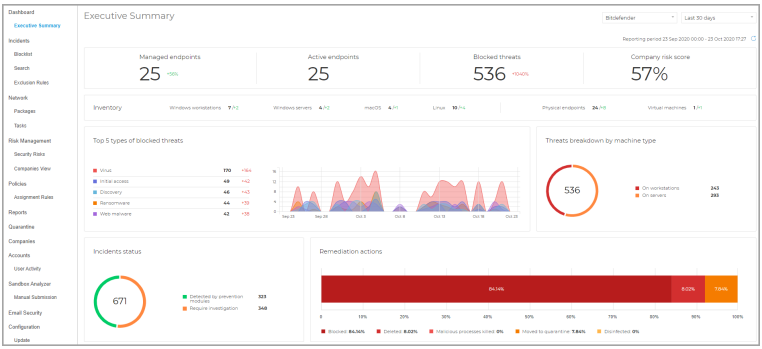
1. Vai alla pagina **Dashboard**.
2. Trascina e rilascia ciascun portlet nella posizione desiderata. Tutti gli altri portlet tra le nuove e vecchie posizioni vengono spostati per preservarne l'ordine.

> **Nota**
> Puoi spostare i portlet solo in posizioni già prese.

8.2. Sintesi

Sintesi presenta una panoramica concisa sulla sicurezza di tutti gli endpoint protetti nella rete ed è stata appositamente progettata per aiutarti a monitorare, analizzare e fornire alla gestione esecutiva dati di facile interpretazione.

Composta principalmente da widget, migliora la visibilità offrendo dettagli su moduli endpoint, rilevamenti e azioni intraprese, tipi e tecniche di minacce, punteggio di rischio della tua azienda e altri.



Sintesi

Importante

- Tutte le statistiche fornite sono basate sui dati ottenuti dopo aver attivato la funzionalità. Non sono inclusi eventi precedenti.

Le sezioni iniziali situate nella parte superiore della pagina sono:

Endpoint gestiti
Questa sezione indica tutte le macchine nella tua rete che hanno l'agente di sicurezza installato.

Endpoint attivi
Questa sezione ti informa su tutti gli endpoint che erano online nel periodo selezionato o che sono online al momento della segnalazione.

Minacce bloccate
Questa sezione presenta il numero totale di minacce bloccate identificate sui tuoi endpoint.

Inventario
Questa sezione ti fornisce dettagli sui tipo di endpoint e i loro sistemi operativi.

Punteggio di rischio azienda
In questa sezione, puoi trovare informazioni sul livello di rischio della tua azienda.

Nell'angolo in alto a destra della pagina, puoi inserire il nome di un'azienda o selezionare l'azienda di tuo interesse nel menu a discesa. Ricordati che la sintesi

fornisce statistiche per una singola azienda alla volta e non per l'intera struttura ad albero.

Puoi anche selezionare un intervallo di tempo predeterminato, relativo al momento attuale:

- **Ultime 24 ore**
- **Ultimi 7 giorni**
- **Ultimi 30 giorni**

Nota

- Tutti i dati presentati sono direttamente correlati al periodo e all'azienda selezionati.
- Per assicurarsi che la console mostri le informazioni più recenti, usa il pulsante **Aggiorna** nell'angolo in alto a destra della pagina.

In base all'intervallo selezionato, potresti notare una differenza (delta) mostrata come percentuale in alcune sezioni.

I valori del delta indicano le differenze nella tua rete che si sono verificate tra due periodi specifici:

- Il periodo precedente all'intervallo selezionato con lo stesso numero di giorni oppure ore.
- L'intervallo selezionato.

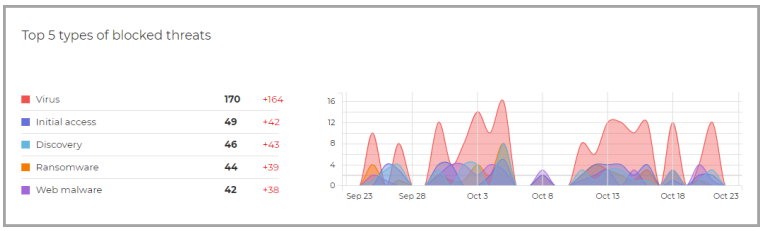
Per esempio, nell'immagine in basso, il numero totale di minacce bloccate nella tua rete è diminuito del **6%** negli **ultimi 30 giorni**. Questa percentuale è risultata dopo aver confrontato i valori dei 30 giorni precedenti l'intervallo selezionato con quelli degli ultimi 30 giorni.

Sintesi - Delta

I widget principali nella sintesi sono:

Primi 5 tipi di minacce bloccate

Il widget offre informazioni sui tipi di minacce più frequenti in base al numero di rilevamenti sugli endpoint. La colonna sulla sinistra mostra i tipi di minaccia e nella colonna di destra puoi trovare il numero di rilevamenti per ogni tipo, nonché i valori del delta.



Sintesi - I 5 principali tipi di minacce bloccate

Ripartizione delle minacce per tipo di macchina

Questo widget presenta i tipi di endpoint, workstation e server, oltre al numero di rilevamenti in ciascuno di essi.

Stato incidenti

Questo widget illustra gli incidenti di sicurezza nella rete dell'azienda.

Le categorie degli incidenti sono descritte come segue:

- **Rilevati dai moduli di prevenzione**: eventi di sicurezza identificati come minacce dai moduli di prevenzione di GravityZone.
- **Richiede indagine**: incidenti sospetti che richiedono indagini sui quali non è stata ancora intrapresa alcuna azione.

Azioni di risanamento

Questa sezione descrive le azioni che sono state intraprese sugli elementi bloccati in base alle impostazioni della policy.

Stato moduli endpoint

Fornisce una panoramica della copertura dei moduli di protezione per i tuoi endpoint. Il grafico presenta i moduli e se sono attivati, disattivati o non installati sui tuoi endpoint.

Punteggio di rischio azienda

Questo widget fornisce informazioni sul livello di rischio a cui la tua organizzazione è esposta, da impostazioni di sistema non configurate

correttamente, a vulnerabilità note delle applicazioni attualmente installate e rischi potenziali causati dall'attività e il comportamento degli utenti.

Rilevamenti basate su regole di policy

Questa sezione descrive il numero di rilevamento e il loro tipo in base alle regole personalizzate nella policy dall'amministratore.

I tipi di rilevamento includono:

- **Dispositivi bloccati**: il numero di rilevamenti basato sulle regole di **Controllo dispositivo**.
- **Connessioni bloccate**: il numero di rilevamenti basato sulle regole del **Firewall**.
- **Applicazioni bloccate**: il numero di rilevamenti basato sulle regole **Blacklist applicazioni**.
- **Siti web bloccati**: il numero di rilevamenti basato sulle regole di **Controllo accesso web**.

Siti web bloccati

Questo widget presenta il numero di rilevamenti organizzati per tipo di minaccia e identificati sui tuoi endpoint da **Protezione rete**.

Tecniche di attacco di rete bloccate

Questa sezione fornisce informazioni sulle tecniche di attacco bloccate scoperte nella tua rete.

9. INDAGARE SUGLI INCIDENTI

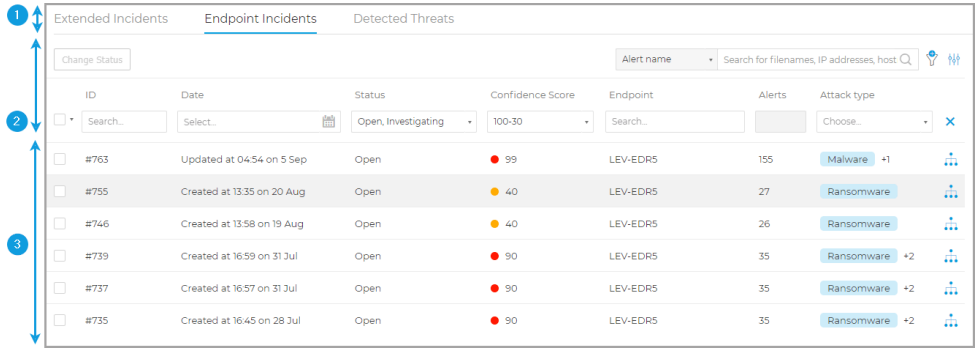
La sezione **Incidenti** aiuta a filtrare, analizzare e intraprendere azioni su tutti gli eventi di sicurezza rilevati dal Sensore incidenti in un determinato intervallo di tempo.

La sezione **Incidenti** include le seguenti pagine:

- **Incidenti**: consente di visualizzare e studiare gli eventi di sicurezza.
- **Lista bloccati**: gestisce i file bloccati coinvolti negli eventi di sicurezza.
- **Ricerca**: fornisce opzioni per analizzare il database degli eventi di sicurezza.

9.1. La pagina Incidenti

Usa la pagina **Incidenti** per filtrare e gestire gli eventi di sicurezza.



Panoramica pagina degli incidenti

Nota
La disponibilità di queste schede potrebbe differire in base alla licenza inclusa nel tuo piano attuale.

Questa pagina include le seguenti aree:

1. Una barra della finestra con schede che includono diversi tipi di incidente:
   - **Incidenti endpoint**: mostra tutti gli incidenti rilevati a livello di endpoint, che richiedono un'indagine e su cui non è ancora stata intrapresa un'azione.

- **Minacce rilevate**: mostra tutti gli eventi di sicurezza identificati come minacce dai moduli di prevenzione di GravityZone. Questi incidenti sono rilevati a livello di endpoint e vengono eseguiti con azioni predefinite nelle policy di sicurezza applicate al tuo ambiente.

2. Opzioni di filtro per personalizzare la tua griglia:
   - Clicca sul pulsante **Mostra/Nascondi colonne** per aggiungere o rimuovere colonne al filtro.

     La pagina si aggiornerà automaticamente, caricando le schede degli eventi di sicurezza con informazioni che corrispondono alle colonne aggiunte.
   - Clicca sul pulsante **Mostra/Nascondi filtri** per mostrare o nascondere la barra dei filtri.
   - Clicca sul pulsante **Cancella filtri** per reimpostare tutti i filtri.
3. La griglia Incidenti, che mostra un elenco degli eventi di sicurezza che corrispondono ai filtri applicati.

Nota
Questa funzionalità non supporta più Internet Explorer.

La barra Panoramica

La barra **Panoramica** elenca gli incidenti aperti, le principali allerte, i dispositivi interessati, oltre a molti altri dati importanti, per darti una rapida visione sulla situazione generale sulle minacce che il tuo ambiente sta affrontando.

La barra Panoramica

Nota
Disponibilità e contenuti della barra **Panoramica** potrebbero differire in base alla licenza inclusa nel tuo piano attuale.

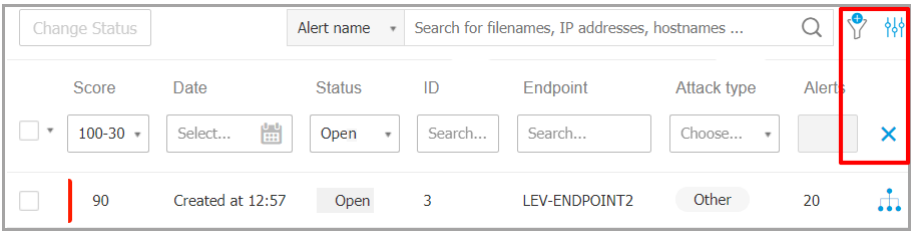
Filtrare gli incidenti dalla barra Panoramica

Puoi filtrare l'elenco degli incidenti selezionando i valori nella barra Panoramica:

- Cliccando su un valore nella sezione **INCIDENTI APERTI**, sarà possibile mostrare solo gli incidenti con il livello di severità selezionato.
- Cliccando su un valore nella sezione **ALLERTE PRINCIPALI**, si inserirà nel campo di ricerca il nome dell'allerta e saranno mostrati solo gli incidenti in cui l'allerta è stata rilevata.
- Cliccando su un valore nella sezione **TECNICHE PRINCIPALI**, si inserirà nel campo di ricerca il nome della tecnica e saranno mostrati solo gli incidenti in cui la tecnica è stata rilevata.
- Cliccando su un valore nella sezione **PRINCIPALI DISPOSITIVI INTERESSATI**, saranno mostrati solo gli incidenti che interessano il dispositivo selezionato.

9.1.1. La griglia dei filtri

La pagina **Incidenti** ti consente di scegliere quali incidenti mostrare personalizzando la griglia dei filtri.



La griglia dei filtri

- Clicca sul pulsante **Mostra/Nascondi colonne** per aggiungere o rimuovere colonne al filtro.

  La pagina si aggiornerà automaticamente, caricando le schede degli eventi di sicurezza con informazioni che corrispondono alle colonne aggiunte.
- Clicca sul pulsante **Mostra/Nascondi filtri** per mostrare o nascondere la barra dei filtri.
- Clicca sul pulsante **Cancella filtri** per reimpostare tutti i filtri.

Puoi trovare maggiori dettagli sulle opzioni di filtraggio disponibili nella seguente tabella:

Opzioni di filtro	Dettagli
Punteggio	Il punteggio di sicurezza è un numero tra 100 e 10, che indica il potenziale livello di pericolosità di un evento di sicurezza. Maggiore è il punteggio, più l'evento è pericoloso con maggiore certezza. Indica il contesto in base agli indicatori di attacco e alle tecniche di attacco, se applicabili. Per filtrare in base al punteggio di sicurezza, trascina la barra di scorrimento fino ai valori desiderati. In alternativa, puoi usare il campo numerico sotto la barra. Clicca su **OK** per confermare la selezione del punteggio.
Data	Per filtrare in base alla data: 1. Clicca sull'icona del calendario o il campo **Data** per aprire la pagina di configurazione della data. 2. Seleziona l'intervallo di tempo quando si è verificato l'incidente: • Clicca sulle schede **Da** e **A** per selezionare le date che definiscono l'intervallo di tempo. **Nota** Puoi indicare il momento esatto per le date di inizio e fine, usando i campi ore e minuti sotto il calendario. • Puoi anche selezionare un intervallo di tempo predeterminato, relativo al momento attuale (gli ultimi 7 giorni. Per ulteriore spazio di archiviazione per gli eventi devi contattare il tuo rappresentante vendite per fare l'upgrade della soluzione con un add-on **Conservazione dati** di 30, 90 o 180 giorni. 3. Clicca su **OK** per applicare il filtro.
Stato	Filtra gli incidenti in base al proprio stato attuale selezionando una o più opzioni di stato, disponibili nel menu a discesa **Stato**: • **Apri**: per gli eventi di sicurezza non analizzati • **In corso di indagine**: per gli eventi di sicurezza sotto indagine.

Opzioni di filtro	Dettagli
	• **Falso positivo**: per gli eventi di sicurezza etichettati come falso allarme • **Chiusi**: per gli eventi di sicurezza con un'indagine chiusa.
ID	Riduci l'elenco degli incidenti cercando un numero ID specifico dell'evento di sicurezza.
Azienda	Filtra gli incidenti in base al nome dell'azienda in cui sono stati attivati gli eventi di sicurezza. Di norma, la pagina **Incidenti** mostra gli incidenti di tutte le aziende sotto la tua gestione. **Nota** Nell'elenco compariranno solo le aziende sotto la tua gestione con una licenza EDR valida.
Endpoint	Riduci l'elenco degli incidenti cercando un determinato nome dell'endpoint dalla tua rete gestita.
Tipo di attacco	Il tipo di attacco è un elenco dinamico dei tipi più comuni di attacco, che cambia in base agli indicatori di attacco presenti negli eventi di sicurezza elencati.
Avvisi	La colonna **Allerte** mostra il numero di allerte attivate per incidente.
SO endpoint	Questa opzione filtra gli eventi di sicurezza in base al sistema operativo degli endpoint coinvolti.

Nota
Le opzioni di filtro potrebbero variare in base al tipo di codice di licenza incluso nel tuo piano attuale.

Per cercare altri elementi non visibili nella griglia del filtro, selezionare una delle opzioni di ricerca dal menu a discesa **Cerca**:

- **Nome dell'allerta** - da 3 a 1.000 caratteri al massimo.
- **Tecnica ATT&CK** - 100 caratteri al massimo.
- **IP endpoint** - 45 caratteri al massimo.

- **MD5** - 32 caratteri al massimo.
- **SHA256** - 64 caratteri al massimo.
- **Nome del nodo** - 360 caratteri al massimo.
- **Nome utente** - 1.000 caratteri al massimo.

La pagina si aggiornerà automaticamente, caricando solo le schede degli eventi di sicurezza che corrispondono all'elemento cercato. Per una ricerca più granulare, puoi creare delle query di ricerca nella Pagina di ricerca.

9.1.2. Visualizzare la lista degli eventi di sicurezza

La pagina **Incidenti** mostra un elenco di eventi di sicurezza che corrispondono ai filtri selezionati.

Di norma, ci sono 20 eventi per pagina, raccolti per data. La pagina si aggiorna automaticamente a intervalli regolari, mentre l'EDR attiva nuovi eventi.

Importante
Tutti gli eventi di sicurezza più vecchi di 90 giorni vengono automaticamente eliminati dalla sezione **Incidenti endpoint** e dalla sezione **Minacce rilevate**, oltre che dall'archivio degli eventi di sicurezza.

Per navigare nella pagina, usa i tasti di direzione o la rotellina del mouse oppure clicca la barra di scorrimento. Cambia il numero di eventi mostrati in fondo alla pagina. Puoi avere fino a 100 eventi per pagina.

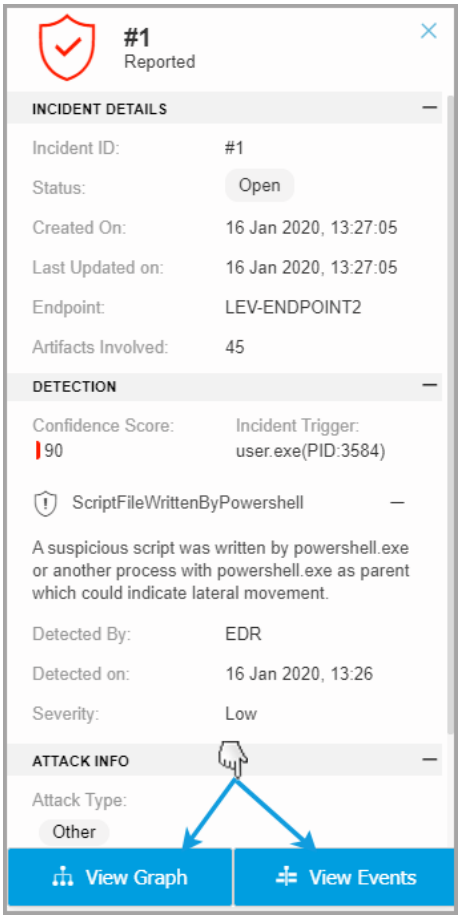
Ogni voce dell'evento di sicurezza è elencata in un formato rich card e fornisce una panoramica di ciascun incidente, con informazioni basate sui filtri selezionati.

Nota
Controlla il colore del bordo sinistro per valutare rapidamente il livello di confidenza (basso, medio o alto).

Scheda evento di sicurezza

- Cliccando sul pulsante **Vedi grafico** corrispondente della scheda di un evento di sicurezza, potrai aprirlo in una nuova pagina, dove potrai analizzare l'incidente in dettaglio e intraprendere le azioni appropriate.

- Cliccando sulla scheda di un evento di sicurezza, si aprirà un pannello di visualizzazione rapida laterale con informazioni sull'incidente selezionato.



Visuale rapida dei dettagli dell'incidente

- Clicca sul pulsante **Vedi grafico** per accedere alla visualizzazione grafica dell'incidente.
- Clicca sul pulsante **Vedi eventi** per accedere alla cronologia dell'incidente.

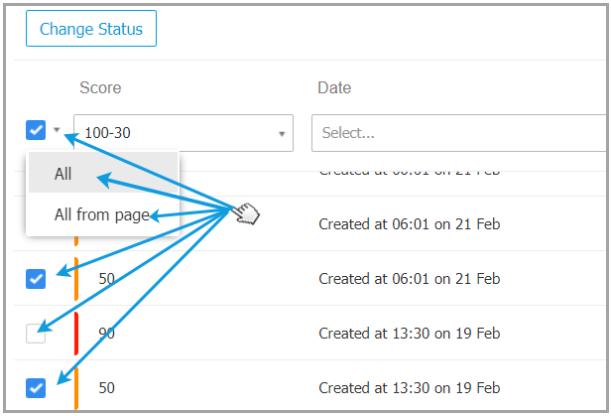
- Selezionando la casella della scheda di un qualsiasi evento di sicurezza, si attiverà il pulsante **Cambia stato**, che ti consentirà di modificare lo stato attuale dell'incidente.

Modificare lo stato degli eventi di sicurezza

Lo stato dell'indagine ti aiuta a tenere traccia degli incidenti che sono già stati analizzati e marcati come chiusi o falsi positivi, degli incidenti che sono attualmente sotto indagine, e dei nuovi incidenti o quelli aperti che devono ancora essere analizzati.

Puoi scegliere di modificare lo stato di uno o più eventi di sicurezza alla volta:

1. Seleziona le caselle delle schede dell'evento di sicurezza che subiranno un cambiamento di stato.

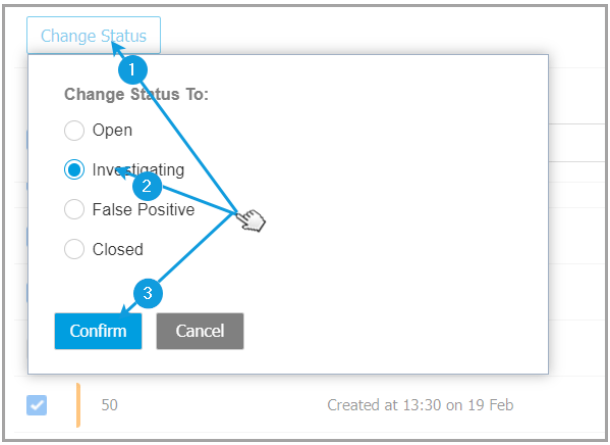


Selezionare le schede degli eventi di sicurezza

Puoi selezionarle individualmente usando le opzioni di selezione in blocco nel menu a discesa.

Nota
Puoi anche scorrere tra le pagine di diversi eventi di sicurezza mantenendo la tua selezione.

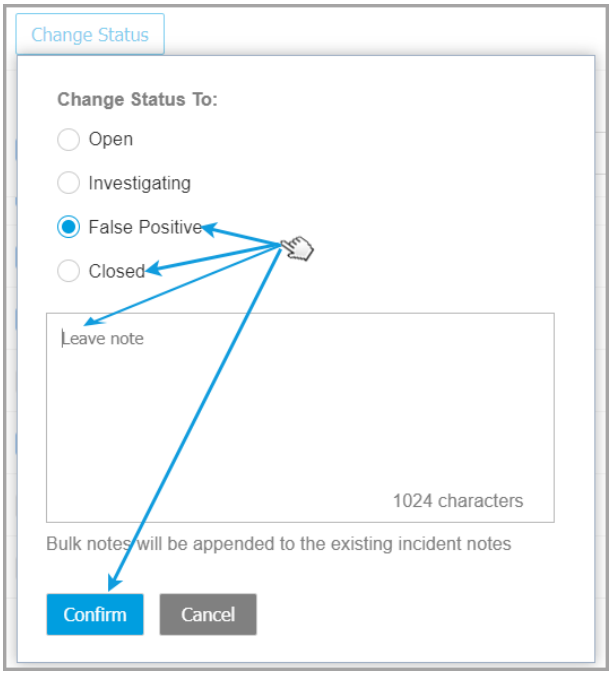
2. Clicca sul pulsante **Cambia stato** e seleziona le opzioni desiderate:



Modificare lo stato dell'evento di sicurezza

- **Aperto** - Quando l'evento di sicurezza non è ancora sotto indagine.
- **Indagine in corso**- quando hai iniziato a indagare sull'evento.
- **Falso positivo** - quando hai analizzato l'evento, identificandolo come un falso positivo.
- **Chiusa**- quando hai completato l'indagine.

Nota
Quando si modifica lo stato degli eventi in **Falso positivo** o **Chiuso** si aprirà una finestra, dove potrai lasciare una nota sulle motivazioni del cambio di stato dell'evento, per eventuali consultazioni successive.



Lasciare una nota per gli eventi indicati come chiusi o falsi positivi

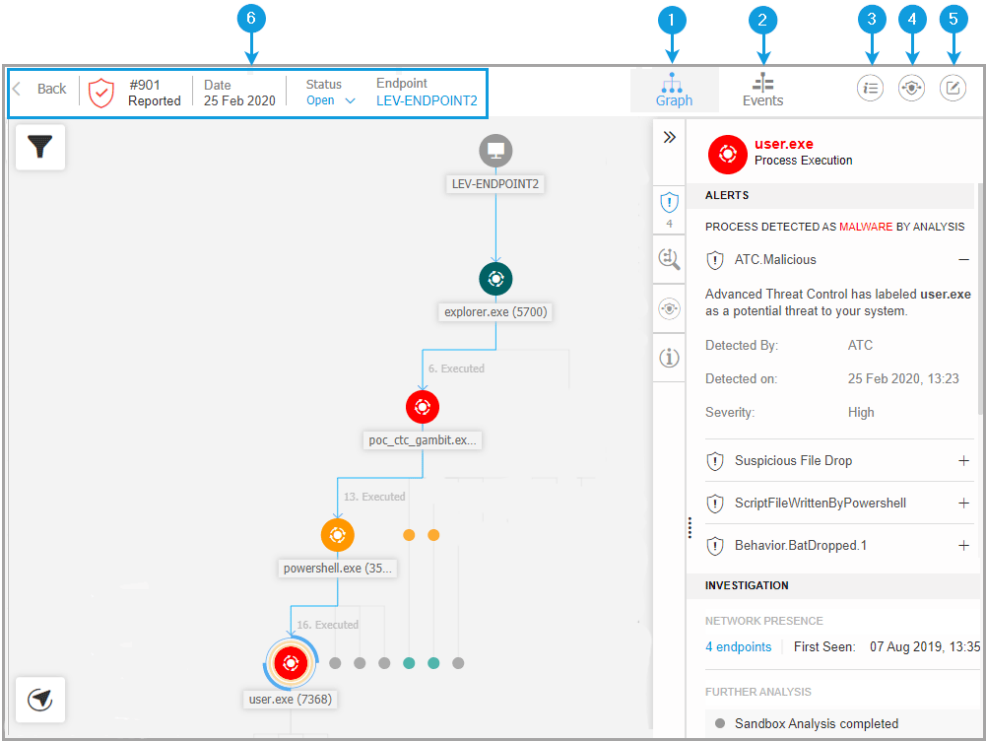
Nota
La nota sarà aggiunta a quelle già esistenti all'interno degli incidenti filtrati.

3. Clicca su **Conferma** per applicare l'opzione di stato selezionata.

9.1.3. Indagare un incidente degli endpoint

Nella pagina **Incidenti**, identifica l'evento di sicurezza che vuoi analizzare e clicca sul pulsante **Vedi grafico** per mostrarlo in una nuova pagina.

Ogni incidente di sicurezza ha una pagina dedicata contenente informazioni dettagliate sulla sequenza degli eventi (visualizzata nel grafico come nodi di eventi di sicurezza collegati) che hanno portato all'attivazione dell'incidente e offre opzioni per eseguire azioni correttive.


6
1
2
3
4
5
Back
#901
Reported
Date
25 Feb 2020
Status
Open
Endpoint
LEV-ENDPOINT2
Graph
Events
LEV-ENDPOINT2
explorer.exe (5700)
6. Executed
poc_ctc_gambit.ex...
13. Executed
powershell.exe (35...
16. Executed
user.exe (7368)
user.exe
Process Execution
ALERTS
PROCESS DETECTED AS MALWARE BY ANALYSIS
ATC.Malicious
Advanced Threat Control has labeled user.exe as a potential threat to your system.
Detected By: ATC
Detected on: 25 Feb 2020, 13:23
Severity: High
Suspicious File Drop
ScriptFileWrittenByPowershell
Behavior.BatDropped.1
INVESTIGATION
NETWORK PRESENCE
4 endpoints
First Seen: 07 Aug 2019, 13:35
FURTHER ANALYSIS
Sandbox Analysis completed

1. Scheda Grafico

   Il grafico mostra l'incidente di sicurezza e i suoi elementi costitutivi, evidenziando il percorso critico dell'incidente e mostrando i dettagli del nodo che ha attivato l'incidente nel pannello **Dettagli nodo**.

2. Scheda Eventi

   La scheda Eventi visualizza eventi e avvisi di sistema rilevati filtrabili, e le relative descrizioni degli eventi.

3. Pannello Informazioni incidente

   Questo pannello include sezioni comprimibili con dettagli come ID incidente, stato attuale, data e ora di creazione e aggiornamento per l'ultima volta, numero di elementi coinvolti, nome del trigger e informazioni sull'attacco.

4. Pannello Riparazione

   Questo pannello include sezioni flessibili con le azioni intraprese automaticamente da GravityZone e i passaggi suggeriti da seguire per contenere l'incidente.

5. Note negli appunti

   Cliccando sul pulsante **Note** si apre un blocco degli appunti in cui è possibile aggiungere note sull'incidente attuale, che sarà possibile leggere quando si rivedrà l'incidente in un secondo momento.

6. Barra stato incidente

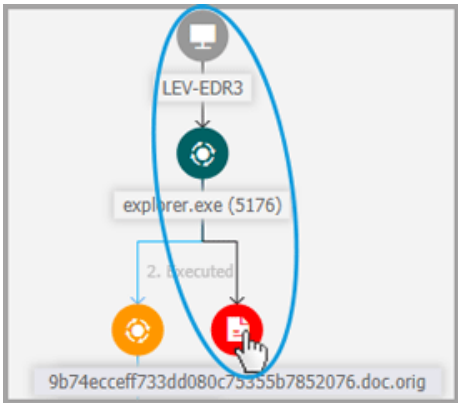
   La barra dello stato offre dettagli sull'ID dell'incidente, la data e l'ora in cui è stato generato, lo stato, il trigger dell'incidente e l'endpoint coinvolto. Cliccando sul pulsante **Indietro** tornerai alla pagina principale **Incidenti**.

Nodi eventi di sicurezza

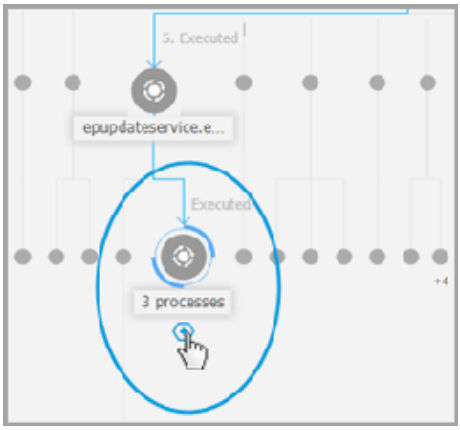
Questo è ciò che devi sapere sui nodi degli eventi di sicurezza:

- Ogni nodo rappresenta un determinato elemento coinvolto nell'incidente analizzato.
- Tutti i nodi che compongono il percorso critico vengono mostrati con più dettagli per impostazione predefinita quando si apre l'incidente, mentre gli altri elementi vengono sbiaditi, per evitare di ingombrare la vista.

– Passando il mouse su un nodo che non fa parte del percorso critico lo evidenzierai, mostrando il percorso per il punto di origine, senza interrompere il Percorso critico.



- Tre o più nodi dello stesso tipo di evento generati da un nodo parentale vengono raggruppati in un nodo cluster espandibile.



– Solo i nodi senza elementi figlio saranno nascosti nel grafico dell'incidente quando il nodo cluster viene eliminato.

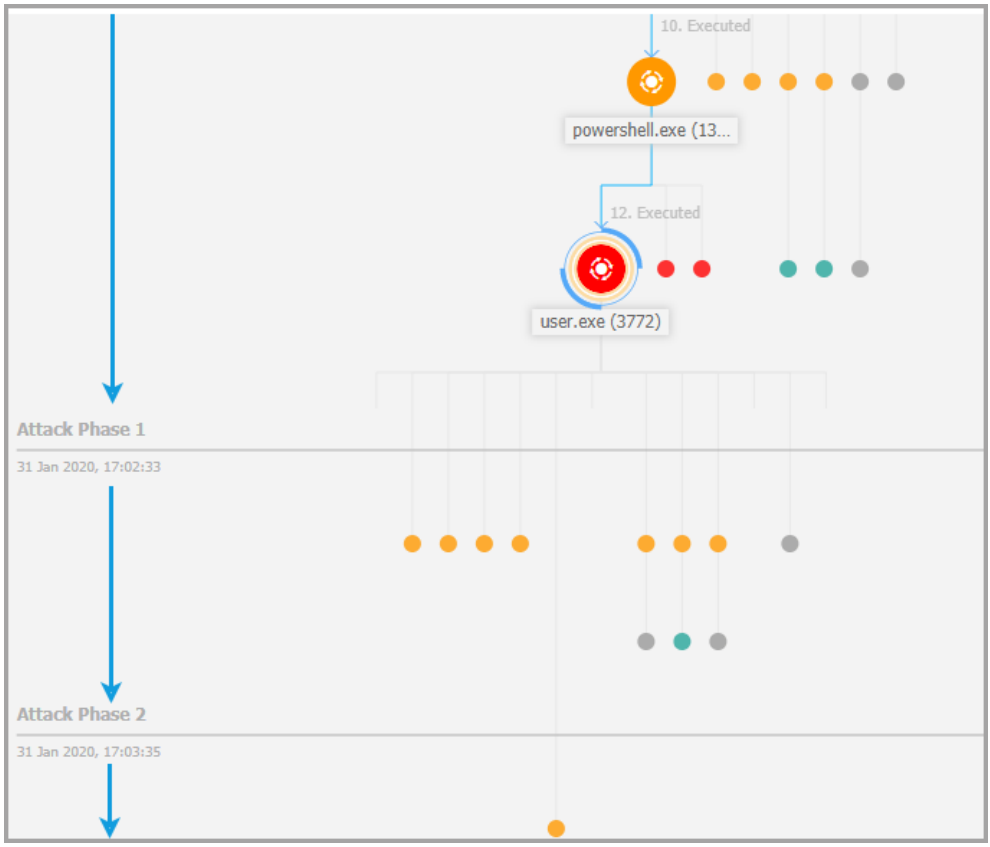
  - I nodi in cui è stata rilevata un'attività sospetta non saranno aggiunti al nodo del cluster.
- Cliccando su un nodo, saranno mostrati i seguenti dettagli:
  - Evidenzierà in blu il percorso per il nodo dell'endpoint insieme a tutti gli altri elementi coinvolti.
  - Un pannello laterale con sezioni espandibili che forniscono informazioni dettagliate sul nodo selezionato, avvisi nel caso in cui vengano evidenziati rilevamenti, le azioni disponibili ed eventuali suggerimenti. Fai riferimento a «Dettagli nodo» (p. 303) per maggiori informazioni.
- I nodi sono collegati da linee di freccia che indicano il corso delle azioni che si sono verificate sull'endpoint durante l'incidente. Ogni linea è indicata con il nome dell'azione e il suo numero cronologico.

I seguenti elementi di un incidente possono essere rappresentati come nodi:

Tipo di nodo	Descrizione
Endpoint	Mostra i dettagli dell'endpoint e lo stato della gestione delle patch.
Dominio	Mostra informazioni sull'host del dominio e i relativi endpoint.
Processo	Mostra i dettagli sul ruolo del processo nell'incidente attuale, informazioni sui file, dettagli sulle esecuzioni dei processi, la presenza di rete e ulteriori opzioni dell'indagine.
File	Mostra dettagli sul ruolo del file nell'incidente attuale, le informazioni dei file, la presenza di rete e ulteriori opzioni dell'indagine.
Registro	Mostra informazioni del registro e dettagli sul processo parentale.

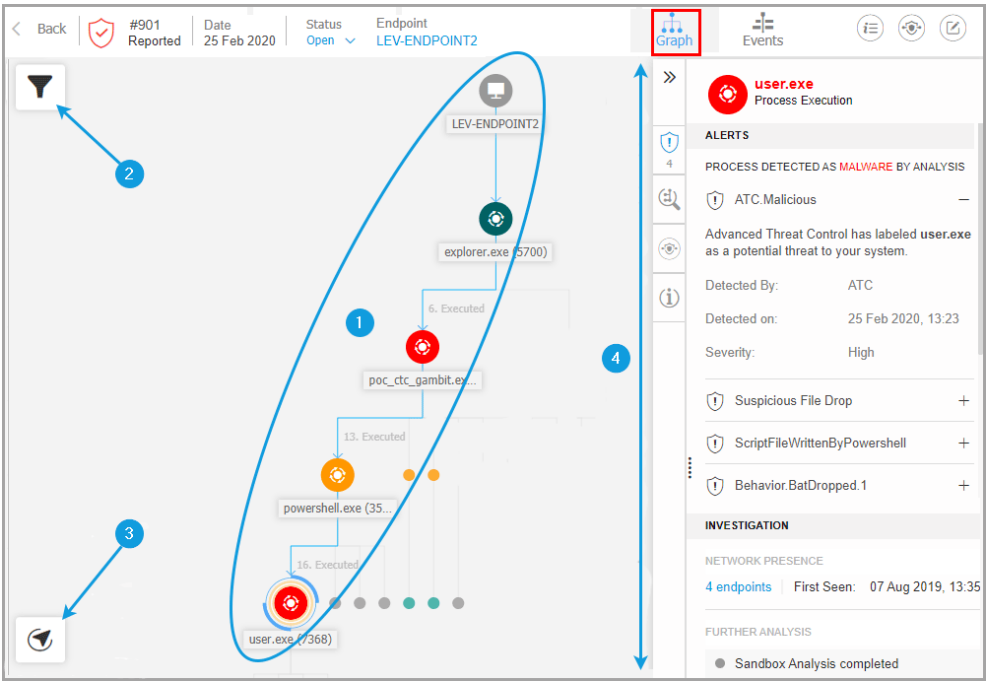
Grafico

Il **Grafico** fornisce una rappresentazione grafica interattiva dell'incidente indagato e il suo contesto, evidenziando la sequenza di elementi direttamente coinvolti nell'attivazione, nota come **Percorso critico** dell'incidente, oltre a tutti gli altri elementi coinvolti, che sono sbiaditi per impostazione predefinita. In caso di incidenti complessi che si evolvono nel tempo, il grafico mostra ogni singola fase dell'attacco.



Attacco organizzato

Il grafico include opzioni di filtraggio che consentono una personalizzazione grafica dell'incidente per migliorarne la visualizzazione, oltre a funzionalità per esplorare la mappa dell'incidente e pannelli di dettagli con maggiori informazioni su ciascun elemento.



La scheda Grafico

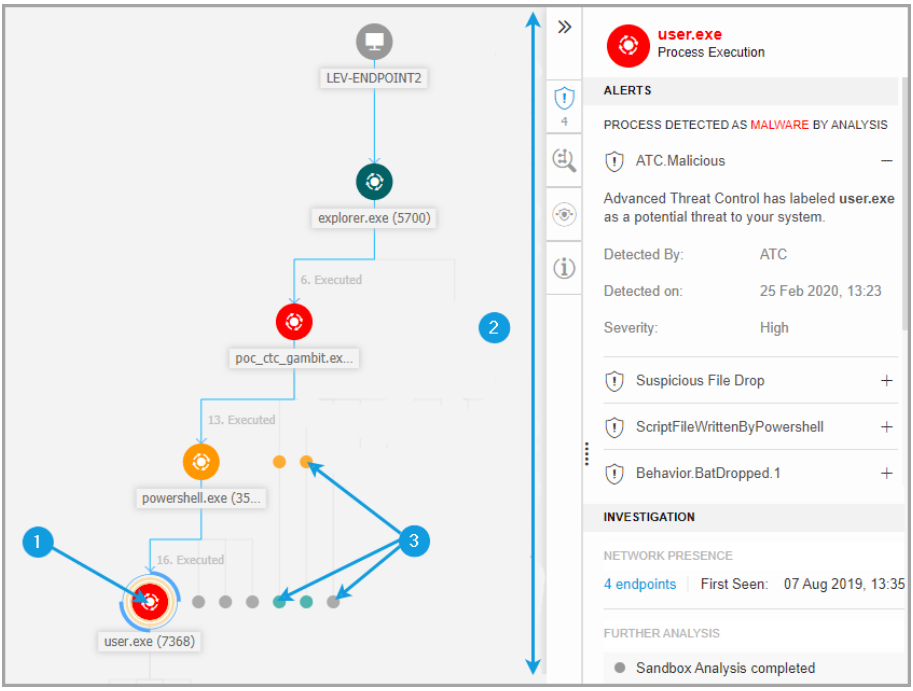
1. Percorso critico
2. Menu Filtri
3. Menu navigatore
4. Pannello dettagli nodo

Percorso critico

Il **Percorso critico** è la sequenza degli eventi di sicurezza collegati che hanno portato alla creazione di un'allerta, a partire dal punto di ingresso nella rete fino al nodo dell'evento che ha causato l'incidente. Il percorso critico dell'incidente è evidenziato per impostazione predefinita nel grafico, con tutti i nodi degli eventi consistenti su di esso, mentre gli altri elementi saranno minimizzati.

Il nodo del trigger si distingue facilmente dal resto degli elementi nel grafico, essendo circondato da funzionalità di evidenziazione aggiuntive (due cerchi

arancioni). Inoltre, viene visualizzato un pannello informativo correlato per impostazione predefinita accanto al grafico dell'incidente, che fornisce informazioni dettagliate sul nodo del trigger.



Percorso critico

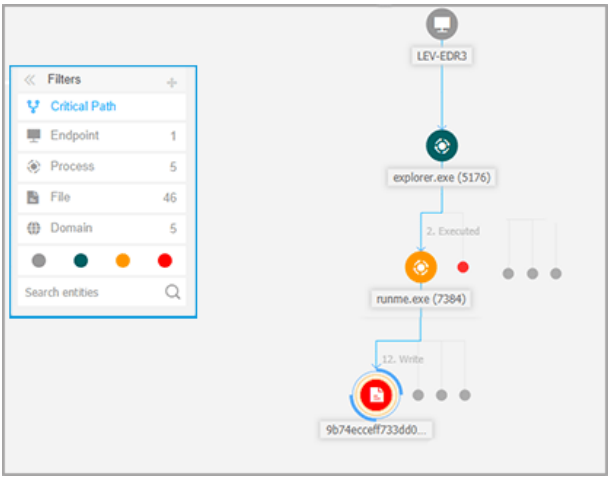
1. Nodo del trigger
2. Il pannello Dettagli nodo con informazioni raggruppate in categorie e sezioni a scomparsa
3. I nodi sbiaditi indirettamente coinvolti nell'incidente

Nota
Cliccando su un altro elemento rispetto al nodo del trigger si interromperà il percorso critico, evidenziando il percorso per l'origine, dal nodo selezionato a monte al nodo dell'endpoint.

Filtri

Il menu **Filtri** offre funzionalità di filtro avanzate, che consentono la completa manipolazione del grafico dell'incidente, evidenziando gli elementi in base al loro tipo o rilevanza, o nascondendoli per rendere l'incidente più compatto e facile da analizzare.

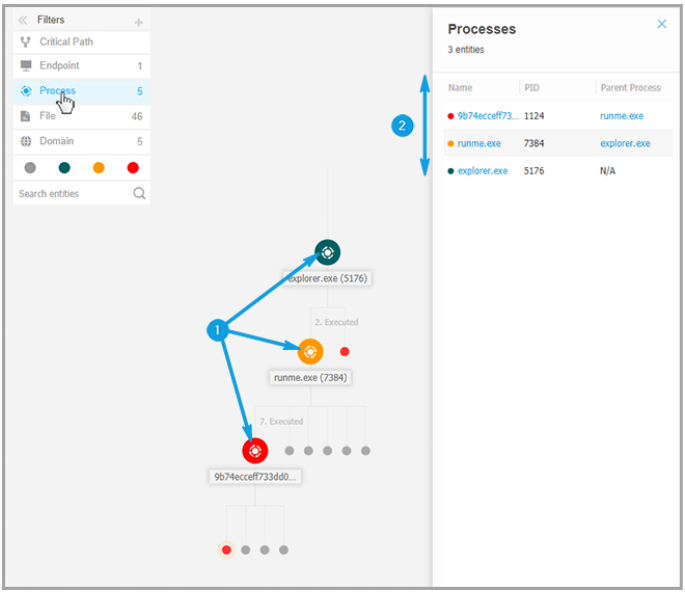
Clicca e tieni premuto sull'icona **Trascina** per posizionare il pannello Filtri in qualsiasi punto del grafico dell'incidente.



Filtri grafico incidente

Quando si seleziona un filtro di tipo elemento:

1. Il grafico dell'incidente si rimpicciolisce ed evidenzia tutti gli elementi del tipo selezionato, mentre gli elementi di un altro tipo vengono sbiaditi.
2. Apre istantaneamente un pannello con l'elenco di tutti gli elementi evidenziati.



Nota
Selezionando un elemento dall'elenco visualizzato lo evidenzierai nel grafico dell'incidente, aprendo anche un pannello con informazioni relativi a quell'elemento. Può essere applicato solo un filtro alla volta.

Le opzioni di filtro includono:

- **Percorso critico**: evidenzia il percorso critico dell'incidente di compromissione.
- **Endpoint**: evidenzia gli endpoint coinvolti dall'incidente.
- **Processo**: evidenzia tutti i nodi di tipo processo coinvolti nell'incidenti.
- **File**: evidenzia i nodi di tipo file coinvolti nell'incidente.
- **Dominio**: evidenzia tutti i nodi di tipo dominio coinvolti nell'incidente.
- **Registro**: evidenzia tutti i nodi di tipo registro coinvolti nell'incidente.

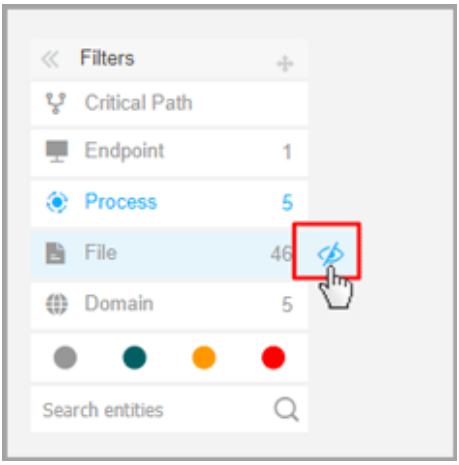
- **Rilevanza degli elementi**: è possibile anche filtrare gli elementi per la loro importanza nell'incidente.
  - **Nodo neutrale**: elementi senza alcun impatto diretto nell'incidente di sicurezza.
  - **Nodo importante**: elementi con un ruolo importante nell'incidente di sicurezza.
  - **Nodo di origine**: il punto di ingresso dell'attacco all'interno della rete.
  - **Nodo sospetto**: elementi con un comportamento sospetto, direttamente coinvolti nell'incidente di sicurezza.
  - **Nodo dannoso**: elementi che hanno causato danni nella tua rete.

    Nota
    Passando il mouse su uno dei filtri colorati viene visualizzato il numero di elementi con la stessa rilevanza coinvolti nell'incidente.

- **Ricerca entità**: è possibile cercare nomi o estensioni di file dei componenti degli incidenti nel campo di ricerca e i risultati saranno visualizzati nel pannello laterale.

Se non viene selezionato alcun filtro, il grafico dell'incidente viene ripristinato al suo stato predefinito, con endpoint, origine ed elementi trigger evidenziati, mentre gli altri elementi vengono sbiaditi.

Puoi anche nascondere determinati elementi dal grafico dell'incidente cliccando sul pulsante **Mostra/Nascondi** posizionando il mouse sul filtro del tipo: File, Dominio e Registro.



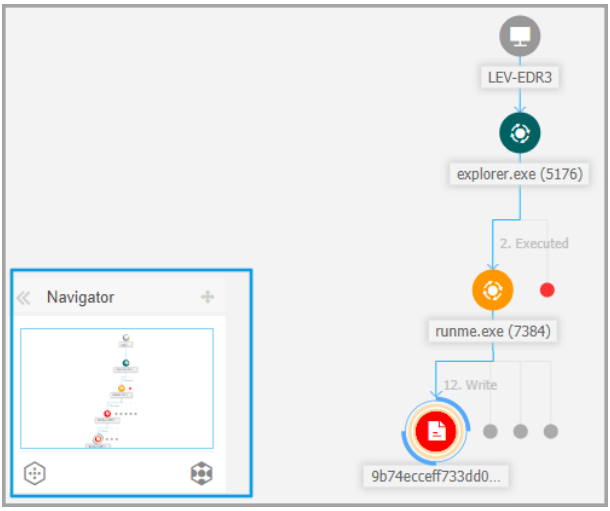
Nascondere un tipo di elemento ridisegna il grafico dell'incidente rimuovendo tutti gli elementi corrispondenti, anche se vengono ingranditi, ad eccezione del nodo trigger e dei nodi con elementi figli.

Navigatore

Il **Navigatore** ti consente di spostarti rapidamente attraverso il grafico dell'incidente ed esplorare tutti gli elementi visualizzati usando la mini-mappa e i diversi livelli di visualizzazione.

Clicca e tieni premuto sull'icona ✣ **Trascina** per posizionare il pannello Navigatore mobile ovunque all'interno del grafico dell'incidente.

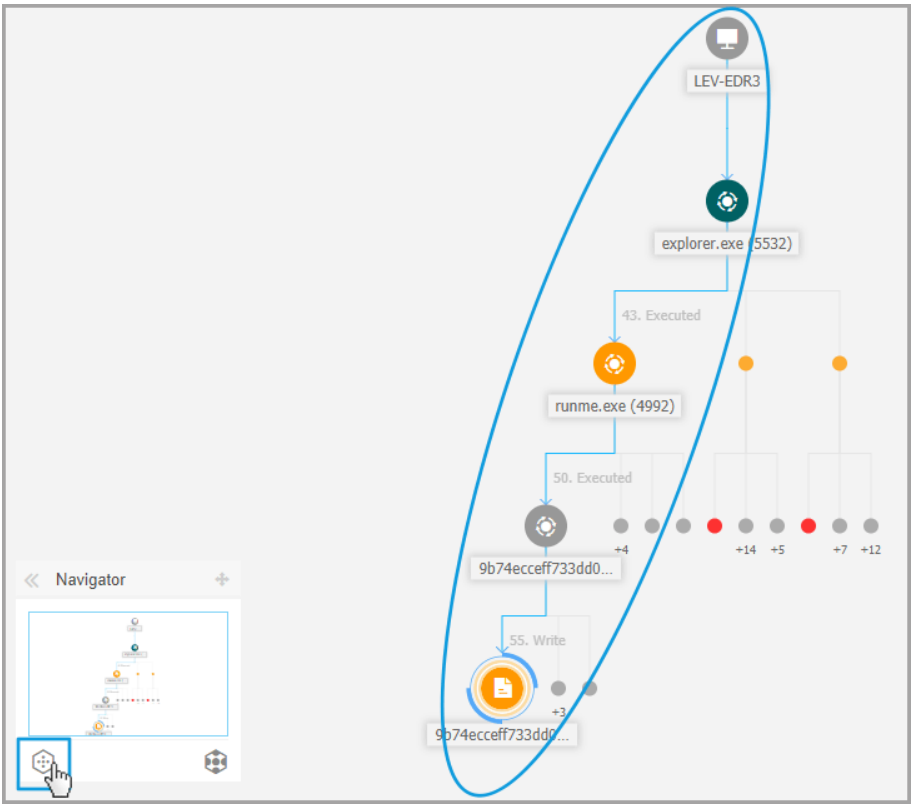
Il **Navigatore** non è selezionato in maniera predefinita. Espandendolo, il menu mostrerà la versione miniaturizzata dell'intera mappa dell'incidente, e i pulsanti azione per regolare il livello di visualizzazione.



Navigatore

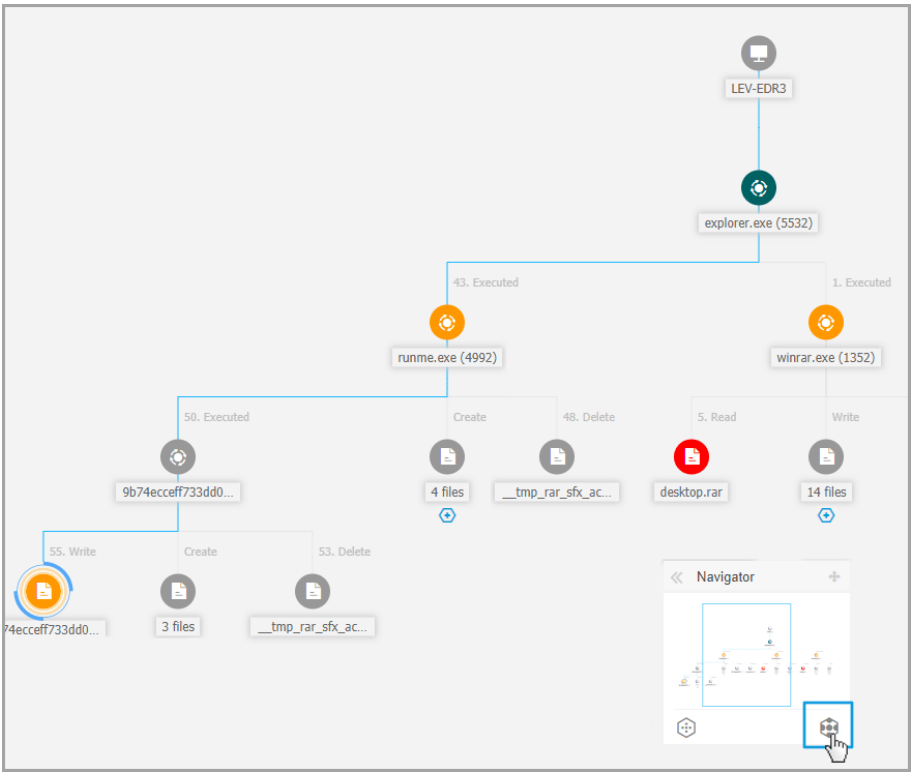
Il menu **Navigatore** fornisce due pulsanti azione per regolare il modo di visualizzare il grafico dell'incidente: il pulsante **Meno dettagli** e il pulsante **Più dettagli**

Cliccando sul pulsante **Meno dettagli**, il grafico viene impostato nel suo stato predefinito, evidenziando solo il percorso critico dell'incidente.



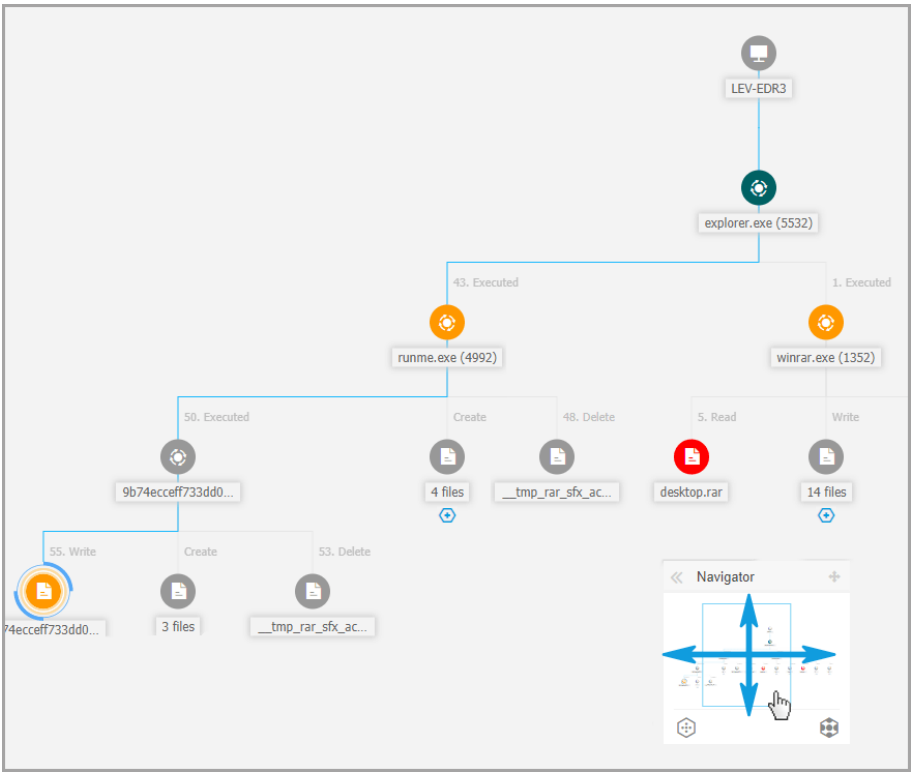
Visualizzazione panoramica

Cliccando sul pulsante **Più dettagli**, tutti gli elementi del grafico dell'incidente vengono espansi, evidenziando ogni nodo e cluster dei nodi.



Visualizzazione ingrandita

Quando l'incidente viene ingrandito e tutti gli elementi vengono evidenziati, il grafico potrebbe spesso espandersi oltre i limiti dello schermo. In questo caso, tieni premuto e trascina il selettore della mappa nella mini-mappa del Navigatore per scorrere facilmente all'area della mappa dell'incidente desiderata, o trascina semplicemente l'area del grafico nella direzione desiderata.

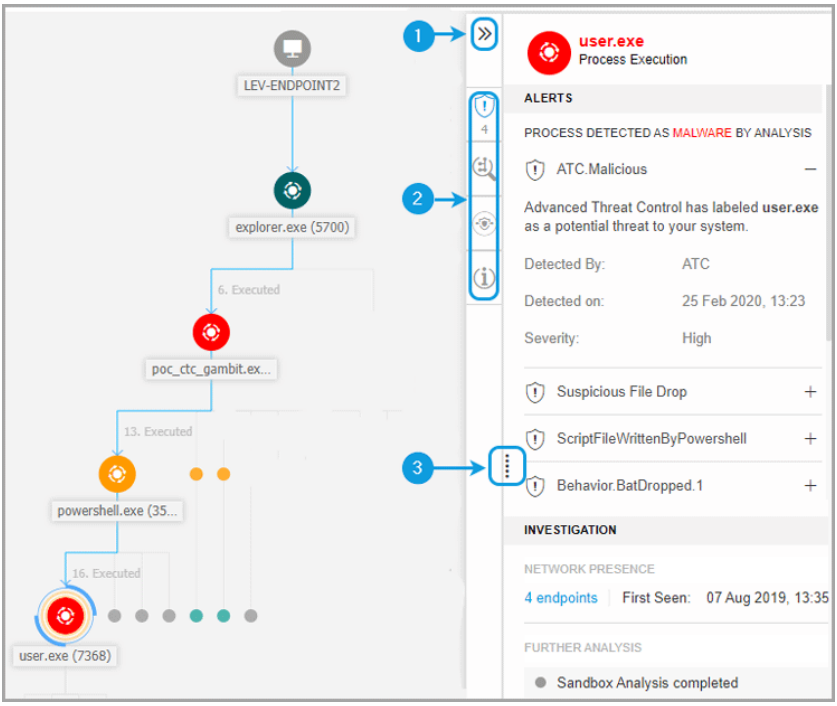


Selettore mini-mappa

Dettagli nodo

Il pannello **Dettagli nodo** include sezioni con informazioni dettagliate sul nodo selezionato, tra cui azioni preventive o di risanamento da poter intraprendere per contenere l'incidente, dettagli sul tipo di rilevamento e le allerte rilevate sul nodo, presenza della rete, dettagli sull'esecuzione dei processi, ulteriori suggerimenti per gestire l'evento di sicurezza, o azioni per esaminare ulteriormente l'elemento.

Per visualizzare queste informazioni e intraprendere azioni all'interno del pannello, seleziona un nodo nella mappa dell'evento di sicurezza.



Pannello dettagli nodo

1. Puoi ridurre o espandere il pannello **Dettagli nodo** cliccando sul pulsante **Comprimi**.
2. Puoi facilmente esplorare le informazioni mostrate nel pannello **Dettagli nodo**, cliccando sulle icone di ciascuna delle quattro categorie principali:
   - **ALLERTE**

     Questa sezione mostra uno o più rilevamenti attivati sul nodo selezionato, incluso dettagli sulla tecnologia di Bitdefender che ha incluso l'elemento nell'incidente, il motivo che ha attivato il rilevamento, il nome del rilevamento, il tipo e la famiglia di malware, e la data del rilevamento.
   - **INDAGINE**

     Questa sezione mostra gli indicatori della data per il rilevamento iniziale e tutti gli endpoint in cui è stato individuato questo elemento.

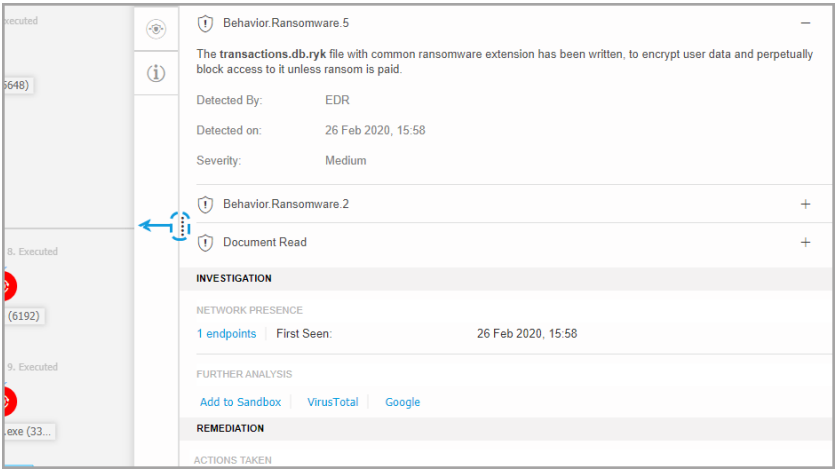
- **RIMEDIO**

  Questa sezione mostra le azioni intraprese automaticamente da GravityZone, azioni che puoi effettuare subito per ridurre l'impatto della minaccia, oltre a suggerimenti dettagliati per ciascuna allerta rilevata nel nodo selezionato per assisterti nella mitigazione dell'incidente e aumentare il livello di sicurezza del tuo ambiente.

- **INFO**

  Questa sezione mostra informazioni generali su ciascun file e informazioni più specifiche in base al tipo di nodo selezionato.

3. Puoi trascinare il pannello **Dettagli nodo** verso il centro della schermata per visualizzarne facilmente i contenuti.



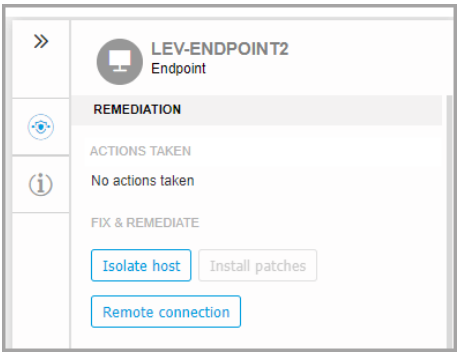
Pannello esteso

Pannello dei dettagli per i nodi dell'endpoint

Il pannello **Dettagli nodo** per gli endpoint include due categorie:

- **RIMEDIO**

  Mostra informazioni sulle azioni intraprese automaticamente da GravityZone per mitigare le minacce, e le azioni che puoi intraprendere:

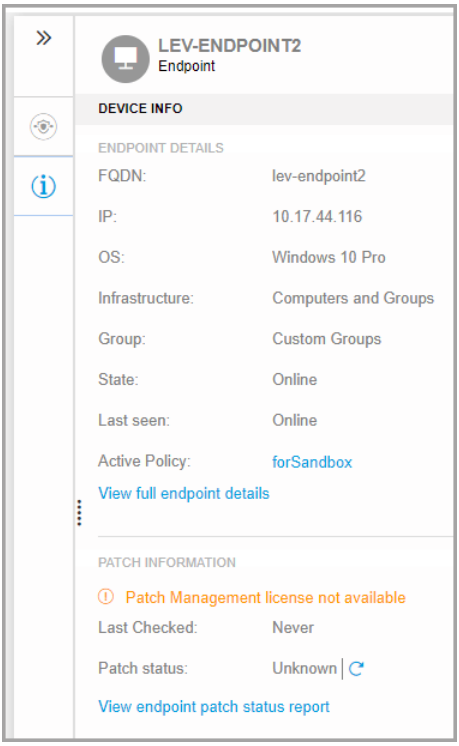


- **Isola host** - Usa questa soluzione di riparazione per isolare l'endpoint dalla rete.
- **Installa patch** - Usa questa azione per installare una patch di sicurezza mancante nell'endpoint bersaglio. Questa opzione risulta disponibile solo con il modulo Gestione patch, un add-on disponibile con un codice di licenza separato. Fai riferimento a Installazione patch per maggiori informazioni.
- **Connessione remota** - Usa questa scheda per stabilire una connessione remota all'endpoint coinvolto nell'incidente attuale ed esegui un numero di comandi shell personali sul suo sistema operativo, per rimediare alla minaccia subito oppure ottenere dati per un'ulteriore indagine.

  Cliccando su questo pulsante mostrerai la finestra Connessione remota.

- **INFORMAZIONI DISPOSITIVO**

  Mostra informazioni generali sull'endpoint interessato, come nome dell'endpoint, indirizzo IP, sistema operativo, gruppo pertinente, stato, policy attive e un link che apre una nuova finestra dove poter visualizzare tutti i dettagli dell'endpoint.



Fornisce anche informazioni come il numero di patch installate, le patch la cui installazione non è riuscita o qualsiasi patch mancante, sia di sicurezza che di diverso tipo. Puoi anche generare un rapporto sullo stato delle patch per negli endpoint. Questa sezione viene fornita su richiesta per l'endpoint bersaglio.

All'interno del pannello puoi eseguire le seguenti azioni:

– Visualizzare informazioni sulle patch per l'endpoint di destinazione Per visualizzare i dettagli della patch, clicca su **Aggiorna** all'interno di questa sezione.

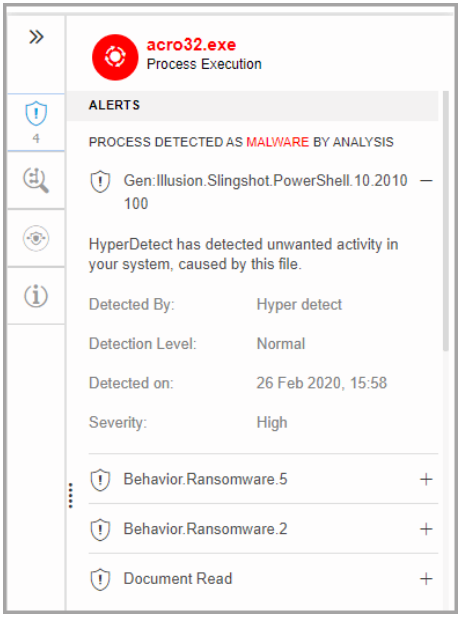
– Visualizzare il rapporto sullo stato delle patch per l'endpoint di destinazione Per generare un rapporto, clicca su **Vedi rapporto stato patch endpoint**.

Pannello dei dettagli per i nodi dei processi

Il pannello **Dettagli nodo** per i nodi dei processi include quattro categorie:

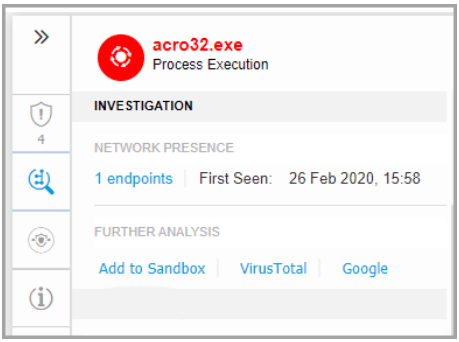
- **ALLERTE**

  Mostra uno o più rilevamenti attivati sul nodo selezionato, incluso dettagli sulla tecnologia di Bitdefender che ha incluso l'elemento nell'incidente, il motivo che ha attivato il rilevamento, il nome del rilevamento, il tipo e la famiglia di malware, e la data del rilevamento. La descrizione per ogni avviso segue gli standard MITRE più recenti.

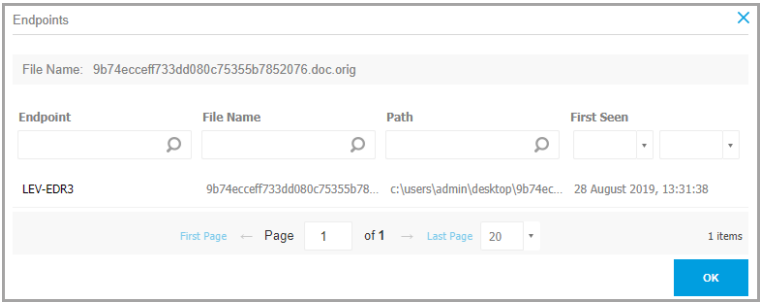


- **INDAGINE**

  Mostra gli indicatori della data per il rilevamento iniziale e tutti gli endpoint in cui è stato individuato questo elemento.



Per visualizzare questo elenco, clicca sul numero mostrato nel campo **endpoint** e comparirà una nuova finestra.

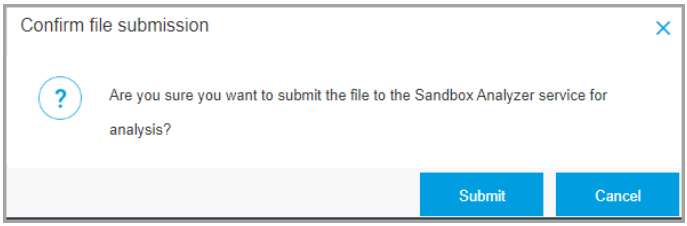


Questa sezione fornisce anche un'analisi esterna, tramite componenti interni e soluzioni di terze parti.

Sono disponibili le seguenti opzioni:

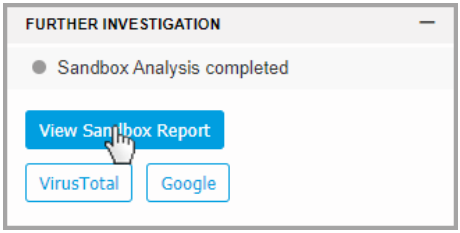
– **Aggiungi a Sandbox** - Usa questa azione per generare un rapporto di Sandbox Analyzer.

  Scegliendo **Aggiungi a Sandbox** ti sarà chiesto di confermare l'invio del file con un'apposita schermata.



Dopo aver confermato, verrai reindirizzato automaticamente alla schermata di invio.

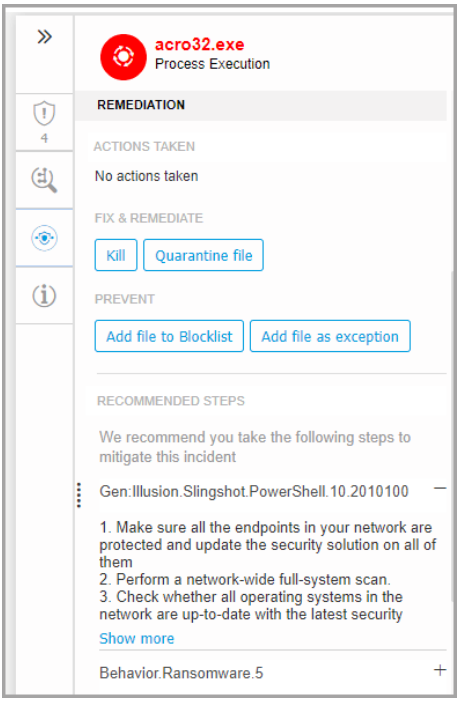
Una volta completata l'analisi, clicca sul pulsante **Vedi rapporto sandbox** per aprire il rapporto completo.



- **VirusTotal** - Usa questa azione per inviare un file esternamente per l'analisi.
- **Google** - Usa questa azione per cercare il valore di hash di un file.

- **RIMEDIO**

  Mostra informazioni sulle azioni intraprese automaticamente da GravityZone per mitigare le minacce, e le azioni che puoi intraprendere:



- **Blocca** - Usa questa azione per bloccare l'esecuzione di un processo. Questa azione crea un'attività di terminazione del processo, visibile nella barra di esecuzione. `Da questa azione sono esclusi i processi system32` e Bitdefender.
- **File di quarantena** - Usa questa azione per archiviare l'elemento in questione e impedirgli di eseguire il suo payload. Questa azione richiede che il modulo Firewall sia stato installato sull'endpoint bersaglio.
- **Aggiungi file a lista elementi bloccati** - Gestisci gli elementi bloccati nella sezione Elementi bloccati.
- **Aggiungi file come eccezione** - Usa questa opzione per escludere attività legittime su una specifica policy. Quando scegli questa azione, si apre una finestra di configurazione in cui ti viene richiesto di selezionare la policy, se

desideri aggiungere un'eccezione. Puoi gestire le eccezioni in **Policy > Antimalware > Impostazioni**.

– **Aggiungi come eccezione EDR** - Usa questa opzione per creare una regola personale che non considererà più il processo come un rilevamento EDR sospetto o dannoso.

1. Cliccando sul pulsante **Aggiungi come eccezione EDR**, comparirà una nuova finestra che ti chiederà di confermare l'azione o annullarla.
2. Dopo aver confermato l'azione, GravityZone ti avviso che la nuova regola è disponibile nella griglia Regole delle eccezioni. Nota che il nome di tutte le regole create all'interno del grafico dell'incidente iniziano con il numero dell'incidente.

Nota
Quando accedi ai dettagli della regola per modificarla, noterai che tutti i criteri per tale regola sono stati inseriti automaticamente, ed è stato aggiunto un criterio di sola lettura con il nome dell'avviso.

Importante
La funzionalità **Aggiungi come eccezione EDR** è disponibile solo per:

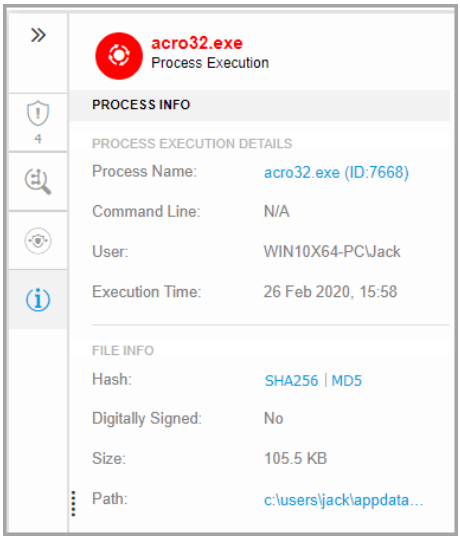
- allerte attivate dalla tecnologia EDR
- nodi generati da un altro processo
- nodi sospetti e dannosi

Se il processo escluso fa parte del percorso critico dell'incidente, allora gli incidenti futuri che corrispondono a questo criterio di eccezione non verranno più generati nella griglia Incidenti. Tali eventi saranno ancora disponibili per la visualizzazione e l'analisi nella pagina Ricerca.
Se il processo escluso non fa parte del percorso critico dell'incidente, allora gli incidenti futuri che corrispondono a questo criterio di eccezione non verranno più generati nella griglia Incidenti, ma non considereranno più tale processo come sospetto o dannoso.

Questa sezione fornisce anche suggerimenti dettagliati per ciascuna allerta rilevata nel nodo selezionato per assisterti nella mitigazione dell'incidente e aumentare il livello di sicurezza del tuo ambiente.

- **INFORMAZIONI SUL PROCESSO**

Mostra dettagli sul nodo del processo selezionato, tra cui il nome del processo, la linea di comando eseguita, l'utente, il momento dell'esecuzione, l'origine e il percorso del file, il valore dell'hash o la firma digitale.



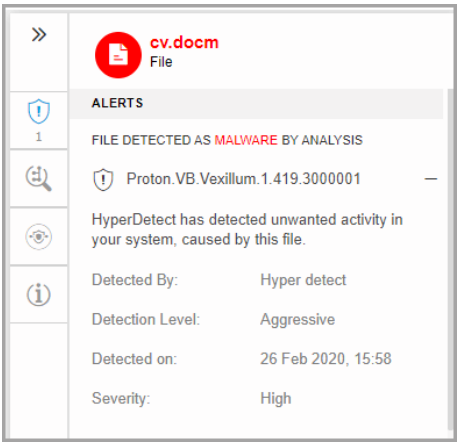
Puoi copiare il valore dell'hash negli appunti cliccando sugli algoritmi di hash disponibili nel campo **Hash** e poi seleziona **Copia negli appunti** per usarlo per aggiungere un valore dell'hash dei file alla **Lista bloccati**. Per maggiori informazioni, fai riferimento a **Inserire file nella lista bloccati**.

Pannello dei dettagli per i nodi dei file

Il pannello **Dettagli del nodo** per i nodi dei file include quattro categorie:

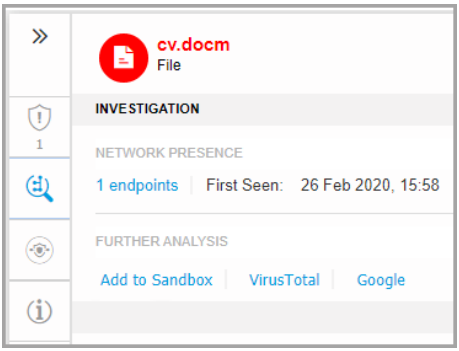
- **ALLERTE**

  Mostra uno o più rilevamenti attivati sul nodo selezionato, incluso dettagli sulla tecnologia di Bitdefender che ha incluso l'elemento nell'incidente, il motivo che ha attivato il rilevamento, il nome del rilevamento, il tipo e la famiglia di malware, e la data del rilevamento. La descrizione per ogni avviso segue gli standard MITRE più recenti.

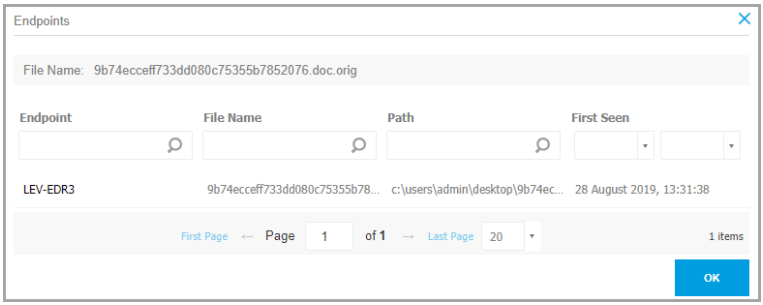


- **INDAGINE**

  Mostra gli indicatori della data per il rilevamento iniziale e tutti gli endpoint in cui è stato individuato questo elemento.



  Per visualizzare questo elenco, clicca sul numero mostrato nel campo **endpoint** e comparirà una nuova finestra.

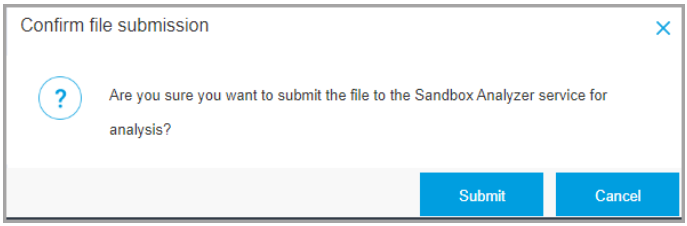


Questa sezione fornisce anche un'analisi esterna, tramite componenti interni e soluzioni di terze parti.

Sono disponibili le seguenti opzioni:

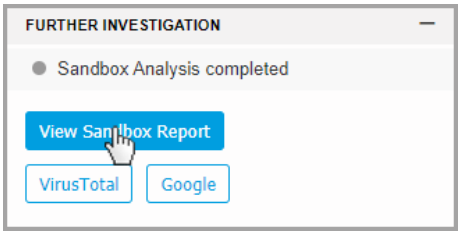
– **Aggiungi a Sandbox** - Usa questa azione per generare un rapporto di Sandbox Analyzer.

  Scegliendo **Aggiungi a Sandbox** ti sarà chiesto di confermare l'invio del file con un'apposita schermata.



  Dopo aver confermato, verrai reindirizzato automaticamente alla schermata di invio.

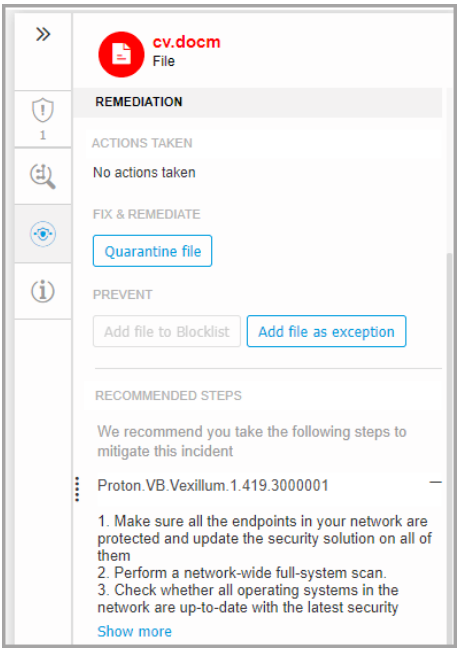
  Una volta completata l'analisi, clicca sul pulsante **Vedi rapporto sandbox** per aprire il rapporto completo.



  - **VirusTotal** - Usa questa azione per inviare un file esternamente per l'analisi.
  - **Google** - Usa questa azione per cercare il valore di hash di un file.

- **RIMEDIO**

  Mostra informazioni sulle azioni intraprese automaticamente da GravityZone per mitigare le minacce, e le azioni che puoi intraprendere:



- **File di quarantena** - Usa questa azione per archiviare l'elemento in questione e impedirgli di eseguire il suo payload. Questa azione richiede che il modulo Firewall sia stato installato sull'endpoint bersaglio.
- **Aggiungi file a lista elementi bloccati** - Gestisci gli elementi bloccati nella sezione Elementi bloccati.
- **Aggiungi file come eccezione** - Usa questa opzione per escludere attività legittime su una specifica policy. Quando scegli questa azione, si apre una finestra di configurazione in cui ti viene richiesto di selezionare la policy, se desideri aggiungere un'eccezione. Puoi gestire le eccezioni in **Policy > Antimalware > Impostazioni**.
- **Aggiungi come eccezione EDR** - Usa questa opzione per creare una regola personale che non considererà più il file come un rilevamento EDR sospetto o dannoso.

  1. Cliccando sul pulsante **Aggiungi come eccezione EDR**, comparirà una nuova finestra che ti chiederà di confermare l'azione o annullarla.

2. Dopo aver confermato l'azione, GravityZone ti avviso che la nuova regola è disponibile nella griglia Regole delle eccezioni. Nota che il nome di tutte le regole create all'interno del grafico dell'incidente iniziano con il numero dell'incidente.

Nota
Quando accedi ai dettagli della regola per modificarla, noterai che tutti i criteri per tale regola sono stati inseriti automaticamente, ed è stato aggiunto un criterio di sola lettura con il nome dell'avviso.

Importante
La funzionalità **Aggiungi come eccezione EDR** è disponibile solo per:

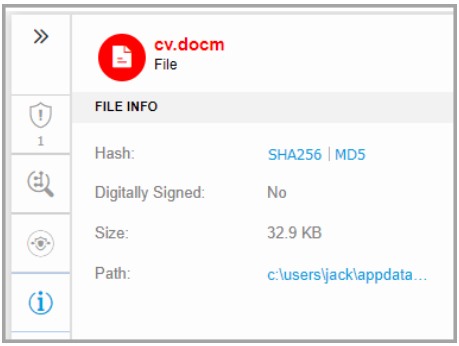
- allerte attivate dalla tecnologia EDR
- nodi generati da un altro processo
- nodi sospetti e dannosi

Se il file escluso fa parte del percorso critico dell'incidente, allora gli incidenti futuri che corrispondono a questo criterio di eccezione non verranno più generati nella griglia Incidenti. Tali eventi saranno ancora disponibili per la visualizzazione e l'analisi nella pagina Ricerca.
Se il file escluso non fa parte del percorso critico dell'incidente, allora gli incidenti futuri che corrispondono a questo criterio di eccezione non verranno più generati nella griglia Incidenti, ma non considereranno più tale processo come sospetto o dannoso.

Questa sezione fornisce anche suggerimenti dettagliati per ciascuna allerta rilevata nel nodo selezionato per assisterti nella mitigazione dell'incidente e aumentare il livello di sicurezza del tuo ambiente.

- **INFO FILE**

  Mostra dettagli sul nodo dei file selezionato, incluso l'origine e il percorso del file, il valore dell'hash o la firma digitale.



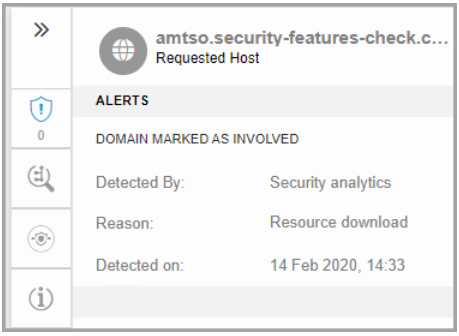
Puoi copiare il valore dell'hash negli appunti cliccando sugli algoritmi di hash disponibili nel campo **Hash** e poi seleziona **Copia negli appunti** per usarlo per aggiungere un valore dell'hash dei file alla **Lista bloccati**. Per maggiori informazioni, fai riferimento a **Inserire file nella lista bloccati**.

Pannello dei dettagli per i nodi dei domini

Il pannello **Dettagli del nodo** per i nodi dei domini include quattro categorie:

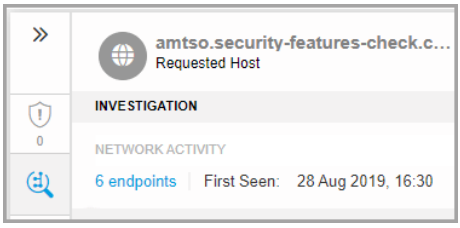
- **ALLERTE**

  Mostra la severità del dominio come indicata dalla tecnologia di Bitdefender che ha incluso tale entità nell'incidente, il motivo che ha attivato il rilevamento e la data in cui è stato rilevato.

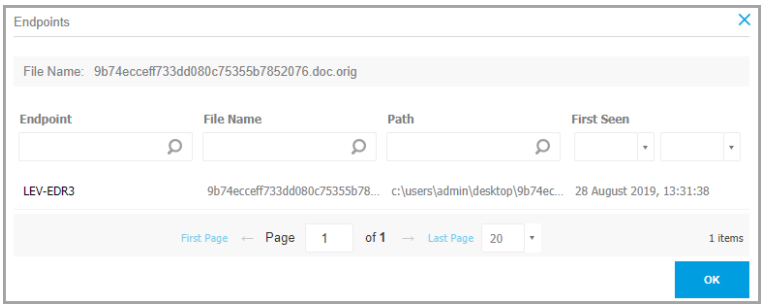


- **INDAGINE**

Mostra gli indicatori della data per il rilevamento iniziale e tutti gli endpoint in cui è stato individuato questo elemento.

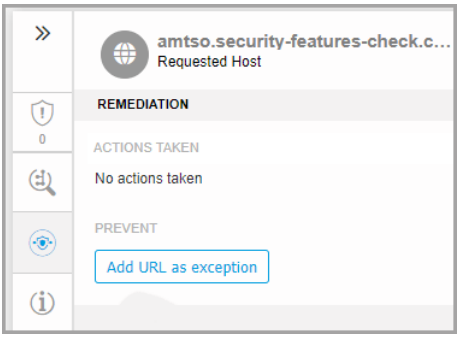


Per visualizzare questo elenco, clicca sul numero mostrato nel campo **endpoint** e comparirà una nuova finestra.



- **RIMEDIO**

  Mostra informazioni sulle azioni intraprese automaticamente da GravityZone per mitigare le minacce, e le azioni che puoi intraprendere:



- **Aggiungi URL come eccezione** - Usa questa opzione per escludere attività legittime su una specifica policy. Quando scegli questa azione, si apre una finestra di configurazione in cui ti viene richiesto di selezionare la policy, se desideri aggiungere un'eccezione. Puoi gestire le eccezioni in **Policy > Antimalware > Impostazioni**.
- **Aggiungi come eccezione EDR** - Usa questa opzione per creare una regola personale che non considererà più il dominio come un rilevamento EDR sospetto o dannoso.

  1. Cliccando sul pulsante **Aggiungi come eccezione EDR**, comparirà una nuova finestra che ti chiederà di confermare l'azione o annullarla.
  2. Dopo aver confermato l'azione, GravityZone ti avviso che la nuova regola è disponibile nella griglia Regole delle eccezioni. Nota che il nome di tutte le regole create all'interno del grafico dell'incidente iniziano con il numero dell'incidente.

  Nota
  Quando accedi ai dettagli della regola per modificarla, noterai che tutti i criteri per tale regola sono stati inseriti automaticamente, ed è stato aggiunto un criterio di sola lettura con il nome dell'avviso.

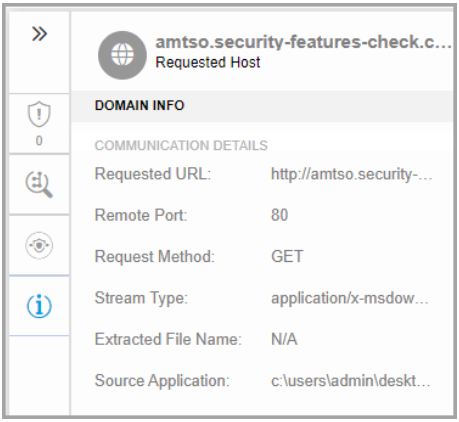
  Importante
  La funzionalità **Aggiungi come eccezione EDR** è disponibile solo per:

  - allerte attivate dalla tecnologia EDR
  - nodi generati da un altro processo
  - nodi sospetti e dannosi

Se il dominio escluso fa parte del percorso critico dell'incidente, allora gli incidenti futuri che corrispondono a questo criterio di eccezione non verranno più generati nella griglia Incidenti. Tali eventi saranno ancora disponibili per la visualizzazione e l'analisi nella pagina Ricerca.
Se il dominio escluso non fa parte del percorso critico dell'incidente, allora gli incidenti futuri che corrispondono a questo criterio di eccezione non verranno più generati nella griglia Incidenti, ma non considereranno più tale processo come sospetto o dannoso.

- **INFORMAZIONI DEL DOMINIO**

  Mostra dettagli sul nodo dei domini selezionato, incluso l'URL richiesto, la porta usata, il metodo della richiesta, il tipo di stream, il nome del file estratto e l'applicazione di origine.

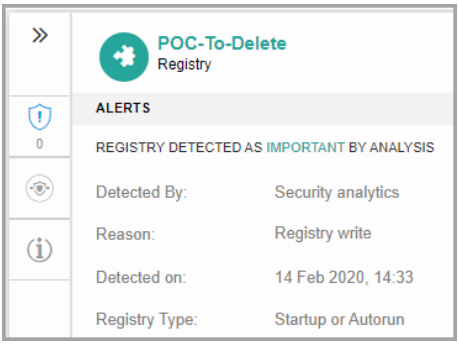


Pannello dei dettagli per i nodi del registro

Il pannello **Dettagli del nodo** per i nodi del registro include tre categorie:

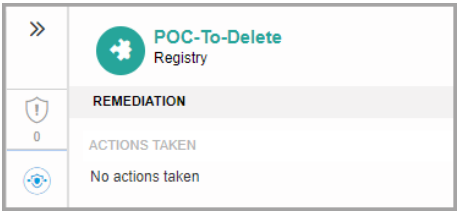
- **ALLERTE**

  Mostra la severità della manipolazione del registro come indicata dalla tecnologia di Bitdefender che ha incluso tale entità nell'incidente, il motivo che ha attivato il rilevamento, la data in cui è stato rilevato e il tipo di registro.



- **RIMEDIO**

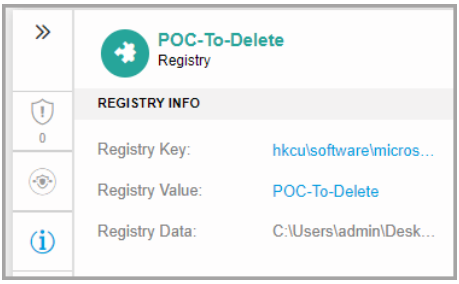
  Mostra informazioni sulle azioni intraprese automaticamente da GravityZone.



  La sezione **RIMEDIO** per i nodi del registro non fornisce alcuna opzione di azione diretta.

- **INFORMAZIONI DEL REGISTRO**

  Mostra dettagli sul nodo del registro selezionato, tra cui la chiave del registro, il valore e i dati.

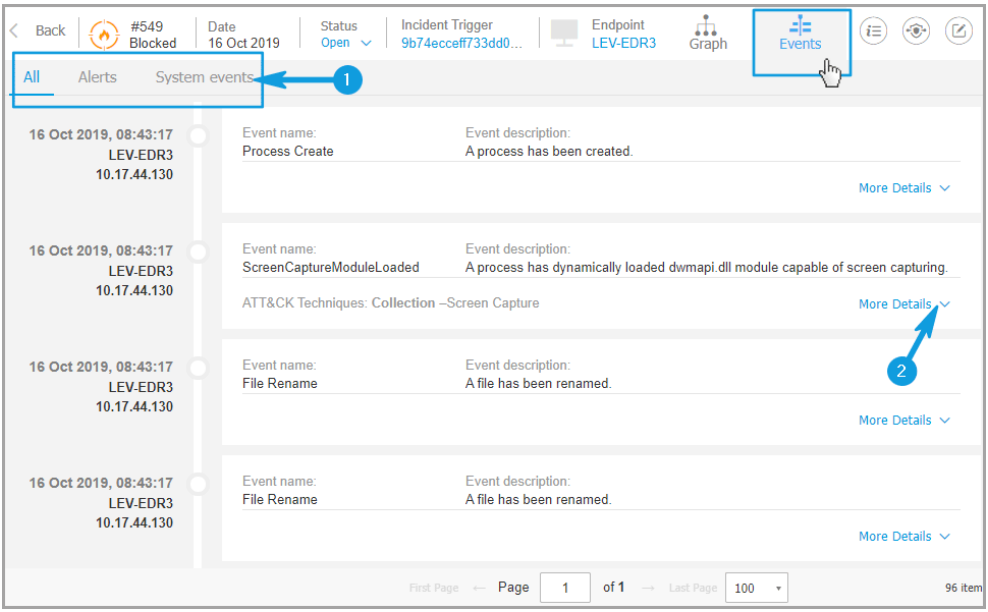


Puoi cliccare sulla chiave del registro e sul valore per copiarla per ulteriori analisi.

Eventi

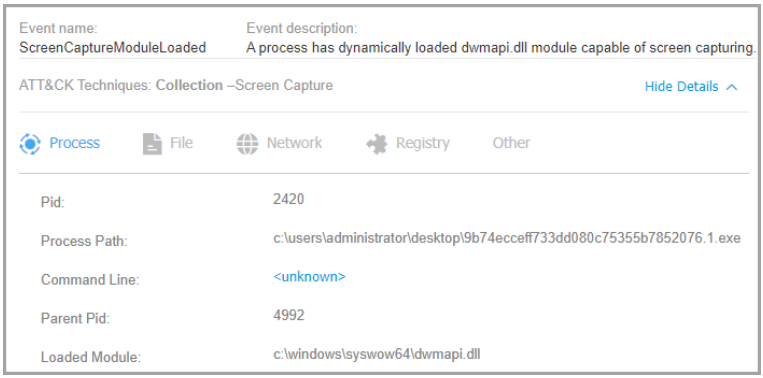
Usa la scheda **Eventi** per visualizzare come si è svolta la sequenza di eventi per innescare l'incidente attualmente indagato. Questa finestra mostra gli avvisi e gli eventi del sistema correlati e rilevati dalle tecnologie di GravityZone, come EDR, Network Attack Defense, Anomaly Detection, Advanced Anti-Exploit e Windows Antimalware Scan Interface (AMSI).

Ogni evento complesso ha una descrizione dettagliata che spiega come è stato rilevato e cosa potrebbe accadere se l'elemento venisse usato per scopi dannosi, in base alle più recenti tecniche e tattiche MITRE.



Scheda Eventi

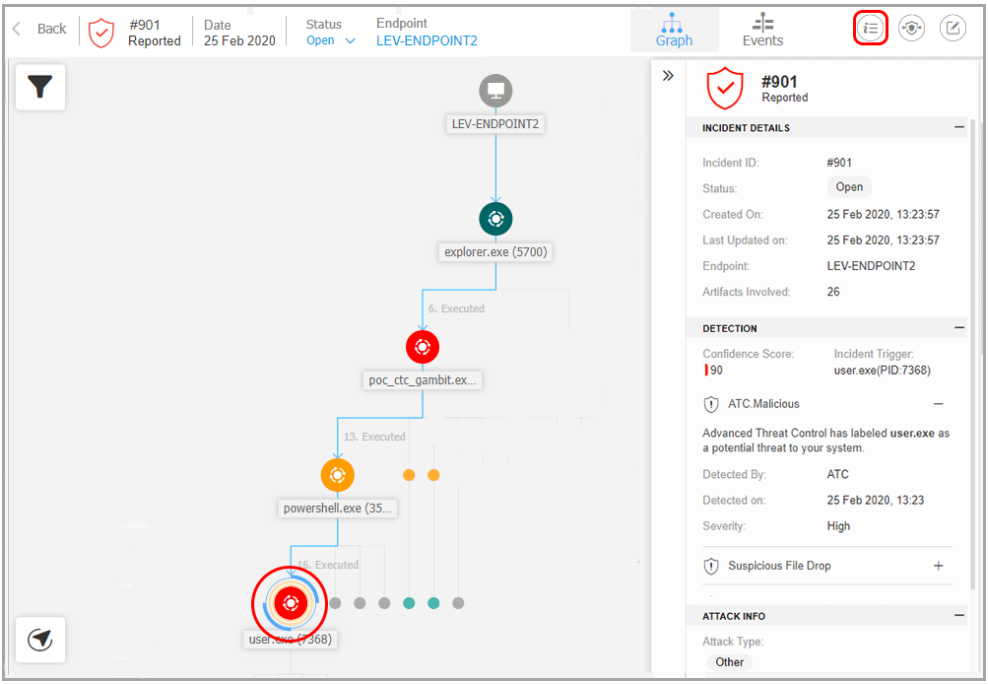
1. Usa le opzioni di filtro per mostrare tutti gli eventi o solo gli eventi del sistema o quelli complessi (avvisi).
2. Clicca sul pulsante **Altri dettagli** per espandere ciascun evento e accedere a informazioni aggiuntive.



Informazioni incidente

Questo pannello include sezioni comprimibili con dettagli come ID incidente, stato attuale, data e ora di creazione e ultimo aggiornamento, numero di elementi coinvolti, nome e descrizione del trigger, e informazioni sull'attacco.

Da questa sezione è possibile accedere all'incidente esteso che include questo incidente dell'endpoint, se il caso.

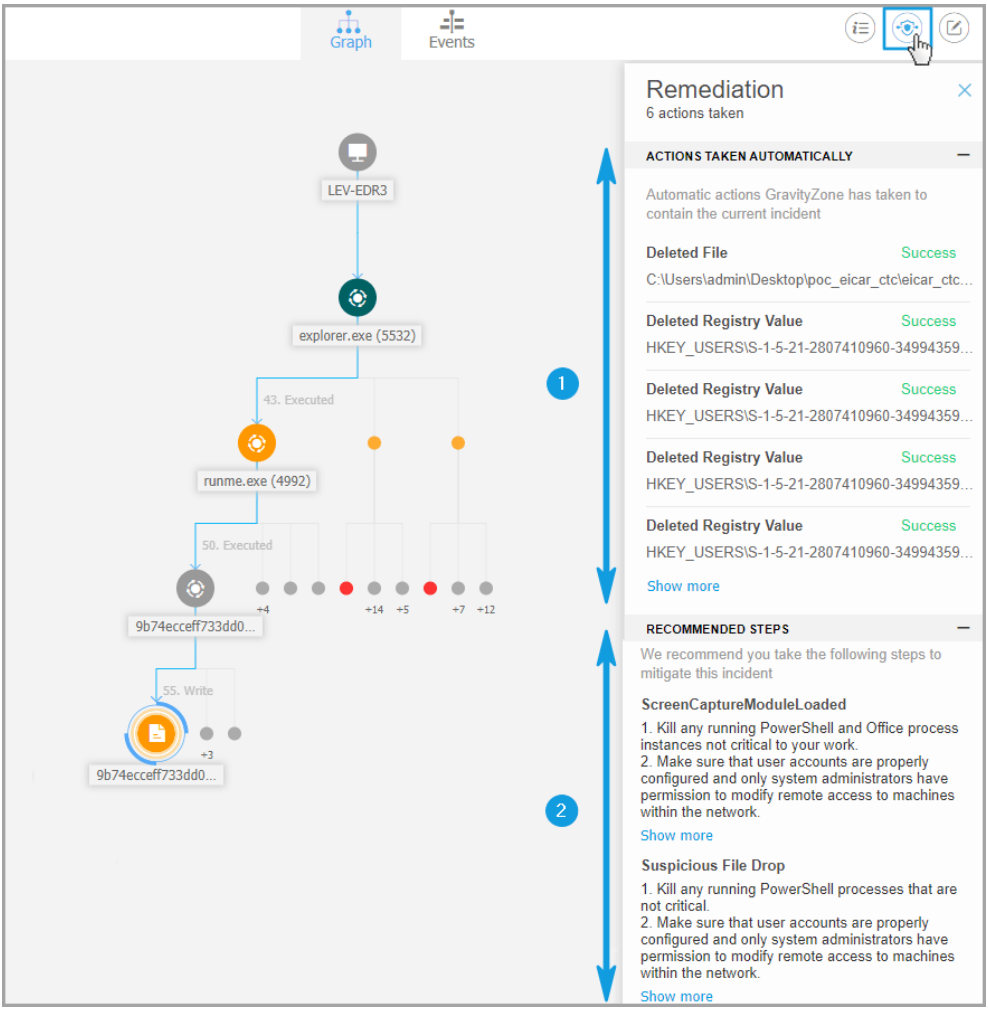


Pannello Informazioni incidente

Il pannello include anche gli avvisi rilevati sull'elemento che hanno innescato l'incidente.

Rimedio

Il pannello **Risanamento** fornisce informazioni complete sulle azioni correttive che sono state intraprese automaticamente da GravityZone in caso di attacchi bloccati da tecnologie come Advanced Threat Control (ATC), HyperDetect e Antimalware, oltre ai passaggi suggeriti da intraprendere per contenere l'incidente e aumentare il livello di sicurezza del proprio sistema.



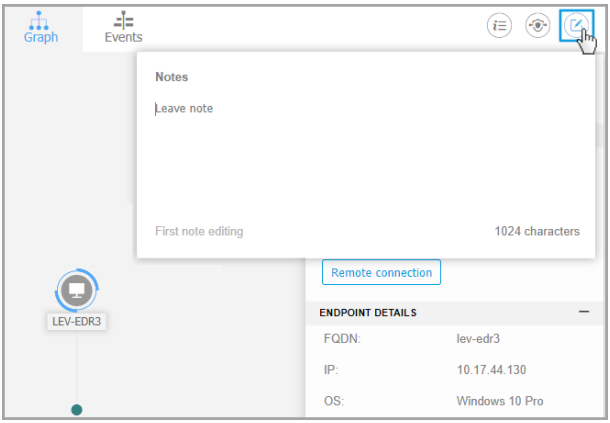
Pannello riparazione

1. Azioni intraprese automaticamente da GravityZone.
2. Suggerimenti per contenere ulteriormente l'incidente e incrementare la sicurezza.

Nota
I passaggi suggeriti corrispondono agli avvisi rilevati sul nodo che ha innescato l'incidente indagato.

Note

La sezione **Note** ti consente di aggiungere una nota per tenere traccia dei recenti cambiamenti e facilitare la modifica della proprietà dell'incidente.

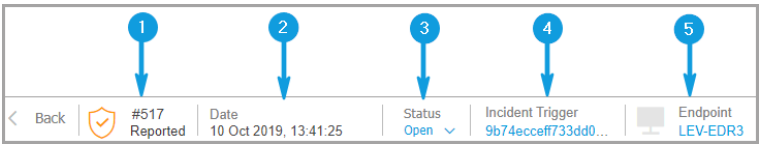


Note negli appunti

1. Per lasciare una nota per l'evento attuale, clicca sul pulsante **Note** per mostrare una nuova finestra.
2. Inserisci il tuo messaggio in questa finestra (massimo 2.048 caratteri).

Barra stato incidente

La barra di stato dell'incidente fornisce tag dell'evento di sicurezza che possono aiutarti a rilevare informazioni chiave sugli endpoint di rete coinvolti.



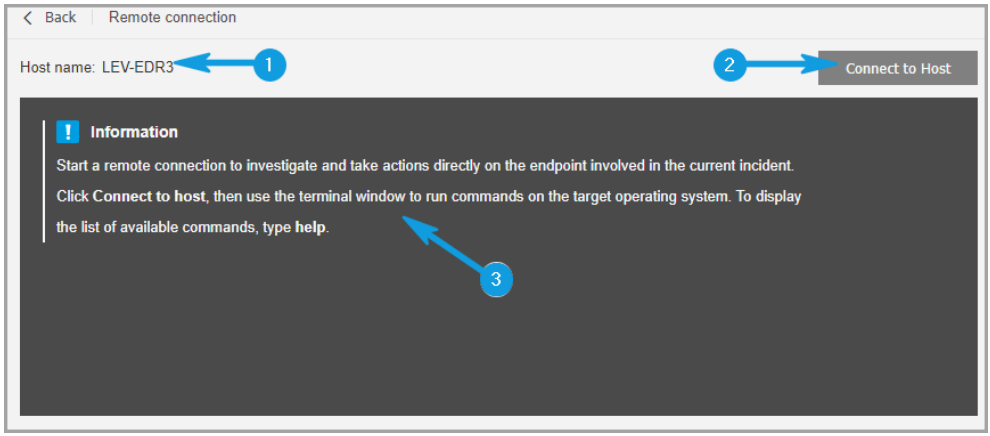
Barra stato incidente

1. ID incidente - il numero di identificazione dell'incidente sotto indagine e se l'incidente è stato bloccato o solo segnalato.
2. Intervallo temporale rilevamento - la data e l'ora in cui l'incidente è stato innescato.
3. Stato dell'incidente - lo stato attuale dell'incidente.
4. Trigger incidente - il nome dell'elemento che ha generato l'incidente.
5. Endpoint - il nome dell'endpoint bersaglio.

Cliccando sul pulsante **Indietro** tornerai alla pagina principale **Incidenti**.

Connessione remota

Usa questa scheda per stabilire una connessione remota all'endpoint coinvolto nell'incidente attuale ed esegui un numero di comandi shell personali sul suo sistema operativo, per annullare la minaccia subito oppure ottenere dati per un'ulteriore indagine.



Scheda Connessione remota

La scheda **Connessione remota** include i seguenti elementi:

1. Il nome dell'endpoint coinvolto nell'evento di sicurezza attuale
2. Il pulsante che controlla la connessione remota (connetti / disconnetti)
3. La finestra del terminale

Prerequisiti della sessione del terminale

- La versione dell'agente di Bitdefender installata sull'endpoint supporta la funzionalità Connessione remota.
- L'endpoint deve essere alimentato ed essere online.
- L'endpoint deve avere un sistema operativo Windows.
- GravityZone è in grado di comunicare con l'endpoint.
- Il tuo account di GravityZone deve avere i permessi di gestione per l'endpoint bersaglio.

Creare una Connessione remota

Ecco come funziona la connessione remota:

1. Avvia la sessione live cliccando sul pulsante **Connetti a host**.

   Lo stato della connessione sarà mostrato accanto al nome dell'endpoint.

Se la connessione fallisse, nella finestra del terminale sarà mostrato un messaggio di errore.

> **Nota**
> Puoi aprire un massimo di cinque sessioni del terminale contemporaneamente con lo stesso endpoint.

2. Una volta connesso, il terminale mostra l'elenco dei comandi disponibili e la loro descrizione. Digita il comando desiderato nella finestra del terminale seguito da `Invio`.

   Per più informazioni su un comando, digita `help` seguito dal nome del comando (per esempio, `help ps`).

3. Il terminale mostra l'output del comando, quando il comando ha successo.

   Se l'endpoint non riesce a completare l'esecuzione del comando, il comando sarà scartato.

   La cronologia dei comandi viene registrata nella finestra del terminale. Tuttavia, puoi visualizzare i comandi digitati in precedenza premendo i tasti freccia.

4. Per terminare la connessione, clicca sul pulsante **Termina sessione**.

   La sessione del terminale scade automaticamente dopo cinque minuti di inattività.

   Anche navigando oltre la scheda **Connessione remota** mentre si è connessi a un endpoint terminerà la sessione del terminale.

Comandi sessione terminale

I comandi della sessione del terminale EDR sono comandi shell personalizzati, indipendenti dalla piattaforma e che usano una sintassi generica. Qui di seguito puoi trovare l'elenco dei comandi disponibili che puoi usare sugli endpoint tramite la sessione del terminale:

- `ps`
  - **Descrizione**: mostra informazioni sui processi attualmente in esecuzione sull'endpoint bersaglio, come ID del processo (PID), nome, percorso o utilizzo della memoria.
  - **Sintassi**: `ps`

  - **Alias**: `tasklist`
  - **Parametri**: -

- `kill`
  - **Descrizione**: Termina un processo o un'applicazione in esecuzione sull'endpoint bersaglio tramite il proprio PID. Usa il comando `ps/tasklist`per ottenere il PID.
  - **Sintassi**: `kill [PID]`
  - **Alias**: -
  - **Parametri**: `[PID]` - l'ID del processo dall'endpoint bersaglio.
- `ls (dir)`
  - **Descrizione**: Mostra informazioni su tutti i file e le cartelle della cartella specificata, come nome, tipo, dimensione e data di modifica. Consente i caratteri jolly per indicare il percorso. Per esempio:

    `C:\Users\admin\Desktop\s*` tutti i contenuti della cartella Desktop che iniziano con "s"

    `C:\Users\publ??` elenca tutti i contenuti del percorso specificato con una qualsiasi delle ultime due lettere.
  - **Sintassi**: `ls [path]`
  - **Alias**: `dir`
  - **Parametri**: `[Path]` - il percorso a un file o una cartella sull'endpoint bersaglio.
- `rm (del, delete)`
  - **Descrizione**: Elimina file o cartelle dal percorso specificato sull'endpoint bersaglio.
  - **Sintassi**: `rm [path]`
  - **Alias**: `del/delete`
  - **Parametri**: `[Path]` - il percorso a un file o una cartella sull'endpoint bersaglio.
- `reg query`

- **Descrizione**: Offre tutte le informazioni (nome, tipo e valore) per il percorso della chiave del registro specificato.
- **Sintassi**: `reg query [keypath] [/k] [keyname] [/v] [valuename]`
- **Alias**: -
- **Parametri**:
  - `keypath`- riporta tutte le informazioni sulle chiave del registro del percorso specificato.
  - `/k [keyname]` - filtra i risultati delle chiavi del registro tramite il nome di una determinata chiave. Puoi anche usare caratteri jolly (*, ?) per filtrare una gamma più ampia di nomi.
  - `/v [valuename]` - filtra i valori del registro tramite un determinato nome del valore. Puoi anche usare caratteri jolly (*, ?) nel nome del valore per filtrare una gamma più ampia di nomi.

- `reg add`
  - **Descrizione**: Aggiunge un nuovo valore o chiave del registro. Sovrascrive un valore del registro, nel caso esistesse già. Nel sovrascrivere informazioni del registro, devi indicare tutti i parametri definiti.
  - **Sintassi**: `reg add [keyname] [/v] [valuename] [/t] [datatype] [/d] [data]`
  - **Alias**: -
  - **Parametri**:
    - `[keyname]` - il nome della chiave di registro.
    - `/v [valuename]` - il nome del valore del registro. Richiede almeno di aggiungere il parametro /d [data].
    - `/t [datatype]` - il tipo di dati del valore del registro. Puoi aggiungere uno dei seguenti tipi di dati:

      `REG_SZ, REG_MULTI_SZ, REG_DWORD, REG_BINARY, REG_DWORD_LITTLE_ENDIAN, REG_LINK, REG_FULL_RESOURCE_DESCRIPTOR, REG_EXPAND_SZ`

      Se non specificato, il tipo `REG_SZ` viene assegnato in modo predefinito.

Una volta impostato il tipo in `REG_BYNARY`, i dati del registro vengono interpretati come valori esadecimali.

- `reg delete`
  - **Descrizione**: elimina una chiave del registro o i suoi valori.
  - **Sintassi**:

    `reg delete [keyname] [/v] [valuename]`

    `reg delete [keyname] [/va]`
  - **Alias**: -
  - **Parametri**:

    `[keyname]` - elimina la chiave del registro e di tutti i suoi valori.

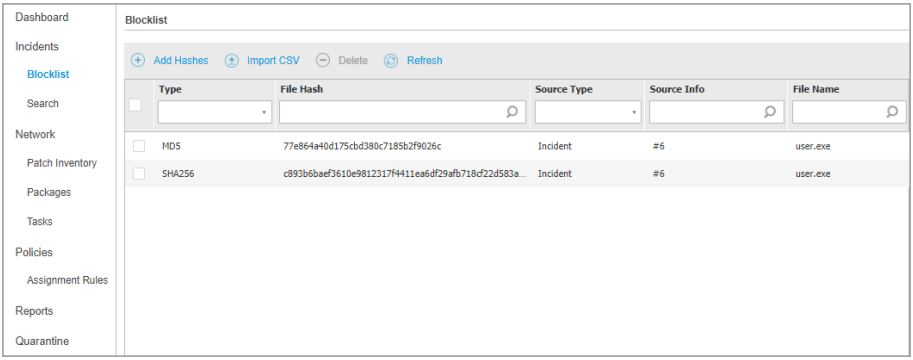
    `/v [valuename]` - elimina il valore del registro specificato.

    `/va` - elimina tutti i valori della chiave del registro specificato.
- `cd`
  - **Descrizione**: Modifica la cartella di lavoro nel percorso specificato. Questo comando richiede, come parametro, il percorso di un'unità o una cartella dell'endpoint bersaglio.
  - **Sintassi**: `cd [path]`
  - **Alias**: -
  - **Parametri**: `[Path]` - il percorso a un file o una cartella sull'endpoint bersaglio.
- `aiuto`
  - **Descrizione**: Senza specificare un parametro, aiuta a elencare tutti i comandi disponibili con una breve descrizione. Quando si inserisce help seguito da un parametro, viene visualizzata la sintassi completa di tale comando, una breve descrizione e un esempio di utilizzo.
  - **Sintassi**: `help [command]`
  - **Alias**: -
  - **Parametri**: command name (per esempio: `cd, kill, ls, ps`)
- `clear (cls)`

- **Descrizione**: Libera la finestra del terminale e mostra il prompt con la cartella di lavoro attuale.
- **Sintassi**: `clear`
- **Alias**: `cls`
- **Parametri**: -

9.2. Inserire file nella lista bloccati

Nella pagina **Lista bloccati**, puoi visualizzare e gestire gli elementi tramite i valori dei propri hash. Vedi le registrazioni delle attività nel Rapporto attività utente.



Pagina Lista bloccati

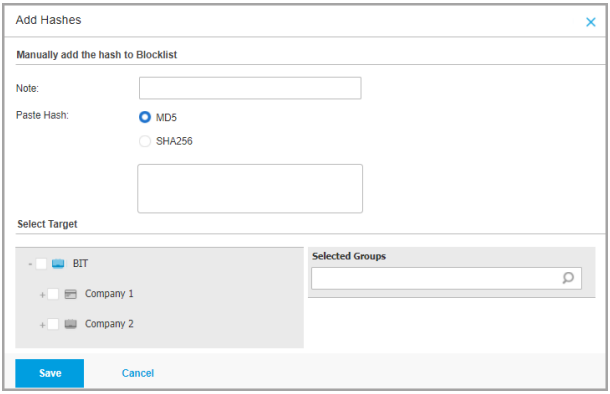
In una tabella di dati, puoi visualizzare i seguenti dettagli per ciascun elemento:

- Tipo di file:
  - MD5
  - SHA256
- Valore hash file
- Tipo di risorsa:
  - Incidente
  - Importa
  - Manuale

- Info sorgente
- Nome File
- Azienda

Aggiungi i valori hash alla Lista bloccati esistente:

1. Copia il valore dell'hash da **Informazioni file**.
2. Scegli da **MD5** o **SHA256** e copia il valore nello spazio sottostante.
   Se necessario, aggiungi una nota.
3. Clicca su **Salva**.

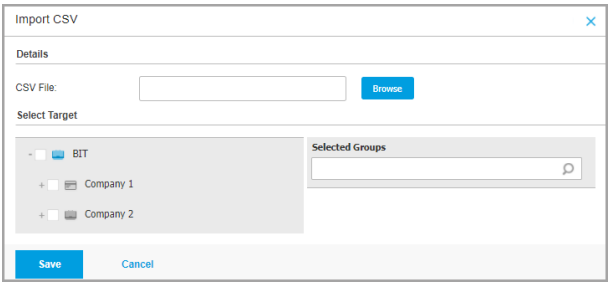


Aggiungere una finestra del valore hash

Importante
Il **Sensore incidenti** bloccherà ogni file binario il cui valore di hash è stato aggiunto alla **Lista bloccati** dall'avvio di un processo.

Importa i valori di hash nella Lista bloccati esistente. Per importare un file CSV:

1. Clicca su **Importa CSV**.
2. Cerca il tuo file CSV e clicca su **Salva**.



Finestra Importa CSV

Puoi anche importare file CSV locali dal tuo dispositivo nella pagina **Lista bloccati**, ma prima assicurati che il tuo file CSV sia valido.

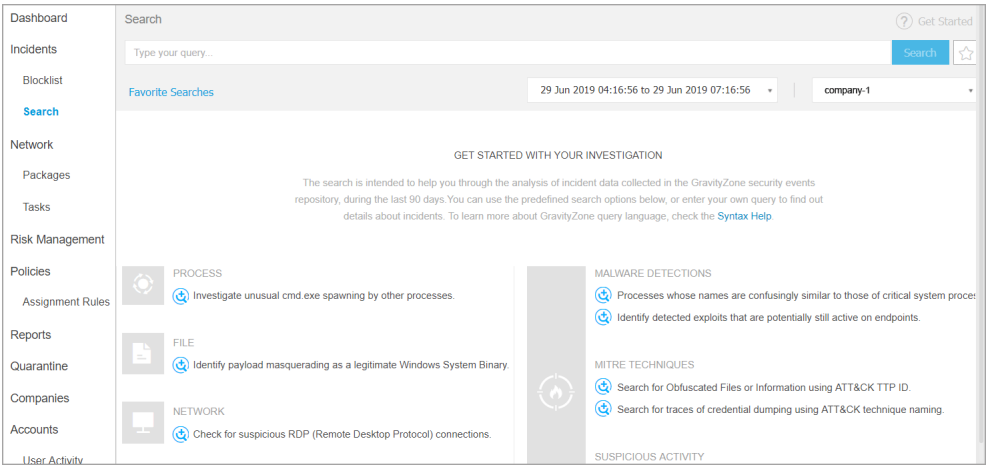
Per creare un file CSV valido per l'importazione, devi prima inserire nelle tre colonne i seguenti dati:

1. La prima colonna del file CSV deve contenere il tipo di hash: `md5` o `sha256`.
2. La seconda colonna deve contenere i valori esadecimali dell'hash corrispondenti.
3. La terza colonna può contenere informazioni opzionali relative alla colonna **Informazioni sorgente** nella pagina **Lista bloccati**.

Nota
Le informazioni corrispondenti alle altre colonne nella pagina **Lista bloccati** saranno compilate automaticamente dopo l'importazione del file CSV.

9.3. Cercare gli eventi di sicurezza

Dalla pagina **Cerca** puoi passare in rassegna gli eventi passati in base a criteri complessi.



Panoramica pagina di ricerca

Per visualizzare gli eventi che ti interessano, devi creare delle query usando il linguaggio query disponibile in GravityZone.

Nella pagina **Cerca** sono disponibili le seguenti opzioni:

- Una barra di ricerca per l'inserimento di query, che puoi cliccare per visualizzare l'elenco dei termini delle query suddivisi per categoria, con una funzionalità di completamento automatico.
- Il salvataggio delle ricerche preferite, da usare in futuro.
- Opzioni di applicazione di filtri per azienda, data e ora.
- Una sezione **Inizia**, con un link alla guida per la sintassi del linguaggio delle query.
- Query predefinite, progettate per casi utili di ricerca di eventi di sicurezza.

9.3.1. Il linguaggio query

Il linguaggio query fornisce il vocabolario (campi e operatori) e la sintassi necessari per creare delle query. Li trovi descritti nel presente documento.

Clicca sul link di **Aiuto sintassi** e seleziona la scheda **Linguaggio query** per visualizzare i relativi contenuti.

Campi

Il campo delle query corrisponde a quello del database di GravityZone. I campi rappresentano elementi come percorsi e hash di file, nomi dell'host o nomi di dominio.

Ciascun campo può avere uno o più valori, che rappresentano il suo stato in un dato momento. Questi valori indicano tipi di dati differenti, a seconda del campo.

Operatori

Gli operatori ti permettono di creare relazioni tra i campi o criteri di ricerca. Puoi usare i seguenti operatori:

Operatore	Esempio	Descrizione
`:`	`fieldCategory.option: value1`	Confronta il valore del campo della query con i valori del campo corrispondente del database.
`" "`	`fieldCategory.option: "value1 value2"`	Le stringhe contenute all'interno delle virgolette vengono prese in considerazione insieme, come frase.
`( )`	`fieldCategory1.option: value1 E (fieldCategory2.option: value2 O fieldCategory3.option: value3)`	Raggruppa i termini della query.
`AND`	`fieldCategory1.option: value1 E fieldCategory2.option: value2`	Restituisce i risultati che corrispondono a tutte le condizioni della tua query.
`o`	`fieldCategory1.option: value1 O fieldCategory2.option: value2`	Restituisce i risultati una qualsiasi delle condizioni della tua query.

Operatore	Esempio	Descrizione
`E NON`	`fieldCategory1.option: value1 E NON fieldCategory2.option: value2`	Questo operatore è utile nelle query complesse e fornisce risultati che non corrispondono al termine specificato, a parte tutte le altre condizioni.
`_exists_`	`_exists_: fieldCategory.option`	Restituisce risultati che contengono il campo indicato.
`-`	`fieldCategory.option: -value`	Usa il segno meno (-) quando il valore deve essere escluso dai risultati.
`?`	`fieldCategory.option: ???_file.path`	Usa un punto di domanda (?) per abbinare un qualsiasi carattere nel valore del campo.
`*`	`fieldCategory.option: file.*`	Usa un asterisco (*) per indicare qualsiasi valore.

Sintassi query

Una query è una condizione o una serie di condizioni logiche legate da operatori che restituiscono come risultato eventi provenienti dal database EDR.

Tutte le condizioni devono essere correlate ai campi. Alcune condizioni richiedono l'immissione di un valore, altre no. Ad esempio, non hai bisogno di inserire un valore se vuoi soltanto sapere se il campo è presente tra i dettagli dell'evento.

Le query possono essere semplici o complesse. Le query complesse hanno query annidate (query in un'altra query).

Una valida sintassi del campo consiste nella categoria del campo seguita da una delle opzioni nella sezione **Lingua query**, e il suo valore corrispondente: `fieldCategory.option: value`.

Per esempio, `file.path: "%system32%\com\svchost.exe"` è una query abbastanza semplice che cerca tutti gli eventi che includono `%system32%\com\svchost.exe`, e consiste in:

- Una categoria di campo obbligatoria e relativa opzione (separate da un punto): `file.path`
- Un operatore: i due punti (:), per confrontare il valore del campo

- Il valore ricercato: `%system32%\com\svchost.exe`
- Virgolette (" "), perché il valore contiene caratteri speciali, come <\> e <.>

9.3.2. Eseguire query

Per eseguire una query:

1. Digita la stringa della query nel campo.

   Clicca il campo **Cerca** per vedere l'elenco dei termini di ricerca suddivisi per categoria. Seleziona il termine che desideri per iniziare a creare la tua query.

   Control Center ti aiuta durante la digitazione, con suggerimenti per il completamento automatico. Usa i tasti di direzione per selezionare una delle opzioni suggerite, quindi premi **Invio** per aggiungerla alla query.

   Se ti serve ulteriore aiuto, clicca il link **Aiuto sintassi**.

   Nota
   Puoi usare le query annidate per effettuare ricerche complesse.

2. Per filtrare gli eventi in base a un intervallo temporale, clicca il campo dell'ora.

   Importante
   L'intervallo di conservazione dei dati predefinito per gli eventi è 7 giorni. Se vuoi aumentare la tua capacità, devi contattare il tuo rappresentante vendite per fare l'upgrade della soluzione con un add-on **Conservazione dati** di 30, 90 o 180 giorni.

   Ha diverse opzioni a disposizione per definire l'intervallo di tempo della ricerca:

   - Solo una data specifica.

     Seleziona una data nella scheda **Da** del calendario.
   - Un intervallo di tempo esatto.
     a. Seleziona la data iniziale nella scheda **Da** del calendario.
     b. Seleziona la data di termine nella scheda **A**.
   - Un intervallo di tempo recente dalle opzioni disponibili.
   - Clicca su **OK**.

3. Seleziona il nome dell'azienda di cui vuoi visualizzare gli eventi. Digita il nome dell'azienda o scegline uno dell'elenco a discesa.

La ricerca può includere una sola azienda per volta.

4. Clicca su **Cerca** o premi **Invio**.

   Puoi vedere gli eventi corrispondenti, insieme ai relativi dettagli, sotto la query.

   Importante

   Quando cerchi la query `detections.detection_type` nel campo *Cerca*, Control Center richiede di completarla con un valore intero compreso tra 1 a 15 (ad esempio `detections.detection_type:1`).

   Ogni valore inserito corrisponde a un determinato tipo di rilevazione, come segue:

   a. `detections.detection_type:1` - Rilevamento di Advanced Threat Control
   b. `detections.detection_type:2` - Rilevamento motori statici antimalware
   c. `detections.detection_type:3` - Rilevamento HyperDetect
   d. `detections.detection_type:4` - Notifica evento sospetto Advanced Threat Control
   e. `detections.detection_type:5` - Rilevamento di HyperDetect per tipo di attacco segnalato
   f. `detections.detection_type:6` - Rilevamento Antimalware CMDLine Scanner
   g. `detections.detection_type:7` - Rilevamento Cross Technologies Correlation
   h. `detections.detection_name:8` - Rilevamento Network Attack Defense
   i. `detections.detection_type:9` - Rilevamento di HyperDetect da tipo di attacco non segnalato
   j. `detections.detection_type:10` - Sandbox Analyzer ha effettuato un rilevamento in un ambiente limitato dopo un'analisi dinamica
   k. `detections.detection_type:11` - Rilevamento Buffer Register Scan
   l. `detections.detection_type:12` - Rilevamento URL
   m. `detections.detection_type:13` - Rilevamento avanzato Anti-Exploit
   n. `detections.detection_type:14` - Rilevamento analisi comportamento utenti

o. `detections.detection_type:15` - Rilevamento interfaccia scansione antimalware

p. `detections.detection_type:16` - Rilevamento della correlazione tra tecnologie basate sul machine learning

Control Center può mostrare fino a 10.000 eventi. Se i risultati della query contengono più di 10.000 eventi, comparirà un messaggio sullo schermo. In questo caso, dovrai restringere la tua ricerca.

9.3.3. Ricerche preferite

La maggior parte delle query è piuttosto lunga e quindi difficile da creare o ricordare. Invece di salvarle in un file per poi copiarle e incollarle in GravityZone, puoi salvarle direttamente in GravityZone in modo da averle sempre a portata di mano.

Per salvare la tua query:

1. Inserisci la stringa nel campo **Cerca**.
2. Clicca sull'icona ☆ a destra del campo **Cerca**.
3. Quando ti viene richiesto di assegnarle un nome, digita il nome che vuoi dare alla query.
4. Clicca su **Add** (Aggiungi).

Clicca sul link **Ricerche preferite** sotto il campo **Query** per visualizzare le query che hai salvato.

A questo punto puoi scegliere tra tre opzioni:

- Eseguire la query.
- Modificare il nome della query.
- Eliminare la query.

Per eseguire una query salvata:

1. Clicca sul link **Ricerche preferite**.
2. Seleziona la query che preferisci.

   La stringa salvata verrà aggiunta al campo **Cerca**.

Nota
Se necessario, modifica la stringa della query. Inoltre, puoi anche salvare la nuova query di ricerca nelle tue ricerche preferite.

3. Usa i filtri per azienda e calendario per restringere la ricerca.
4. Clicca su **Cerca**.

Se devi modificare l'elenco delle tue query, posiziona il cursore del mouse sulla query salvata per vedere le opzioni incorporate.

- Clicca sull'icona **Modifica** per rinominare la query.
- Se non hai più bisogno della query, clicca sull'icona **Elimina**.

9.3.4. Query predefinite

La pagina **Cerca** contiene alcuni esempi di ricerche tramite query complesse, specifiche per indagini relative a eventi di sicurezza.

Le query predefinite sono raggruppate per categoria di indagine di sicurezza.

Per eseguire una query predefinita:

- Clicca l'icona accanto alla descrizione della query predefinita.
- La frase della query comparirà automaticamente nella barra **Cerca**. Inserisci i dettagli specifici dei termini della query.
- Clicca il pulsante **Cerca** per eseguire la query.

Nota
Dalla pagina **Cerca** puoi ritornare in qualsiasi momento alle opzioni **Inizia**, cliccando sul link **Inizia** nell'angolo in alto a destra della pagina.

9.4. Regole personali

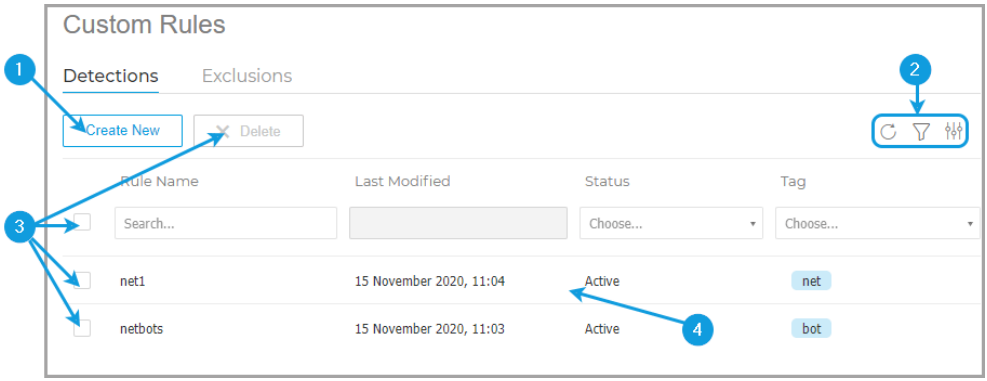
La pagina **Regole personali** fornisce la struttura per creare e gestire regole personali per includere o escludere determinati comportamenti dall'attivare gli incidenti.

Questa funzionalità EDR include due categorie principali:

- Rilevazioni
- Eccezioni

9.4.1. Rilevazioni

La scheda **Rilevamenti** ti fornisce la struttura per creare e gestire regole di rilevamento personali, indicare un determinato comportamento del tuo ambiente come un rilevamento valido e generare gli incidenti corrispondenti nella pagina Incidenti.



Scheda Rilevamenti

1. Clicca sul pulsante **Crea nuova** per creare una nuova regola di rilevamento personale. Consulta la sezione Crea regole di rilevamento personali per maggiori dettagli.
2. Usa questi pulsanti azione per personalizzare la griglia:
   - Clicca sul pulsante **Mostra/Nascondi colonne** per aggiungere o rimuovere colonne al filtro.

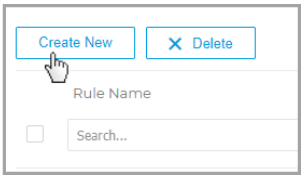
     La pagina si aggiornerà automaticamente, caricando le schede con le informazioni che corrispondono alle colonne aggiunte.

     Puoi sempre reimpostare le colonne di filtro dal pulsante **Reimposta** nel menu a discesa **Mostra/Nascondi colonne**.
   - Clicca sul pulsante **Mostra/Nascondi filtri** per mostrare o nascondere la barra dei filtri.
   - Clicca sul pulsante **Aggiorna** per aggiornare l'elenco.

3. Marca la casella globale o le singole caselle delle regole per selezionarle e clicca su **Elimina** per rimuoverle dall'elenco.
4. Clicca su una regola nell'elenco per espandere il suo pannello dei dettagli, visualizzare i dettagli della regola e aggiornarla o eliminarla, se necessario. Consulta il Pannello dettagli Regola di rilevamento per maggiori dettagli.

Creare regole di rilevamento personali

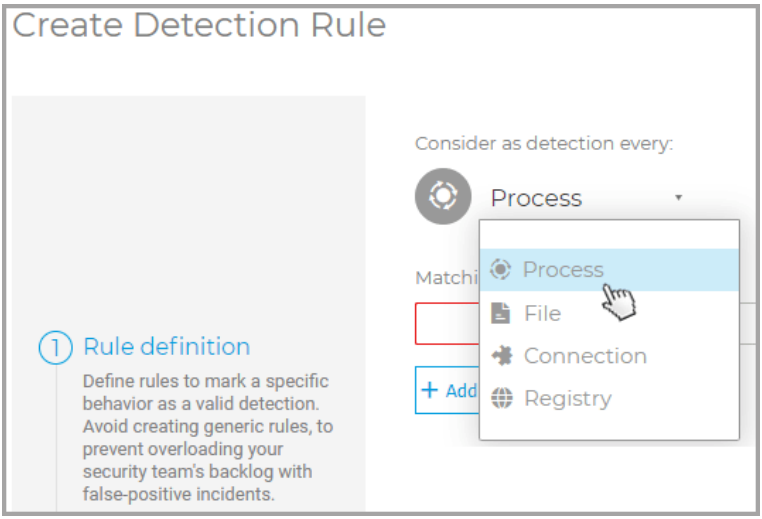
Per creare una regola di rilevamento personale, clicca sul pulsante **Crea nuova**.



Crea una nuova regola di rilevamento

Ti condurrà alla finestra **Crea regola di rilevamento**, nella sezione **Definizione regola**, dove potrai iniziare a modificare la regola:

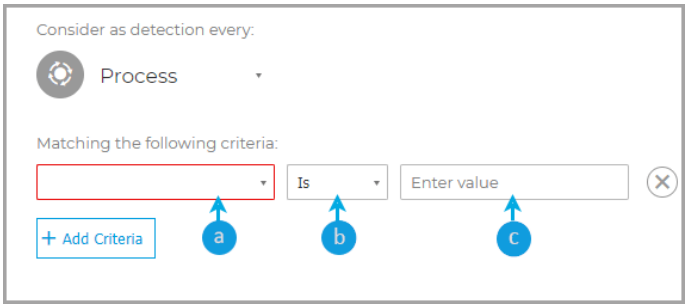
1. Seleziona quale tipo di elemento vuoi includere nella regola di eccezione.



Puoi scegliere tra:

- Processo
- File
- Connessione
- Registro

2. Ogni tipo di elemento ha un determinato criterio di abbinamento che puoi selezionare nel menu a discesa:



a. Seleziona uno dei criteri disponibili.

b. Seleziona il tipo di relazione tra i criteri di abbinamento e il suo valore:

- **È** - Includerà tutti gli incidenti con elementi che corrispondono al valore esatto inserito nel campo del valore.
- **Contiene** - Includerà tutti gli incidenti con elementi che contengono il valore inserito nel campo del valore (per esempio, caratteri jolly, estensioni dei file, ecc.).

  Importante
  Utilizzare caratteri jolly quando si crea una regola di rilevamento aumenta il rischio di renderla troppo generica, incrementando così la possibilità di sovraccaricare il tuo arretrato di lavoro con incidenti relativi a falsi positivi.

- **È uno di** - Includerà tutti gli incidenti con elementi che corrispondono a uno dei valori inseriti nel campo del valore (tra i valori inseriti viene applicato l'operatore **O**).

c. Inserisci il valore specifico per ogni criterio.

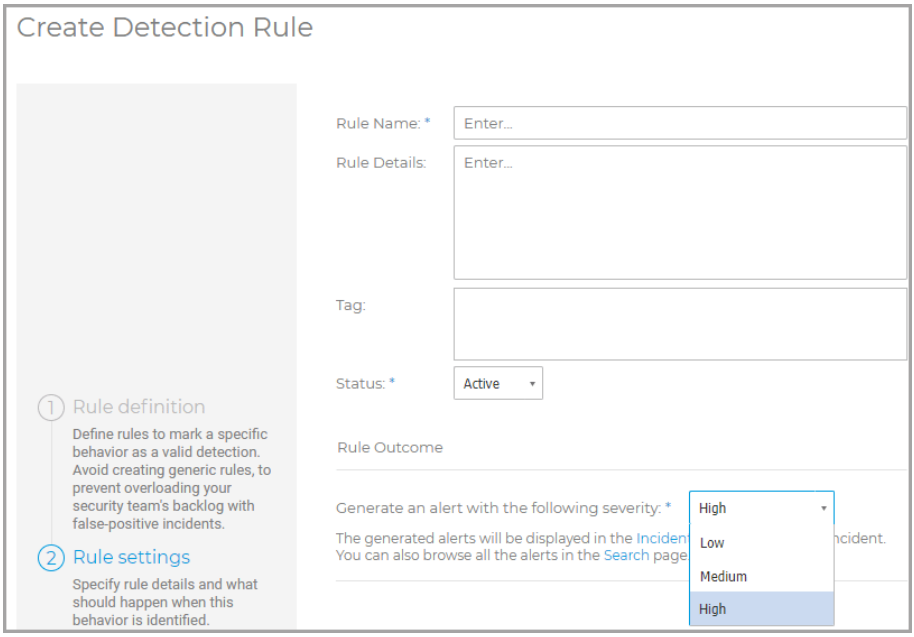
Nota
Inserendo più valori per un criterio (quando si utilizza la condizione **È uno di**), devi premere **Invio** dopo ogni valore per completare l'azione.

3. Usa l'opzione **Aggiungi criterio** per aggiungere un nuovo criterio alla regola.

Nota
La regola attiverà gli incidenti che includono ogni criterio definito (aggiungendo più criteri, tra di essi viene usato l'operatore **E**).

4. Una volta definiti tutti i criteri, clicca su **Prossimo passaggio**.

   Ti porterà alla sezione **Impostazioni regola**, dove dovrai inserire i dettagli della regola.



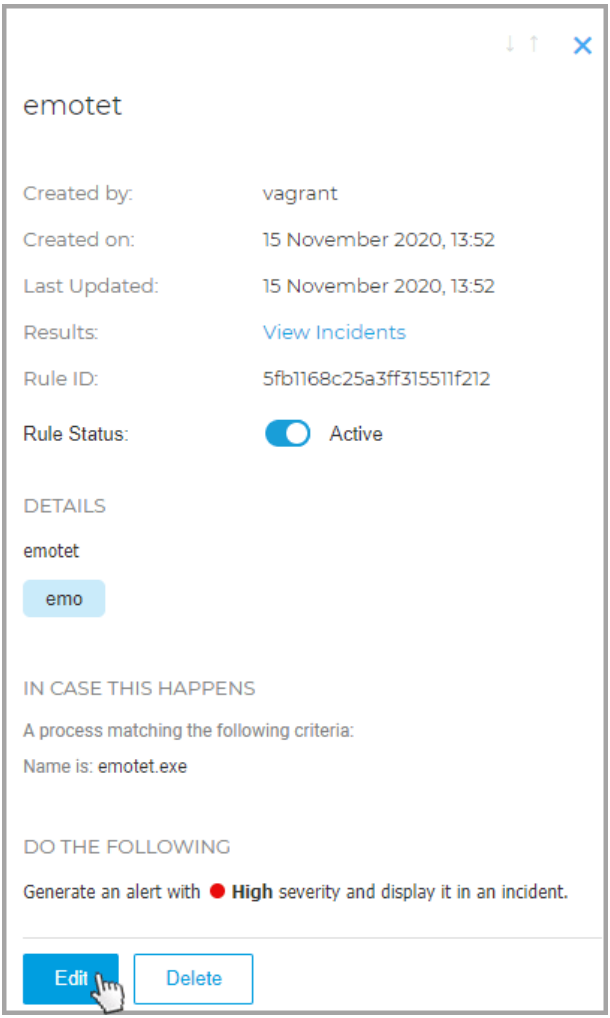
5. Dai un nome alla nuova regola nel campo **Nome della regola**. Il campo è obbligatorio.
6. Aggiungi una breve descrizione della regola nell'area di testo **Dettagli della regola**.
7. Aggiungi determinati tag alla regola nel campo **Tag** per raggrupparle e gestirle più facilmente.
8. Imposta lo stato della regola in Attiva o Inattiva nel menu a discesa **Stato**.

9. Imposta la severità delle allerte attivate da questa regola su Bassa / Media / Alta, nel menu a discesa.
10. Clicca su **Crea regola** per completare la creazione della regola di eccezione personalizzata.

    La nuova regola è disponibile nella scheda **Rilevamenti**.

Pannello dettagli regola di rilevamento

Il pannello **Dettagli regola** include informazioni dettagliate sulla regola selezionata, tra cui la data di creazione e chi l'ha creata, la data dell'ultimo aggiornamento, un ID unico e lo stato, oltre a un link all'elenco degli eventi che corrispondono ai criteri della regola. Include anche una descrizione della regola, i tag associati, i criteri di abbinamento inclusi e l'esito della regola.

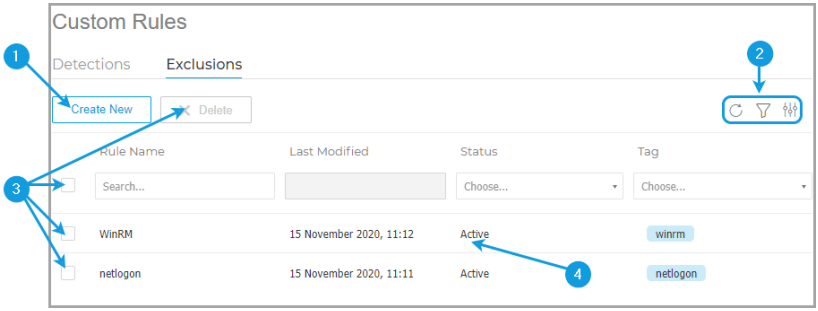


Pannello Dettagli regola

- Clicca su **Modifica** per andare alla finestra **Crea regola di rilevamento**, dove potrai aggiornare la definizione della regola.
- Clicca su **Elimina** per rimuovere la regola di eccezione dall'elenco.

9.4.2. Eccezioni

La scheda **Eccezioni** ti fornisce la struttura per creare e gestire regole di eccezione personalizzate, per escludere incidenti che ritieni irrilevanti per la tua organizzazione, che altrimenti sarebbero normalmente contrassegnati da EDR nella pagina Incidenti.



Scheda Eccezioni

1. Clicca sul pulsante **Crea nuova** per creare una nuova regola di eccezione personalizzata. Consulta la sezione Crea regole delle eccezioni personalizzate per maggiori dettagli.

   In alternativa, puoi sempre creare una regola dal grafico dell'incidente, selezionando un nodo bersaglio e aggiungendolo come eccezione dal pannello dei dettagli laterale. Consulta la funzionalità Aggiungi come eccezione EDR per maggiori dettagli.

2. Usa questi pulsanti azione per personalizzare la griglia:

   - Clicca sul pulsante **Mostra/Nascondi colonne** per aggiungere o rimuovere colonne al filtro.

     La pagina si aggiornerà automaticamente, caricando le schede con le informazioni che corrispondono alle colonne aggiunte.

     Puoi sempre reimpostare le colonne di filtro dal pulsante **Reimposta** nel menu a discesa **Mostra/Nascondi colonne**.

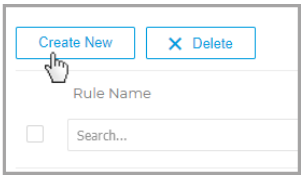
   - Clicca sul pulsante **Mostra/Nascondi filtri** per mostrare o nascondere la barra dei filtri.

   - Clicca sul pulsante **Aggiorna** per aggiornare l'elenco.

3. Marca la casella globale o le singole caselle delle regole per selezionarle e clicca su **Elimina** per rimuoverle dall'elenco.
4. Clicca su una regola nell'elenco per espandere il suo pannello dei dettagli, visualizzare i dettagli della regola e aggiornarla o eliminarla, se necessario. Consulta il Pannello dettagli Regola di eccezione per maggiori dettagli.

Creare regole delle eccezioni personalizzate

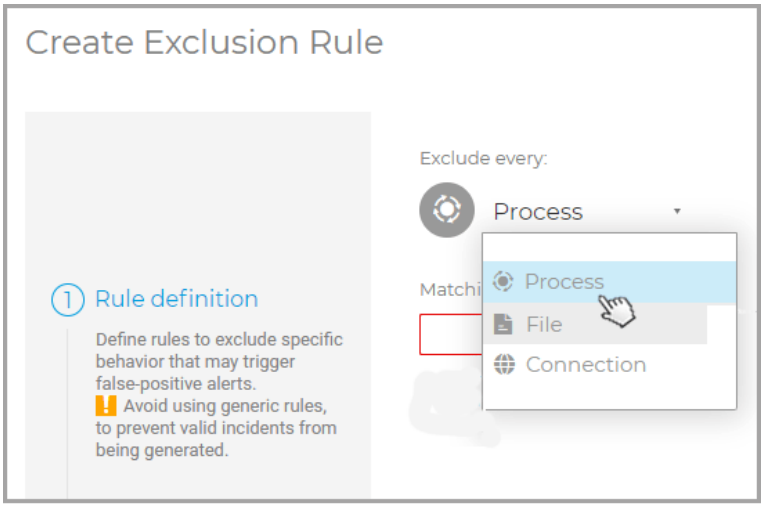
Per creare una regola di eccezione personale, clicca sul pulsante **Crea nuova** nella scheda **Eccezioni**.



Creare una nuova regola di eccezione

Ti condurrà alla pagina **Crea regola di eccezione**, nella sezione **Definizione regola**, dove potrai iniziare a modificare la regola:

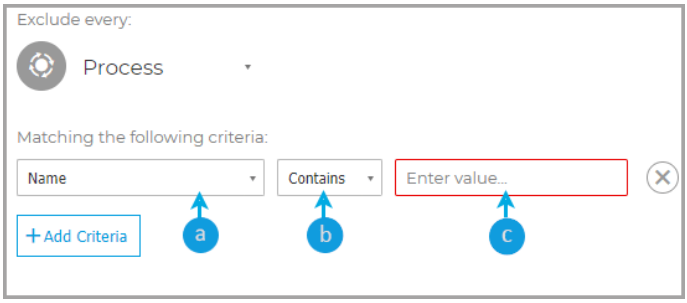
1. Seleziona quale tipo di elemento vuoi includere nella regola di eccezione.



Puoi scegliere tra:

- Processo
- File
- Connessione

2. Ogni tipo di elemento ha un determinato criterio di abbinamento che puoi selezionare nel menu a discesa:



a. Seleziona uno dei criteri disponibili.
b. Seleziona il tipo di relazione tra i criteri di abbinamento e il suo valore:
   - **È** - Escluderà tutti gli incidenti con elementi che corrispondono al valore esatto inserito nel campo del valore.
   - **Contiene** - Escluderà tutti gli incidenti con elementi che contengono il valore inserito nel campo del valore (per esempio, caratteri jolly, estensioni dei file, ecc.).

     Importante
     Utilizzare caratteri jolly quando si crea una regola di eccezione aumenta il rischio di renderla troppo generica, incrementando anche la possibilità di ignorare minacce reali e rendendo così l'azienda più vulnerabile.

   - **È uno di** - Escluderà tutti gli incidenti con elementi che corrispondono a uno dei valori inseriti nel campo del valore (tra i valori inseriti viene applicato l'operatore **O**).
c. Inserisci il valore specifico per ogni criterio.

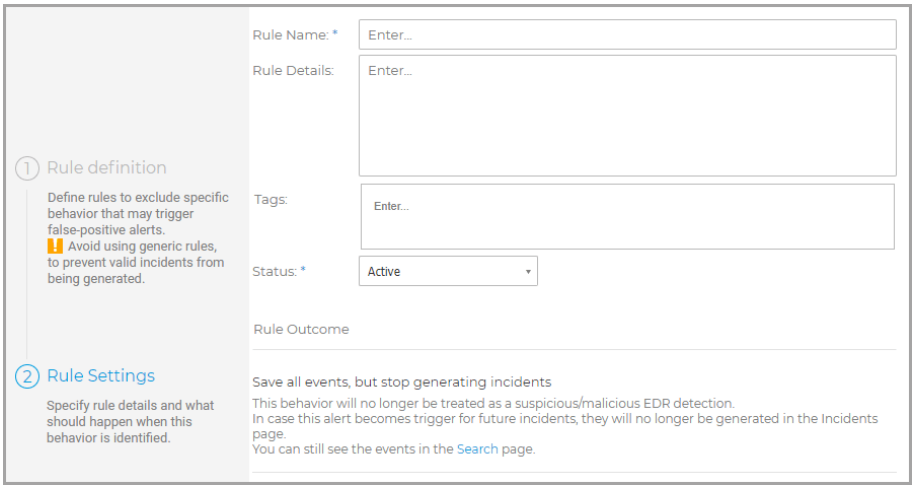
   Nota
   Inserendo più valori per un criterio (quando si utilizza la condizione **È uno di**), devi premere **Invio** dopo ogni valore per completare l'azione.

3. Usa l'opzione **Aggiungi criterio** per aggiungere un nuovo criterio alla regola.

Nota
La regola escluderà gli incidenti che includono ogni criterio definito (aggiungendo più criteri, tra di essi viene usato l'operatore **E**).

4. Una volta definiti tutti i criteri, clicca su **Prossimo passaggio**.

   Ti porterà alla sezione **Impostazioni regola**, dove dovrai inserire i dettagli della regola.

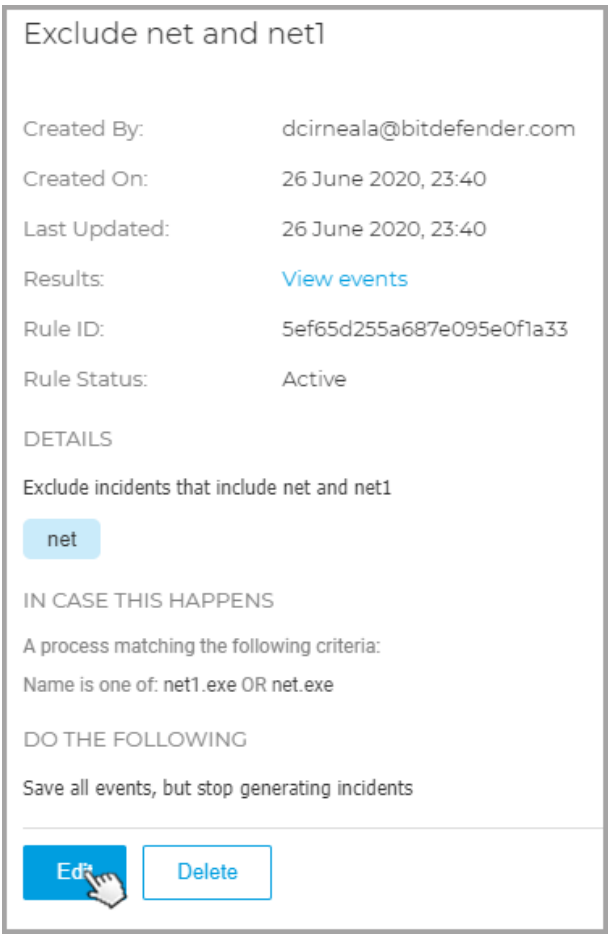


5. Dai un nome alla nuova regola nel campo **Nome della regola**. Il campo è obbligatorio.
6. Aggiungi una breve descrizione della regola nell'area di testo **Dettagli della regola**.
7. Aggiungi determinati tag alla regola nel campo **Tag** per raggrupparle e gestirle più facilmente.
8. Imposta lo stato della regola in Attiva o Inattiva nel menu a discesa *Stato*.
9. Clicca su **Crea regola** per completare la creazione della regola di eccezione personalizzata.

   La nuova regola è disponibile nella pagina **Regole delle eccezioni**.

Pannello dettagli regola di eccezione

Il pannello **Dettagli regola** include informazioni dettagliate sulla regola selezionata, tra cui la data di creazione e chi l'ha creata, la data dell'ultimo aggiornamento, un ID unico e lo stato, oltre a un link all'elenco degli eventi che corrispondono ai criteri della regola. Include anche una descrizione della regola, i tag associati, i criteri di abbinamento inclusi e l'esito della regola.



Pannello Dettagli regola

- Clicca su **Modifica** per andare alla pagina **Crea regola di eccezione**, dove potrai aggiornare la definizione della regola.
- Clicca su **Elimina** per rimuovere la regola di eccezione dall'elenco.

10. GESTIRE I RISCHI DEGLI ENDPOINT

Endpoint Risk Analytics (ERA) ti aiuta a valutare e rafforzare le configurazioni di sicurezza dei tuoi endpoint rispetto alle best practice del settore, in modo da ridurre la superficie d'attacco.

Importante
Il modulo Endpoint Risk Analytics è disponibile solo per i sistemi operativi Windows desktop e server supportati.

ERA raccoglie e analizza i dati tramite le attività di scansione dei rischi eseguite sui dispositivi selezionati nella tua rete.

Per farlo devi prima assicurarti che il modulo ERA sia stato attivato dalla policy applicata ai dispositivi selezionati:

1. Vai alla pagina **Policy**
2. Clicca sul pulsante **Aggiungi** e configura le impostazioni **Generali**.
3. Scorri e seleziona la policy **Gestione rischi**.
4. Seleziona la casella per attivare le funzionalità di **Gestione rischi** e avviare le policy di configurazione che definiscono come eseguire l'attività di **Scansione dei rischi**.

Nota
Per maggiori informazioni sugli indicatori di rischio di GravityZone, fai riferimento a questo articolo della KB.
Per maggiori informazioni sulle vulnerabilità dell'applicazione note, fai riferimento al sito web Dettagli CVE.

Segui questi passaggi per eseguire le attività di scansione dei rischi e valutarne i risultati:

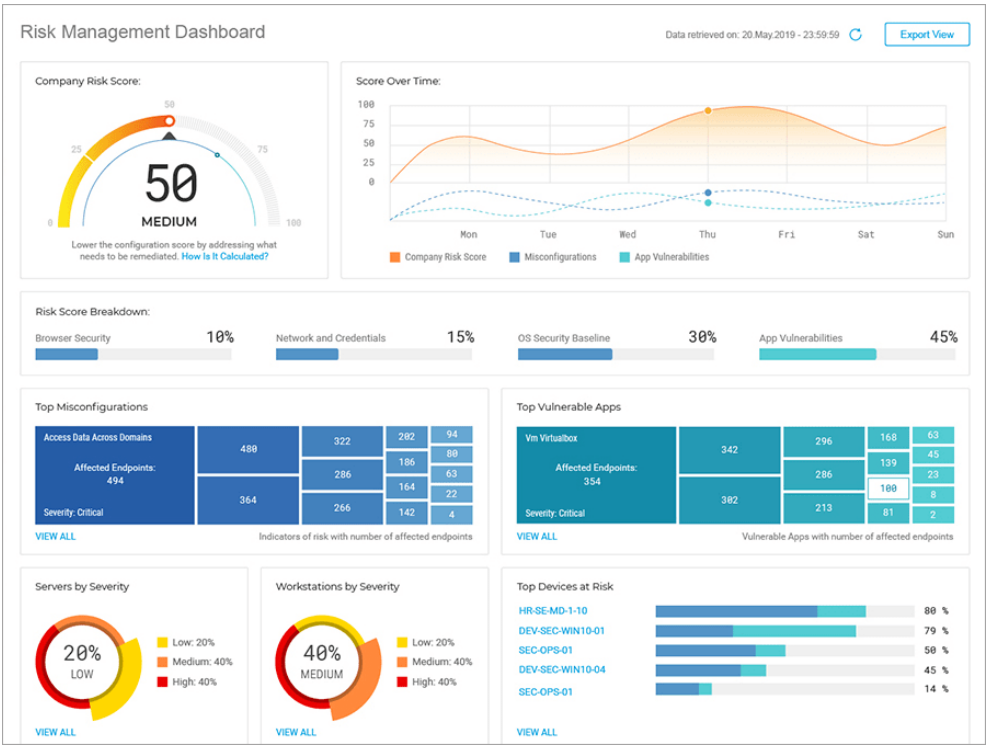
1. Puoi eseguire attività di scansione dei rischi sugli endpoint in due modi:
   a. A richiesta- selezionando gli endpoint dalla pagina **Rete** e inviando un'attività di **Scansione rischi** dal menu **Attività**.
   b. Programmata, configurando dalla policy un'attività di scansione dei rischi che viene eseguita automaticamente sugli endpoint bersaglio a un intervallo stabilito.

Una volta completata la scansione dei rischi, GravityZone calcola un punteggio di rischio per ciascun endpoint..

2. Accedi alla dashboard di **Gestione rischi** per ottenere le seguenti informazioni:
   - Il punteggio di rischio dell'azienda e l'evoluzione del punteggio
   - Statistiche e punteggi di rischio suddivisi in configurazioni errate, applicazioni vulnerabili, rischi umani e dispositivi interessati.
   - La descrizione di ciascun indicatore di rischio e le azioni di rimedio consigliate.
3. Accedi alla pagina Rischi di sicurezza per analizzare e attenuare le configurazioni errate, le vulnerabilità delle applicazioni e i potenziali rischi causati dal comportamento degli utenti trovati.
4. Accedi alla pagina Visuale aziende per una panoramica del punteggio di rischio di tutte le aziende sotto la tua gestione.

10.1. La dashboard di Gestione rischi

La pagina **Gestione rischi** fornisce una panoramica della tua sicurezza di rete e informazioni sulla valutazione dei rischi.



Dashboard gestione rischi

1. Punteggio di rischio azienda
2. Punteggio nel tempo
3. Principali configurazioni errate
4. Principali app vulnerabili
5. Principali rischi umani
6. Server per severità
7. Workstation per severità
8. Principali dispositivi a rischio
9. Principali utenti per comportamento di sicurezza

I dati mostrati in questa pagina sono organizzati in diversi widget:

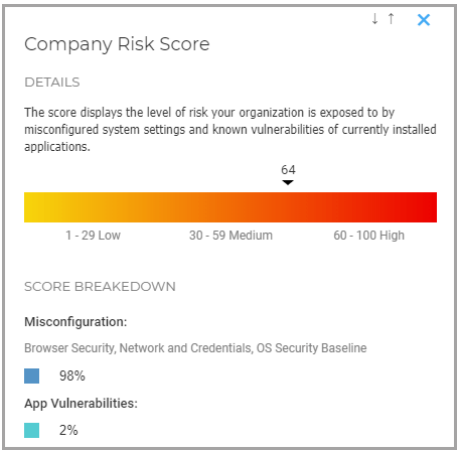
Punteggio di rischio azienda

Il punteggio di rischio globale mostra il livello di rischio a cui è esposta la tua organizzazione per via di impostazioni di sistema errate, vulnerabilità note delle applicazioni attualmente installate e potenziali rischi causati da comportamenti degli utenti. Il punteggio viene regolato dinamicamente dal modificatore settore sanitario, che calcola il rischio causato dalle vulnerabilità delle specifiche app sfruttate per il tuo settore.

Il punteggio rappresenta una media delle tre categorie di rischio principali **Configurazione errata**, **Vulnerabilità app** e **Rischio umano**.

Widget punteggio di rischio azienda

Clicca sul widget e si aprirà un pannello dei dettagli in cui è possibile visualizzare i dettagli su come il rischio globale è stato calcolato e suddiviso in sottocategorie.

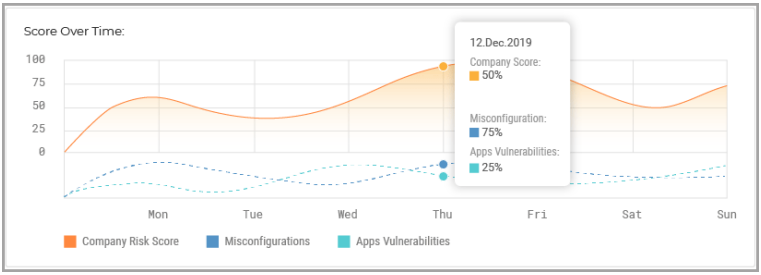


Pannello dettagli punteggio di rischio azienda

Nota
Eseguire una Scansione dei rischi su richiesta su un nuovo dispositivo bersaglio influenzerà il punteggio globale. I risultati saranno mantenuti per 90 giorni o fino alla prossima scansione.

Punteggio nel tempo

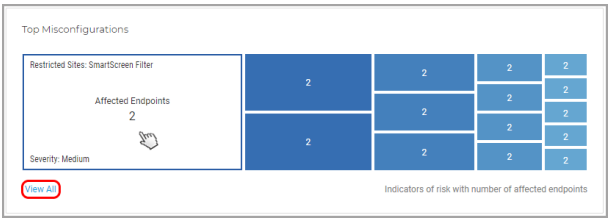
Questo widget è un istogramma che mostra l'evoluzione settimanale del numero di dispositivi interessati rilevati come vulnerabili dopo la scansione dei rischi. I dati dell'istogramma rappresentano il numero di dispositivi interessati da indicatori di rischio negli ultimi sette giorni, fino alle 00:00 (orario del server) del giorno corrente.



Widget punteggio nel tempo

Principali configurazioni errate

Questo widget mostra i primi 15 risultati per gli indicatori che hanno attivato un'allerta di rischio dopo la scansione degli endpoint, ordinati in base al numero di endpoint interessati. Ogni scheda rappresenta un indicatore che ha attivato un'allerta di rischio per almeno un endpoint.



Widget principali configurazioni errate

Ogni scheda mostra i seguenti elementi:

- Il nome dell'indicatore.
- Il numero di dispositivi rilevati come vulnerabili a questo indicatore.
- La severità della configurazione errata.

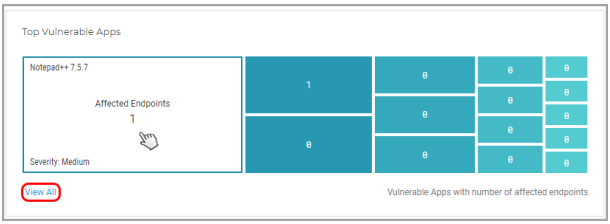
Cliccando sul widget dell'indicatore individuale si aprirà l'indicatore di rischio selezionato nella scheda Configurazioni errate della pagina **Rischi di sicurezza**, dove potrai intraprendere le azioni appropriate per ridurre tale rischio.

Cliccando sul pulsante **Vedi tutto**, visualizzerai l'intero elenco delle configurazioni errate rilevate nella scheda Configurazioni errate della pagina **Rischi di sicurezza**.

Nota
Per maggiori dettagli sulle configurazioni errate, fai riferimento a questo articolo della KB.

Principali app vulnerabili

Questo widget mostra i primi 15 risultati per le vulnerabilità delle applicazioni note che hanno attivato un'allerta di rischio dopo la scansione degli endpoint, ordinati in base al numero di endpoint interessati. Ogni scheda rappresenta un'applicazione vulnerabile che ha attivato un'allerta di rischio per almeno un endpoint.



Widget principali app vulnerabili

Ogni scheda mostra i seguenti elementi:

- Il nome dell'applicazione.
- Il numero di dispositivi reso vulnerabile da questa applicazione.
- La severità per l'applicazione vulnerabile.

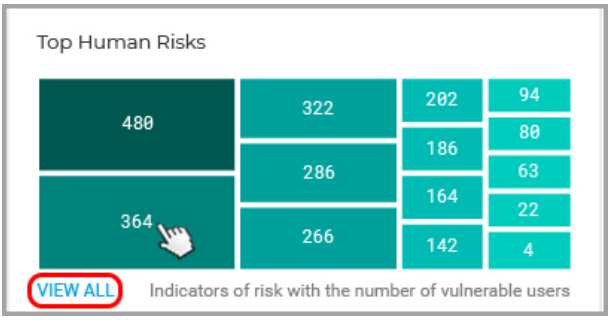
Cliccando sul widget della app individuale si aprirà la vulnerabilità selezionata nella scheda Vulnerabilità app della pagina **Rischi di sicurezza**, dove potrai intraprendere le azioni appropriate per ridurre tale rischio.

Cliccando sul pulsante **Vedi tutto**, visualizzerai l'intero elenco delle vulnerabilità delle applicazioni scoperte nella scheda Vulnerabilità app della pagina **Rischi della sicurezza**.

Nota
Puoi trovare maggiori dettagli sulle vulnerabilità delle applicazioni note nel sito web Dettagli CVE.

Principali rischi umani

Questo widget mostra i migliori 15 risultati per i rischi potenziali causati da un comportamento involontario o incauto di utenti attivi nella tua rete, ordinati in base al numero di utenti vulnerabili. Ogni scheda rappresenta un rischio basato su un comportamento umano e causato da almeno un utente.



Widget migliori rischi umani

Ogni scheda mostra i seguenti elementi:

- Il nome del rischio umano.
- Il numero di utenti il cui comportamento sconsiderato o incauto potrebbe esporre la tua organizzazione.
- La severità per il rischio umano.

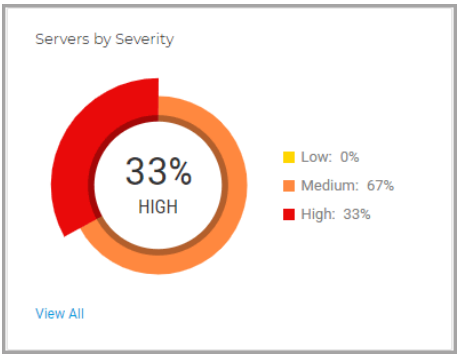
Cliccando sul widget rischio umano individuale si aprirà il rischio selezionato nella scheda Rischi umani della pagina **Rischi di sicurezza**, dove puoi visualizzarlo e analizzarlo nei dettagli.

Cliccando sul pulsante **Vedi tutto**, visualizzerai l'intero elenco di tutti i rischi umani generati dalle attività degli utenti nella scheda Rischi umani della pagina **Rischi di sicurezza**.

Nota
Questa nuova funzionalità ERA è disponibile come versione in anteprima, consentendoti solo di visualizzare i rischi basati sulle attività umane, e ignorandoli se dovessero essere irrilevanti per il tuo ambiente. In un prossimo futuro, la funzionalità sarà migliorata ulteriormente.

Server per severità

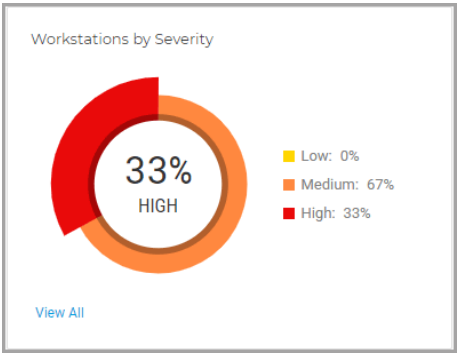
Questo widget mostra la severità dei rischi che minacciano i server nel tuo ambiente. L'impatto delle configurazioni errate e delle vulnerabilità delle applicazioni scoperte viene mostrato con un valore percentuale.



Widget server per severità

Workstation per severità

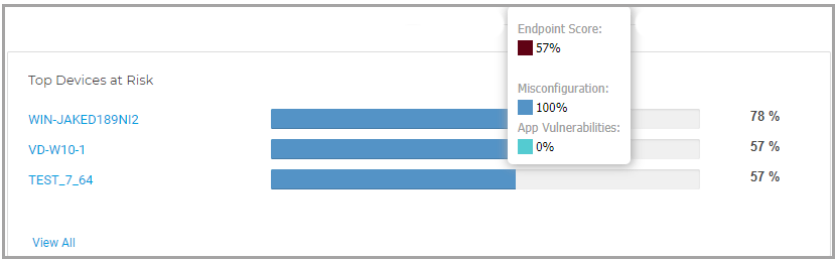
Questo widget mostra la severità dei rischi che minacciano le workstation nel tuo ambiente. L'impatto delle configurazioni errate e delle vulnerabilità delle applicazioni scoperte viene mostrato con un valore percentuale.



Widget workstation per severità

Principali dispositivi a rischio

Questo widget mostra i server e le workstation più vulnerabili nel tuo ambiente, in base al punteggio globale calcolato dopo la scansione per la ricerca di configurazioni errate e vulnerabilità.

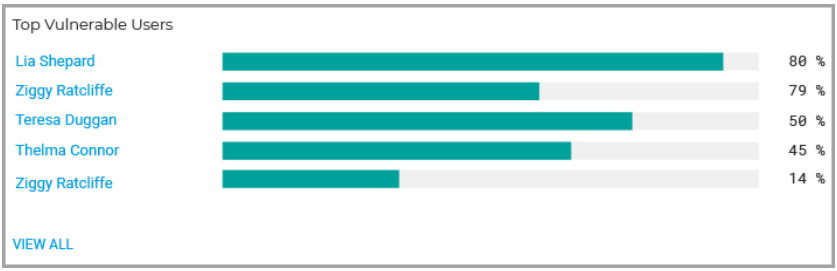


Widget principali dispositivi a rischio

Cliccando sul pulsante **Vedi tutto**, potrai visualizzare l'intero elenco dei dispositivi esposti a potenziali rischi nella scheda Dispositivi della pagina **Rischi di sicurezza**.

Utenti più vulnerabili

Questo widget mostra gli utenti più vulnerabili nel tuo ambiente, in base al punteggio globale calcolato dopo aver analizzato il loro comportamento e attività.

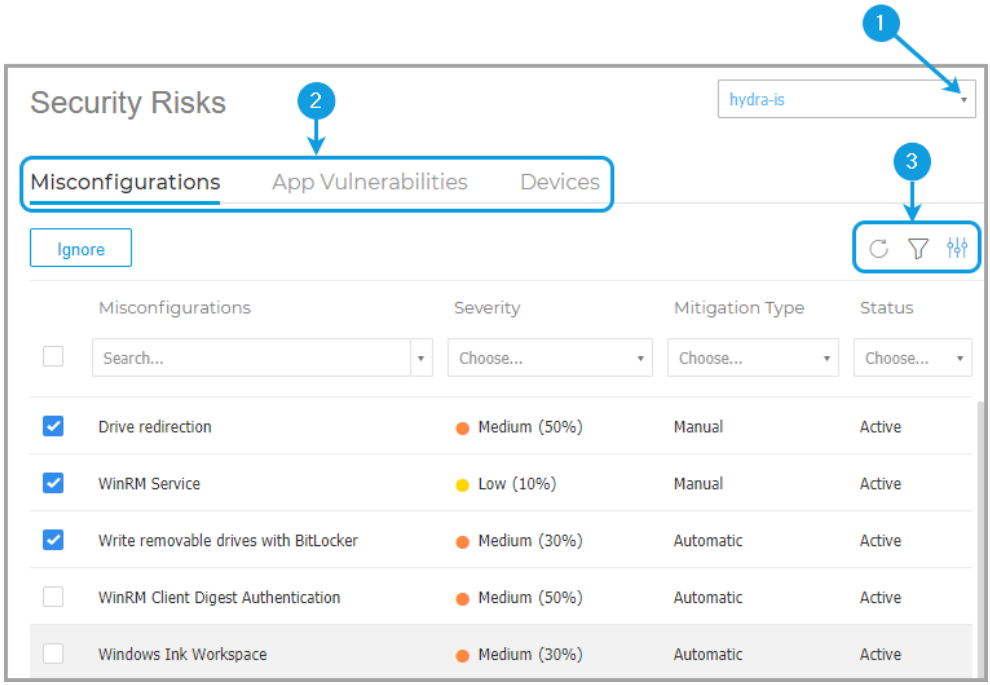


Widget principali utenti vulnerabili

Cliccando sul pulsante **Vedi tutto**, potrai visualizzare l'intero elenco degli utenti che potrebbero aver esposto l'organizzazione a potenziali minacce con il loro comportamento nella scheda Utenti della pagina **Rischi di sicurezza**.

10.2. Rischi per la sicurezza

Questa pagina mostra tutti i rischi, i dispositivi interessati e gli utenti vulnerabili scoperti nel tuo ambiente dopo aver eseguito una **Scansione per i rischi**.



La pagina Rischi per la sicurezza

Gli indicatori di rischio vengono mostrati in una griglia completamente personalizzabile con opzioni di filtro complesse:

1. Seleziona l'azienda sotto la tua gestione per analizzare e mitigare i rischi che possono colpirla.
2. Seleziona quale categoria analizzare:
   - Configurazioni errate
   - Vulnerabilità delle app
   - Rischi umani
   - Dispositivi
   - Utenti

3. Usa questi pulsanti azione per personalizzare la griglia:
   - Clicca sul pulsante **Mostra/Nascondi colonne** per aggiungere o rimuovere colonne al filtro.

     La pagina si aggiornerà automaticamente, caricando le schede degli indicatori di rischio con informazioni che corrispondono alle colonne aggiunte.

     Puoi sempre reimpostare le colonne di filtro dal pulsante **Reimposta** nel menu a discesa **Mostra/Nascondi colonne**.
   - Clicca sul pulsante **Mostra/Nascondi filtri** per mostrare o nascondere la barra dei filtri.
   - Clicca sul pulsante **Aggiorna** per aggiornare l'elenco.

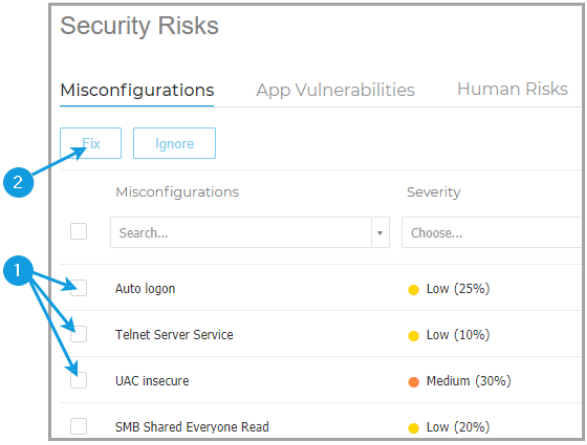
Ogni voce dell'indicatore è elencata in un formato rich card e fornisce una panoramica di ciascun indicatore di rischio, con informazioni basate sui filtri selezionati.

Configurazioni errate

La scheda **Configurazioni errate** mostra in maniera predefinita tutti gli indicatori di rischio di GravityZone. Fornisce informazioni dettagliate sulla loro severità, il numero di dispositivi interessati, il tipo di configurazione errata, il tipo di mitigazione (manuale o automatica) e lo stato (attivo o ignorato).

Per risolvere più configurazioni errate alla volta:

1. Seleziona la casella principale o le singole caselle degli indicatori di rischio per selezionarli.



Risolvere più rischi nella scheda Configurazioni errate

2. Clicca sul pulsante **Risolvi rischi**.

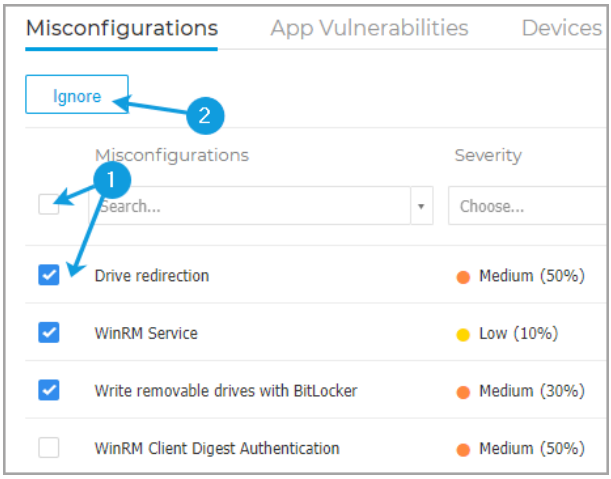
   Viene visualizzata una nuova finestra in cui è necessario confermare l'azione o annullarla.

3. Viene creata una nuova attività per applicare l'impostazione suggerita su tutti i dispositivi interessati.

> **Nota**
> Puoi controllare i progressi dell'attività nella pagina **Rete** > **Attività**.
> Se l'indicatore di rischio può essere mitigato solo manualmente, devi accedere ai dispositivi interessati e applicare la configurazione suggerita.

Per modificare lo stato delle configurazioni errate:

1. Seleziona la casella principale o le singole caselle degli indicatori di rischio per selezionarle per il cambio di stato.



Cambiare lo stato di più rischi nella scheda Configurazioni errate

2. Clicca sul pulsante **Ignora/Ripristina rischi** per cambiare lo stato da **Attivo** a **Ignorato**, o viceversa.

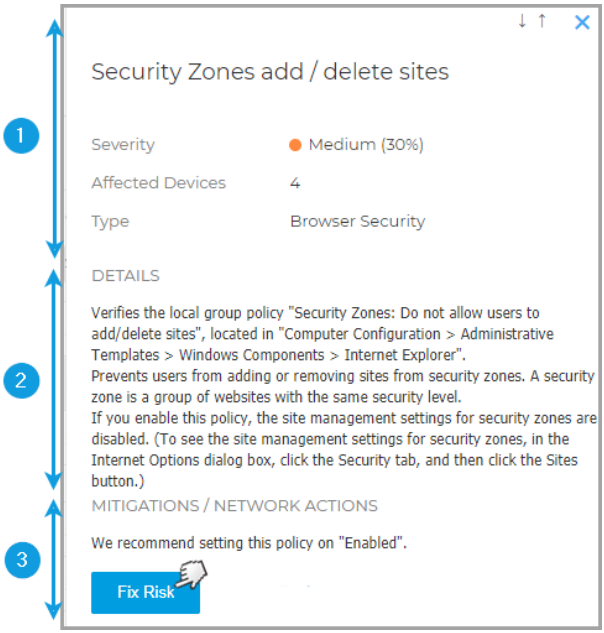
> **Nota**
> L'azione **Ignora rischi** si applica a tutti i dispositivi selezionati e influenza il punteggio di rischio globale dell'azienda all'esecuzione di una nuova scansione dei rischi. Ti consigliamo vivamente di valutare in che modo gli indicatori di rischio ignorati possano influire sulla sicurezza della tua organizzazione.

Puoi personalizzare le informazioni mostrate nelle schede e filtrare le configurazioni errate usando queste opzioni:

Opzioni di filtro	Dettagli
Configurazione errata	Questa colonna include un menu a discesa ricercabile che consente di filtrare l'elenco di indicatori per nome.
Gravità	Questa colonna ti consente di filtrare l'elenco degli indicatori in base al livello di severità di ciascun indicatore di rischio. Puoi scegliere tra Basso, Medio e Alto.

Opzioni di filtro	Dettagli
Dispositivi interessati	Questa colonna mostra il numero di server e workstation che potrebbero essere esposte alle minacce di un determinato indicatore di rischio.
Tipo	Questa colonna ti consente di filtrare l'elenco degli indicatori di rischio in base al loro tipo: • Sicurezza browser • Rete e credenziali • Sicurezza SO
Tipo di mitigazione	Questa colonna ti consente di filtrare l'elenco degli indicatori di rischio che possono essere mitigati manualmente o automaticamente.
Stato	Questa colonna ti consente di filtrare l'elenco degli indicatori di rischio in base al loro stato, Attivo o Ignorato.

Clicca sulla configurazione errata che vuoi analizzare per espandere il suo pannello laterale.



Pannello dei dettagli delle configurazioni errate

Ogni pannello include:

1. Una sezione informativa con il nome dell'indicatore di rischio, il suo livello di severità, il numero di dispositivi interessati e il tipo.
2. Una sezione **Dettagli** che descrive accuratamente le impostazioni e le linee guida della configurazione.
3. Una sezione **Mitigazioni** che include suggerimenti per minimizzare il rischio sui dispositivi interessati, nonché le azioni disponibili:
   a. Clicca sul pulsante **Risolvi rischio** per configurare correttamente tale impostazione.

      Viene visualizzata una nuova finestra in cui è necessario confermare l'azione o annullarla.

   b. Viene creata una nuova attività per applicare l'impostazione suggerita su tutti i dispositivi interessati.

> **Nota**
> Puoi controllare i progressi dell'attività nella pagina **Rete** > **Attività**.
> Se l'indicatore di rischio può essere mitigato solo manualmente, devi accedere ai dispositivi interessati e applicare la configurazione suggerita.

c. Il pulsante **Ignora rischio** cambia lo stato del rischio selezionato da **Attivo** a **Ignorato**.

> **Nota**
> Puoi tornare allo stato attivo in qualsiasi momento desideri, cliccando sul pulsante **Ripristina rischio**.

d. Il pulsante **Vedi dispositivi** ti porta alla scheda Dispositivi per visualizzare tutti i dispositivi interessati attualmente da tale indicatore di rischio.

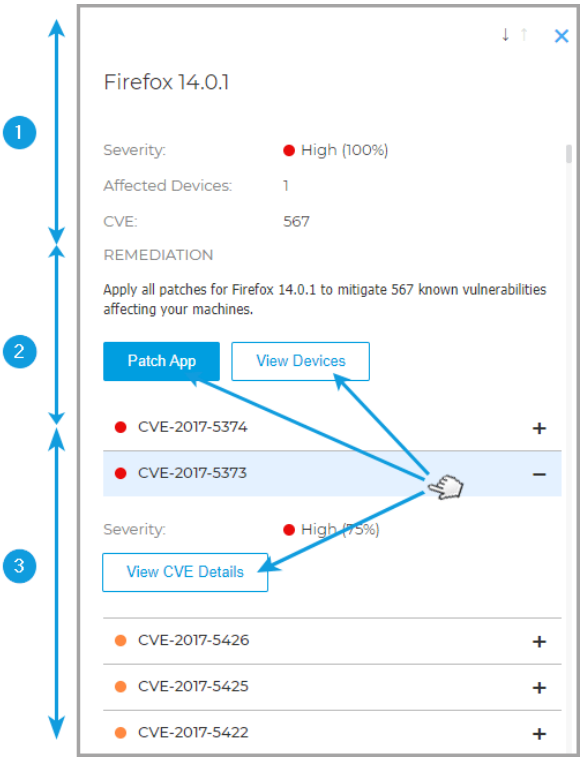
Vulnerabilità delle app

La scheda **Vulnerabilità app** mostra tutte le applicazioni vulnerabili scoperte sui dispositivi nel tuo ambiente durante la scansione. Fornisce informazioni dettagliate sul loro livello di sicurezza, il numero di CVE noti per l'applicazione e il numero di dispositivi interessati.

Puoi personalizzare le informazioni mostrate nelle schede e filtrare le applicazioni vulnerabili usando queste opzioni:

Opzioni di filtro	Dettagli
Applicazioni	Questa colonna include un menu a discesa ricercabile che consente di filtrare l'elenco di applicazioni vulnerabili per nome.
Gravità	Questa colonna ti consente di filtrare l'elenco delle applicazioni vulnerabili in base al livello di severità di ciascuna app. Puoi scegliere tra Basso, Medio e Alto.
CVE	Questa colonna mostra il numero di vulnerabilità ed esposizioni comuni (CVE) per le applicazioni attualmente installate nel tuo ambiente.
Dispositivi interessati	Questa colonna mostra il numero di server e workstation che potrebbero essere esposte alle minacce di un determinato indicatore di rischio.

Clicca sulla app vulnerabile che vuoi analizzare per espandere il suo pannello laterale.



Pannello dei dettagli per le applicazioni vulnerabili

Ogni pannello include:

1. Una sezione di informazioni con il nome dell'applicazione, il livello di severità, quanti dispositivi influenza e a quanti exploit è stato concesso di danneggiare il tuo ambiente.
2. Una sezione **Rimedio** con le azioni di mitigazione e l'elenco dei CVE scoperti:
   a. Clicca sul pulsante **Patcha app** per applicare le patch disponibili per l'applicazione vulnerabili.

Importante
La funzionalità **Patcha app** solo per i dispositivi esaminati che hanno il modulo Gestione patch installato.

Viene visualizzata una nuova finestra in cui è necessario confermare l'azione o annullarla.

b. Una nuova attività sarà creata per applicare le patch alle applicazioni vulnerabili su tutti i dispositivi interessati.

Nota
Puoi controllare i progressi dell'attività nella pagina **Rete** > **Attività**.

c. Il pulsante **Ignora app** cambia lo stato della app selezionata da **Attivo** a **Ignorato**.

Nota
Puoi tornare allo stato attivo in qualsiasi momento desideri, cliccando sul pulsante **Ripristina app**.

3. Espandi i CVE elencati e clicca sul pulsante **Vedi dettagli CVE** per accedere al database con informazioni specifiche.

Rischi umani

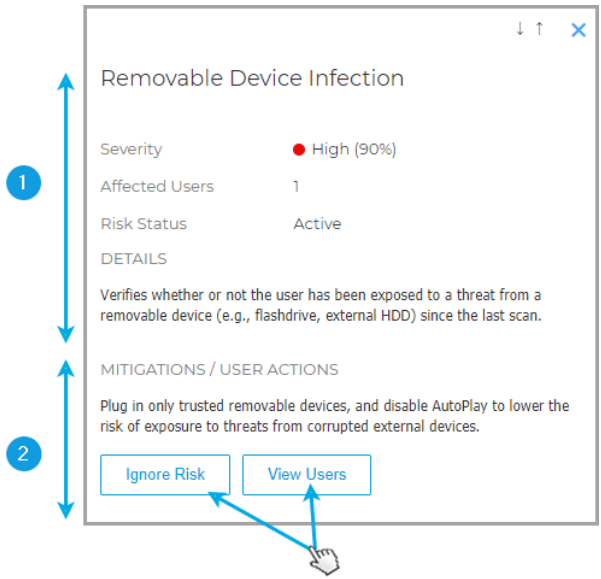
La scheda **Rischi umani** mostra tutti i rischi causati dalle azioni incaute o involontarie degli utenti attivi, o la mancanza di misure intraprese per proteggere adeguatamente le proprie sessioni di lavoro mentre si trovano nella tua rete. Fornisce informazioni dettagliate a livello di severità, numero di utenti vulnerabili, stato e tipologia di rischio.

Nota
Consulta Raccolta dati rischio umano per maggiori dettagli su come vengono elaborati i dati degli utenti.

Puoi personalizzare le informazioni mostrate nelle schede e filtrare i rischi del fattore umano usando queste opzioni:

Opzioni di filtro	Dettagli
Rischi umani	Questa colonna include un menu a discesa ricercabile che consente di filtrare l'elenco di rischi umani per nome.
Gravità	Questa colonna ti consente di filtrare l'elenco dei rischi umani in base al loro livello di severità. Puoi scegliere tra Basso, Medio e Alto.
Utenti vulnerabili	Questa colonna mostra il numero di utenti che causano rischi umani.
Tipo di mitigazione	Questa colonna ti consente di filtrare l'elenco dei rischi che possono essere mitigati manualmente o automaticamente.
Stato	Questa colonna ti consente di filtrare l'elenco dei rischi in base al loro stato, Attivo o Ignorato.

Clicca sul rischio umano che vuoi analizzare per espandere il suo pannello laterale.



Pannello dei dettagli per i rischi umani

Ogni pannello include:

1. Una sezione di informazioni con il nome del rischio, il livello di sicurezza, gli utenti vulnerabili, lo stato del rischio e una descrizione dettagliata del rischio.
2. Una sezione **Mitigazioni/Azioni dell'utente** con le azioni di attenuazione:
   a. Il pulsante **Ignora rischio** cambia lo stato del rischio selezionato da **Attivo** a **Ignorato**.

      Nota
      Puoi tornare allo stato attivo in qualsiasi momento desideri, cliccando sul pulsante **Ripristina rischio**.

   b. L'azione **Vedi utenti** ti porta alla scheda Utenti per visualizzare tutti gli utenti che hanno attivato questo rischio mentre erano attivi nella tua rete.

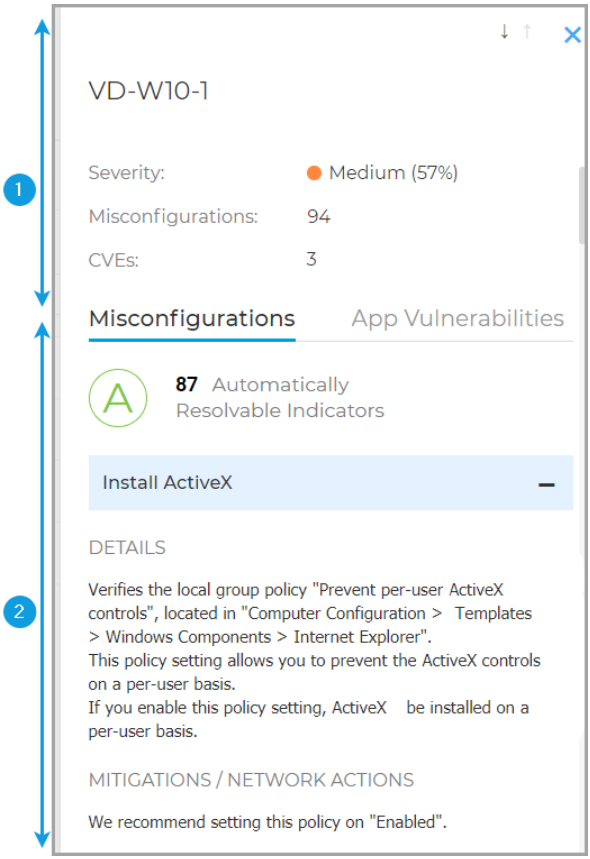
Dispositivi

La scheda **Dispositivi** mostra tutti le workstation e i server esaminati sotto la tua gestione. Fornisce informazioni dettagliate sul proprio nome, livello di sicurezza, tipo di dispositivo e il numero di rischi che li interessano.

Puoi personalizzare le informazioni mostrate nelle schede e filtrare i dispositivi usando queste opzioni:

Opzioni di filtro	Dettagli
Dispositivo	Questa colonna include un menu a discesa ricercabile che consente di filtrare l'elenco di server e workstation vulnerabili per nome.
Gravità	Questa colonna ti consente di filtrare l'elenco dei dispositivi in base al livello di severità che influenza ciascun dispositivo. Puoi scegliere tra Basso, Medio e Alto.
Configurazioni errate	Questa colonna mostra il numero di configurazioni errate scoperte per dispositivo.
CVE	Questa colonna mostra il numero di vulnerabilità ed esposizioni comuni (CVE) scoperti per dispositivo.
Tipo di dispositivo	Questa colonna ti consente di filtrare l'elenco di dispositivi in base al loro tipo. Puoi selezionare tra Server e Workstation.

Clicca sul dispositivo che vuoi analizzare per espandere il suo specifico pannello laterale.



Dettagli pannello per i dispositivi

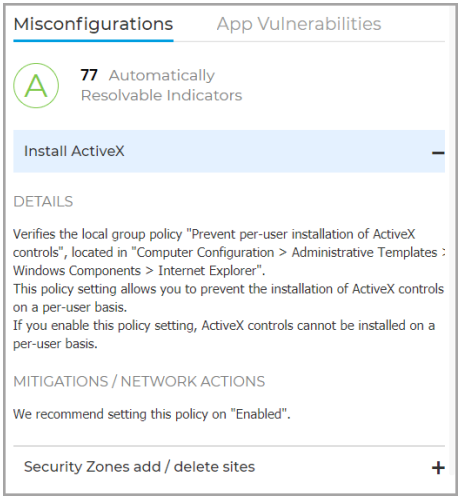
Ogni pannello include:

1. Una sezione informativa con il nome del dispositivo, il livello di severità e il numero di configurazioni errate e vulnerabilità ed esposizioni comuni che lo interessano.

   Il pulsante **Ignora endpoint** cambia lo stato del dispositivo selezionato da **Attivo** a **Ignorato**.

Nota
Puoi tornare allo stato attivo in qualsiasi momento desideri, cliccando sul pulsante **Ripristina endpoint**.

2. Una sezione dei rischi che mostra in dettaglio ogni errata configurazione e le vulnerabilità ed esposizioni comuni scoperte nel dispositivo, raggruppate in due schede.
   - La scheda **Configurazioni errate** include tutte le configurazioni errate scoperte sul dispositivo, raggruppate in indicatori di rischio che possono essere risolti automaticamente e manualmente.



   a. Clicca sul pulsante **Risolvi tutti i rischi** per sistemare tutte le impostazioni e le policy configurate erroneamente che influenzano questo dispositivo.

      Viene visualizzata una nuova finestra in cui è necessario confermare l'azione o annullarla.

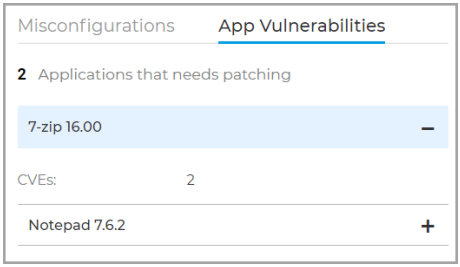
   b. Viene creata una nuova attività per applicare l'impostazione suggerita sul dispositivo interessato.

      Nota
      Puoi controllare i progressi dell'attività nella pagina **Rete** > **Attività**.

Per gli indicatori di rischio che possono essere attenuati sono manualmente, devi accedere al dispositivo interessato e applicare la configurazione suggerita.

Nota
Puoi anche scegliere di investigare separatamente ogni configurazione errata che influenza il dispositivo attuale e risolverle una alla volta utilizzando il pulsante **Risolvi rischio**.

- La scheda **Vulnerabilità app** include tutte le applicazioni vulnerabili scoperte sul dispositivo e il numero di CVE che influenzano ogni applicazione.



a. Clicca sul pulsante **Patcha tutte le app** per applicare le patch disponibili per tutte le applicazioni vulnerabili che espongono il dispositivo selezionato alle minacce.

Importante
La funzionalità **Patcha tutte le app** funziona solo per i dispositivi esaminati che hanno installato il modulo Gestione patch.

Viene visualizzata una nuova finestra in cui è necessario confermare l'azione o annullarla.

b. Sarà creata una nuova attività per applicare le patch alle applicazioni vulnerabili sul dispositivo interessato.

Nota
Puoi controllare i progressi dell'attività nella pagina **Rete** > **Attività**.

Nota
Puoi anche scegliere di investigare separatamente ogni app vulnerabile che influenza il dispositivo attuale e patcharle una alla volta utilizzando il pulsante **Patcha app**.

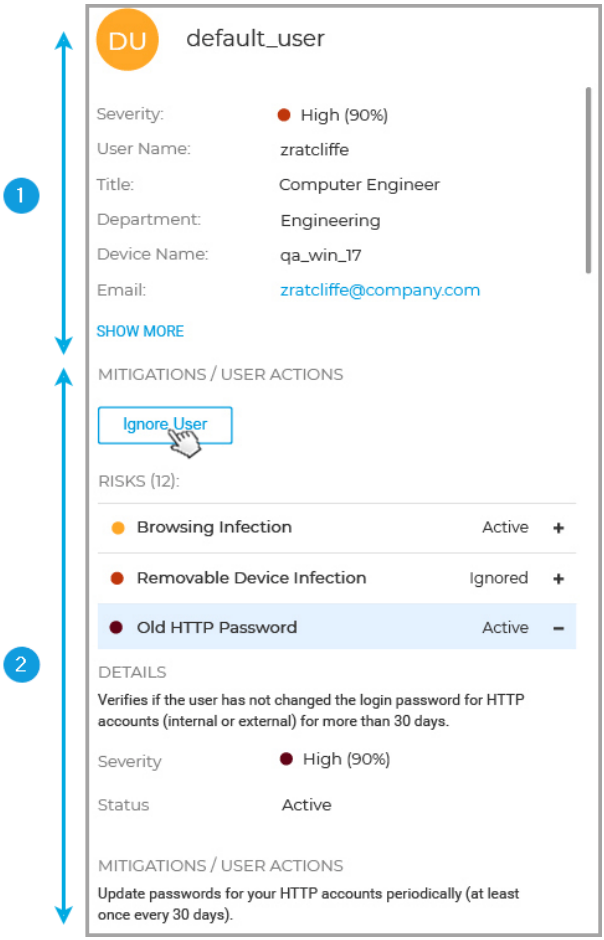
Utenti

La scheda **Utenti** mostra tutti gli utenti che, intenzionalmente oppure no, stanno esponendo il tuo ambiente a delle minacce. Fornisce informazioni quali il nome utente, il livello di severità del rischio globale per quell'utente, il titolo e il dipartimento dell'utente, il numero di rischi a cui sono esposti e il loro stato nel calcolare il rischio aziendale globale.

Puoi personalizzare le informazioni mostrate nelle schede e filtrare i dispositivi usando queste opzioni:

Opzioni di filtro	Dettagli
Utenti	Questa colonna include un campo che consente di filtrare l'elenco degli utenti vulnerabili per nome.
Gravità	Questa colonna ti consente di filtrare l'elenco degli utenti vulnerabili in base al loro livello di severità. Puoi scegliere tra Basso, Medio e Alto.
N. di rischi	Questa colonna mostra il numero di rischi umani che ogni utente sta creando.
Titolo	Questa colonna ti consente di filtrare l'elenco degli utenti in base al loro titolo all'interno dell'organizzazione
Dipartimento	Questa colonna ti consente di filtrare l'elenco degli utenti in base al dipartimento di cui fanno parte nell'organizzazione.
Stato	Questa colonna ti consente di filtrare l'elenco degli utenti in base al loro stato, Attivo o Ignorato.

Clicca sull'utente che vuoi analizzare per espandere il suo specifico pannello laterale.



Dettagli pannello per gli utenti

Ogni pannello include:

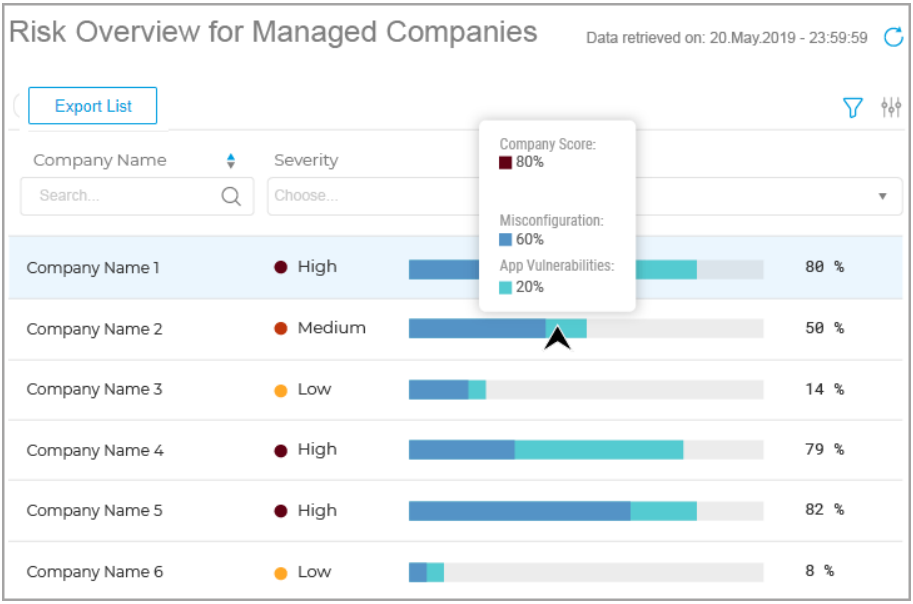
1. Una sezione informativa con il nome dell'utente, il titolo e il dipartimento, le informazioni di contatto, il livello di sicurezza e lo stato.
2. Una sezione **Mitigazioni/Azioni dell'utente** con le azioni di attenuazione:
   a. Il pulsante **Ignora utente** cambia lo stato dell'utente selezionato da **Attivo** a **Ignorato**.

Nota
Puoi tornare allo stato attivo in qualsiasi momento desideri, cliccando sul pulsante **Ripristina utente**.

10.3. Visuale aziende

La pagina **Visuale aziende** fornisce una panoramica del rischio globale per tutte le aziende sotto la tua gestione.

Le aziende con la massima esposizione alle minacce si trovano in cima alla gerarchia dell'elenco, così potrai accedervi facilmente e intraprendere rapidamente tutte le azioni necessarie per rafforzare la loro sicurezza.



La pagina Visuale aziende

Personalizza l'elenco delle aziende gestite usando queste opzioni:

Opzioni di filtro	Dettagli
Nome azienda	Questa colonna include un menu a discesa ricercabile che consente di filtrare l'elenco di aziende per nome.
Gravità	Questa colonna ti consente di filtrare l'elenco delle aziende in base al livello di severità del rischio che le sta interessando. Puoi scegliere tra Basso, Medio e Alto.

Dopo aver personalizzato l'elenco con le aziende sarà semplice accedervi, analizzarne i rischi che le rendono vulnerabili a potenziali minacce e intraprendere azioni:

1. Clicca su un'azienda nell'elenco e raggiungerai l'area della dashboard con i relativi dati.
2. Selezionando un'azienda dall'elenco raggiungerai la sua area della dashboard, viene "compilata" anche la pagina Rischi per la sicurezza, dove potrai analizzare le configurazioni errate, le applicazioni vulnerabili e i dispositivi interessati nell'azienda.
3. Puoi anche esportare l'elenco delle aziende sotto la tua gestione in formato `.csv`.

Nota
La pagina **Visuale aziende** sarà vuota se in precedenza non è stata eseguita alcuna attività di **Scansione dei rischi** per le aziende sotto la tua gestione.

11. UTILIZZARE I RAPPORTI

Control Center ti consente di creare e visualizzare rapporti centralizzati sullo stato di sicurezza degli elementi di rete gestiti. I rapporti possono essere usati per diversi scopi, come:

- Monitorare e assicurare la conformità alle policy di sicurezza dell'organizzazione.
- Controllare e valutare lo stato di sicurezza della rete.
- Identificare problemi, minacce e vulnerabilità di sicurezza della rete.
- Monitorare gli incidenti di sicurezza.
- Fornire una gestione superiore con dati di facile interpretazione sulla sicurezza della rete.

Sono disponibili diversi tipi di rapporto, così da poter ottenere facilmente tutte le informazioni di cui necessiti. Le informazioni vengono presentate con tabelle e diagrammi di facile interpretazione, consentendoti di controllare rapidamente lo stato di sicurezza della rete e individuare eventuali problemi.

I rapporti possono raccogliere i dati dall'intera rete di elementi gestiti o solo da alcuni gruppi specifici. In questo modo, da un singolo rapporto, puoi scoprire:

- Dati statistici relativi a tutti gli elementi di rete gestiti o a gruppi di essi.
- Informazioni dettagliate per ogni elemento di rete gestito.
- L'elenco di computer che soddisfano determinati criteri (per esempio, quelli con la protezione antimalware disattivata).

Alcuni rapporti ti consentono anche di risolvere rapidamente eventuali problemi rilevati nella tua rete. Per esempio, puoi aggiornare facilmente tutti gli elementi di rete bersaglio direttamente dal rapporto, senza dover uscire ed eseguire un'attività di aggiornamento dalla pagina **Rete**.

Tutti i rapporti programmati sono disponibili in Control Center ma puoi salvarli sul computer o inviarli via e-mail.

I formati disponibili includono Portable Document Format (PDF) e comma-separated values (CSV).

11.1. Tipo di rapporto

Per ogni tipo di endpoint sono disponibili diverse tipologie di rapporto:

- Rapporti per computer e virtual machine
- Rapporti Exchange

11.1.1. Rapporti per computer e virtual machine

Questi sono i tipi di rapporto disponibili per macchine virtuali e fisiche:

Attività antiphishing

Ti informa sulle attività del modulo Antiphishing di Bitdefender Endpoint Security Tools. Puoi visualizzare il numero di siti web phishing bloccati sugli endpoint selezionati e l'utente che era collegato al momento dell'ultima rilevazione. Cliccando sui link della colonna **Siti web bloccati**, puoi anche visualizzare gli URL dei siti web, quante volte sono stati bloccati e quando si è verificato l'ultimo evento di blocco.

Applicazioni bloccate

Ti informa sulle attività dei seguenti moduli: Antimalware, Firewall, Controllo contenuti, Anti-exploit avanzato e ATC/IDS. Puoi visualizzare il numero di applicazioni bloccate sugli endpoint selezionati e l'utente che era collegato al momento dell'ultima rilevazione.

Clicca sul numero associato a un bersaglio per visualizzare informazioni aggiuntive sulle applicazioni bloccate, il numero di eventi verificatesi e la data e l'ora dell'ultimo evento di blocco.

In questo rapporto, puoi istruire rapidamente i moduli di protezione per consente all'applicazione selezionata di avviarsi sull'endpoint di destinazione:

Clicca sul pulsante **Aggiungi eccezione** per definire le eccezioni nei seguenti moduli: Antimalware, ATC, Controllo contenuti e Firewall. Comparirà una finestra di conferma, informandoti della nuova regola che modificherà la policy esistente per quel particolare endpoint.

Siti web bloccati

Ti informa sulle attività del modulo Controllo web di Bitdefender Endpoint Security Tools. Per ogni bersaglio, puoi visualizzare il numero di siti web bloccati. Cliccando su questo numero, puoi visualizzare informazioni aggiuntive, come:

- URL del sito web e categoria
- Numero di tentativi di accesso per sito web
- Data e ora dell'ultimo tentativo, oltre all'utente che era collegato al momento della rilevazione.
- Il motivo del blocco, che include accesso programmato, rilevazione malware, filtro categorie e blacklist.

Panoramica stato cliente

Ti aiuta a rilevare problemi di protezione nelle aziende clienti. Un'azienda ha problemi se viene rilevato un malware, l'antimalware è datato o la licenza è scaduta. Il nome dell'azienda è un link a una nuova finestra, in cui potrai trovare i dettagli aziendali.

Protezione dati

Ti informa sulle attività del modulo Protezione dati di Bitdefender Endpoint Security Tools. Puoi visualizzare il numero di e-mail e siti web bloccati sugli endpoint selezionati, oltre all'utente che era collegato al momento dell'ultima rilevazione.

Attività controllo dispositivi

Ti informa sugli eventi verificatisi durante l'accesso agli endpoint tramite i dispositivi monitorati. Per ogni endpoint bersaglio, puoi visualizzare il numero di accessi consentiti / bloccati e gli eventi di sola lettura. Se tali eventi si verificano, sono disponibili ulteriori informazioni cliccando sui numeri corrispondenti. I dettagli fanno riferimento a:

- Utente collegato alla macchina
- ID e tipo di dispositivo
- ID prodotto e fornitore dispositivo
- Data e ora dell'evento.

Stato cifratura endpoint

Ti fornisce dati relativi allo stato di cifratura sugli endpoint. Un diagramma mostra il numero di macchine conformi e non alle impostazioni della policy di cifratura.

Una tabella sottostante il diagramma offre maggiori dettagli, come:

- Nome endpoint.
- Full Qualified Domain Name (FQDN).
- IP della macchina.
- Sistema operativo.
- Conformità policy dispositivo:
  - **Conforme** - Quando i volumi sono tutti cifrati o non cifrati in base alla policy.

- **Non conforme** - Quando lo stato dei volumi non è consistente con la policy assegnata (per esempio, solo uno dei due volumi è cifrato o è in corso un processo di cifratura su quel volume).

- Policy del dispositivo (**Cifratura** o **Decifratura**).
- Clicca sui numeri nella colonna Sommario volumi per visualizzare informazioni sui volumi di ciascun endpoint: ID, nome, stato della cifratura (**Cifrato** o **Non cifrato**), problemi, tipo (**Avvio** o **Non avvio**), dimensione, ID codice di ripristino.
- Nome azienda.

Stato moduli endpoint

Fornisce una panoramica della copertura dei moduli di protezione sui bersagli selezionati. Nei dettagli del rapporto, per ogni endpoint bersaglio puoi visualizzare quali moduli sono attivi, disattivati o non installati, e anche il motore di scansione in uso. Cliccando sul nome dell'endpoint comparirà la finestra **Informazioni** con dettagli sull'endpoint e i livelli di protezione installati.

Cliccando sul pulsante **Riconfigura client**, puoi avviare un'attività per modificare le impostazioni iniziali di uno o più endpoint selezionati. Per maggiori dettagli, fai riferimento a Riconfigura client.

Stato protezione endpoint

Ti fornisce diverse informazioni sullo stato relative agli endpoint selezionati della tua rete.

- Stato protezione antimalware
- Stato aggiornamento Bitdefender Endpoint Security Tools
- Stato attività di rete (online/offline)
- Stato gestione

Puoi applicare filtri per aspetto e stato della sicurezza così da trovare le informazioni che stai cercando.

Attività Firewall

Ti informa sulle attività del modulo Firewall di Bitdefender Endpoint Security Tools. Puoi visualizzare il numero di tentativi di traffico bloccato e i port scan bloccati sugli endpoint selezionati, oltre all'utente che aveva eseguito l'accesso al momento dell'ultimo rilevamento.

Attività HyperDetect

Ti informa sulle attività del modulo HyperDetect di Bitdefender Endpoint Security Tools.

Il grafico nella parte superiore della pagina del rapporto ti mostra le dinamiche dei tentativi di attacco nel periodo di tempo indicato e la loro distribuzione per tipo di attacco. Spostando il mouse sui valori della legenda evidenzierai il relativo tipo di attacco nel grafico. Cliccando sul valore mostrerai o nasconderai la rispettiva linea nel grafico. Cliccando su un punto qualsiasi su una linea filtrerai i dati della tabella in base al tipo selezionato. Per esempio, cliccando su un punto nella linea arancione, la tabella mostrerà solo gli exploit.

I dettagli nella parte inferiore del rapporto consentono di identificare le violazioni nella rete e se sono state risolte. Si riferiscono a:

- Il percorso del file dannoso o l'URL rilevato in caso di file infetti. Per gli attacchi privi di file viene riportato il nome dell'eseguibile usato nell'attacco, con un link a una finestra di dettagli contenente i motivi per cui è stato rilevato e la stringa della riga di comando dannosa.
- L'endpoint su cui è stato fatto il rilevamento
- Il modulo di protezione che ha rilevato la minaccia. Poiché HyperDetect è un livello aggiuntivo dei moduli Antimalware e Controllo contenuti, il rapporto fornirà informazioni su uno di questi moduli, in base al tipo di rilevamento.
- Il tipo di attacco previsto (attacco mirato, grayware, exploit, ransomware, file sospetti e traffico di rete)
- Lo stato della minaccia
- Il livello di protezione del modulo a cui è stata rilevata la minaccia (Permissivo, normale, aggressivo)
- Numero di volte che la minaccia è stata rilevata
- Rilevamento più recente
- Identificazione come attacco privo di file (sì o no), per filtrare rapidamente gli attacchi di questo tipo rilevati

Nota
Un file può essere utilizzato in più tipi di attacchi. Inoltre, GravityZone lo segnala per ogni tipo di attacco in cui è stato coinvolto.

Da questo rapporto, puoi risolvere rapidamente falsi positivi, aggiungendo eccezioni nelle policy di sicurezza assegnate. Per farlo:

1. Seleziona quanti valori nella tabella ti servono.

   Nota
   I rilevamenti di attacchi privi di file non possono essere aggiunti all'elenco delle eccezioni, poiché l'eseguibile rilevato non è di per sé un malware, ma può essere una minaccia utilizzando una linea di comando codificata dannosa.

2. Clicca sul pulsante **Aggiungi eccezione** nel lato superiore della tabella.
3. Nella finestra di configurazione, seleziona le policy a cui deve essere aggiunta l'eccezione, quindi clicca su **Aggiungi**.

   Di norma, le informazioni relative a ogni eccezione aggiunta vengono inviate ai Bitdefender Labs per aiutare a migliorare le capacità di rilevazione dei prodotti Bitdefender. Puoi controllare questa azione utilizzando la casella **Invia questo feedback a Bitdefender per ulteriori analisi**.

Se la minaccia viene rilevata dal modulo Antimalware, l'eccezione sarà applicata sia alla modalità Scansione all'accesso che alla Scansione a richiesta.

Nota
Puoi trovare queste eccezioni nelle seguenti sezioni delle policy selezionate: **Antimalware > Impostazioni** per i file, e **Controllo contenuti > Traffico** per gli URL.

Stato della licenza

Ti informa sulla copertura della protezione di Bitdefender nella tua rete. Vengono forniti dettagli relativi al tipo, l'utilizzo e la durata delle licenze per le aziende selezionate.

Cliccando nel numero nella colonna **Uso**, che corrisponde a un'azienda con licenza mensile, puoi anche visualizzare i dettagli di utilizzo, come il numero totale di posti della licenza e il numero di posti restanti disponibili per l'installazione.

Stato malware

Ti aiuta a scoprire quanti e quali endpoint selezionati sono stati influenzati dai malware in un determinato periodo di tempo e come sono state gestite le minacce. Puoi anche visualizzare l'utente che aveva eseguito l'accesso al momento dell'ultimo rilevamento.

Gli endpoint sono raggruppati in base a questi criteri:

- Endpoint senza rilevazioni (nel periodo indicato non è stata rilevata alcuna minaccia malware)
- Endpoint con malware risolti (tutti i file rilevati sono stati disinfettati o spostati in quarantena con successo)
- Endpoint con malware non risolti (non è stato possibile accedere ad alcuni dei file rilevati)

Per ogni endpoint, cliccando sui link disponibili nelle colonne del risultato della disinfezione, puoi visualizzare l'elenco delle minacce e i percorsi dei file influenzati.

In questo rapporto, puoi eseguire rapidamente un'attività di Scansione completa sui bersagli non risolti, cliccando sul pulsante **Esamina bersagli infetti** dalla barra degli strumenti sopra la tabella dei dati.

Utilizzo licenza mensile

Fornisce informazioni dettagliate sull'utilizzo della licenza per ogni mese, in un determinato periodo di tempo e per le aziende selezionate che usano un abbonamento mensile. Per visualizzare la gerarchia di un'azienda figlia, clicca sul simbolo più di fronte al nome dell'azienda. Se necessario, puoi facilmente modificare i dettagli della licenza, cliccando sul nome dell'azienda.

Il rapporto include informazioni relative a:

- Tipi di azienda
- Codici licenza
- Endpoint con licenza
- Uso endpoint
- Uso cifratura
- Uso Gestione patch
- Uso Security for Virtualized Environments (desktop e server virtuali)
- Uso Advanced Threat Security (HyperDetect e Sandbox Analyzer)
- Uso EDR
- Posti riservati
- Data di fine abbonamento
- Rinnovo automatico abbonamento
- Utilizzo minimo

Clicca sui numeri in ciascuna colonna per visualizzare maggiori dettagli su ogni modulo e add-on disponibile. Puoi anche facilmente personalizzare il rapporto cliccando sul pulsante **Mostra/Nascondi colonne**.

Email Security - Uso licenza mensile

Questo rapporto fornisce informazioni sull'uso della licenza per il servizio Email Security. Tutti gli intervalli del rapporto recuperano informazioni sull'uso della licenza fino alla fine del giorno precedente. Per esempio, puoi generare un rapporto lunedì alle 12:00 e impostare l'intervallo in **Questo mese**. Il rapporto fornirà informazioni sull'uso della licenza fino al termine della domenica.

Incidenti di rete

Ti informa sulle attività del modulo Network Attack Defense. Un grafico mostra il numero di tentativi di attacco rilevato in un determinato intervallo. I dettagli del rapporto includono:

- Nome endpoint, IP e FQDN
- Utente
- Nome rilevato
- Tecnica di attacco
- Numero di tentativi
- IP dell'aggressore
- IP colpito e porta
- Quando l'attacco è stato bloccato più di recente

Cliccando sul pulsante **Aggiungi eccezioni** per un determinato rilevamento, si crea automaticamente un valore in **Eccezioni globali** nella sezione **Protezione rete**.

Stato patch rete

Controlla lo stato dell'aggiornamento del software che è stato installato nella tua rete. Il rapporto svela i seguenti dettagli:

- Macchina obiettivo (nome endpoint, IP e sistema operativo).
- Patch di sicurezza (patch installate, patch fallite, patch di sicurezza e non mancanti).
- Stato e ultima modifica per gli endpoint controllati.

Stato protezione rete

Ti fornisce informazioni dettagliate sullo stato della sicurezza generale degli endpoint bersaglio. Ad esempio, puoi vedere informazioni su:

- Nome, IP e FQDN

- Stato:
  - **Ha problemi** - L'endpoint ha delle vulnerabilità nella protezione (agente di sicurezza non aggiornato, minacce alla sicurezza rilevate, ecc.)
  - **Nessun problema** - L'endpoint è protetto e non ci sono motivi di preoccupazione.
  - **Sconosciuto** - L'endpoint era offline quando il rapporto è stato generato.
  - **Non gestito** - L'agente di sicurezza non è ancora stato installato sull'endpoint.
- Livelli di protezione disponibili
- Endpoint gestiti e non gestiti (l'agente di sicurezza è installato oppure no)
- Tipo e stato della licenza (per impostazione predefinita, le colonne aggiuntive relative alla licenza sono nascoste)
- Stato dell'infezione (l'endpoint è "pulito" oppure no)
- Stato di aggiornamento del prodotto e del contenuto di sicurezza
- Stato delle patch di sicurezza dei software (patch mancanti, di sicurezza o differenti)

Per gli endpoint non gestiti, vedrai lo stato **Non gestito** sotto altre colonne.

Scansione a richiesta

Fornisce informazioni relative alle scansioni a richiesta eseguite sui bersagli selezionati. Un diagramma mostra le statistiche delle scansioni fallite e avvenute con successo. La tabella sotto il diagramma fornisce maggiori dettagli sul tipo di scansione, la frequenza e l'ultima scansione avvenuta con successo per ciascun endpoint.

Conformità policy

Fornisce informazioni relative alle policy di sicurezza applicate ai bersagli selezionati. Un diagramma che mostra lo stato della policy. Nella tabella sotto il diagramma, puoi visualizzare la policy assegnata su ciascun endpoint e il tipo di policy, oltre alla data e all'utente che l'ha assegnata.

Invii non riusciti di Sandbox Analyzer

Mostra tutti gli invii di elementi falliti inviati dagli endpoint a Sandbox Analyzer in un determinato periodo di tempo. Un invio viene considerato fallito dopo diversi tentativi.

Il grafico mostra la variazione degli invii falliti durante il periodo selezionato, mentre nella tabella dei dettagli del rapporto è possibile visualizzare quali file possono essere inviati a Sandbox Analyzer, la macchina da cui l'elemento è stato inviato, la data e l'ora di ogni tentativo, il codice di errore ricevuto, la descrizione di ogni tentativo fallito e il nome dell'azienda.

Risultati di Sandbox Analyzer (deprecati)

Ti fornisce informazioni dettagliate relative ai file sugli endpoint bersaglio, che sono stati analizzati nel sandbox nel corso di un determinato periodo di tempo. Un grafico a linea mostra il numero di file puliti o pericolosi analizzati, mentre la tabella ti offre alcuni dettagli su ciascun caso.

Puoi generare un rapporto dei risultati di Sandbox Analyzer per tutti i file analizzati o solo per quelli rilevati come dannosi.

Puoi visualizzare:

- Il verdetto dell'analisi, che indica se il file è pulito, pericoloso o sconosciuto (**Minaccia rilevata** / **Nessuna minaccia rilevata** / **Non supportata**). Questa colonna compare solo quando selezioni il rapporto per visualizzare tutti gli elementi analizzati.

  Per visualizzare l'elenco completo delle estensioni e dei tipi di file supportati da Sandbox Analyzer, fai riferimento a «Estensioni e tipi di file supportati per l'invio manuale» (p. 461).
- Tipo di minaccia, come adware, rootkit, downloader, exploit, host-modifier, strumenti dannosi, ladri di password, ransomware, spam o Trojan.
- Data e ora del rilevamento, che puoi filtrare in base al periodo del rapporto.
- Il nome dell'host o l'IP dell'endpoint in cui il file è stato rilevato.
- Il nome dei file, se sono stati inviati individualmente o il numero di file analizzati in caso di un pacchetto. Clicca sul nome del file o il link del bundle per visualizzare i dettagli e le azioni intraprese.
- Lo stato dell'azione di risanamento per i file inviati (**Parziale**, **Fallito**, **Solo segnalato**, **Avvenuto con successo**).
- Nome azienda.
- Maggiori informazioni sulle proprietà del file analizzato sono disponibili cliccando sul pulsante **Leggi altro** nella colonna **Risultato analisi**. Qui puoi visualizzare approfondimenti sulla sicurezza e rapporti dettagliati sul comportamento del campione.

Sandbox Analyzer cattura i seguenti eventi comportamentali:

- Scrittura / eliminazione / spostamento / duplicazione / sostituzione dei file sul sistema e su unità rimovibili.

- Esecuzione di file appena creati.
- Modifiche al file di sistema.
- Modifiche alle applicazioni in esecuzione nella virtual machine.
- Modifiche alla barra delle applicazioni di Windows e al menu Start.
- Creazione / conclusione / inserimento processi.
- Scrittura / eliminazione chiavi del registro.
- Creazione di oggetti mutex.
- Creazione / esecuzione / blocco / modifica / interrogazione / eliminazione di servizi.
- Modificare le impostazioni di sicurezza del browser.
- Modificare le impostazioni di visualizzazione di Windows Explorer.
- Aggiungere file all'elenco delle eccezioni del firewall.
- Modificare le impostazioni della rete.
- Attivare l'esecuzione all'avvio del sistema.
- Connessione a un host remoto.
- Accesso a determinati domini.
- Trasferimento dati a e da determinati domini.
- Accesso a URL, IP e porte tramite diversi protocolli di comunicazione.
- Verifica degli indicatori dell'ambiente virtuale.
- Verifica degli indicatori degli strumenti di monitoraggio.
- Creazione di istantanee
- Hook SSDT, IDT, IRP.
- Dump di memoria per processi sospetti.
- Chiamate di funzioni API di Windows.
- Disattivazione per un determinato periodo di tempo per ritardare l'esecuzione.
- Creazione di file con azioni da eseguire in determinati intervalli di tempo.

Nella finestra **Risultato analisi**, clicca sul pulsante **Scarica** per salvare i contenuti del Riepilogo comportamento nei seguenti formati: XML, HTML, JSON, PDF.

Questo rapporto continuerà a essere supportato per un numero limitato di volte. Invece si consiglia di usare le schede di invio per raccogliere le informazioni necessarie sui campioni analizzati. Le schede di invio sono disponibili nella sezione **Sandbox Analyzer**, nel menu principale di Control Center.

Verifica sicurezza

Fornisce informazioni sugli eventi di sicurezza che si sono verificati su un bersaglio selezionato. Le informazioni fanno riferimento ai seguenti eventi:

- Rilevamento malware
- Applicazione bloccata
- Porta di scansione bloccata
- Traffico bloccato
- Sito web bloccato
- Blocca dispositivo
- E-mail bloccata
- Processo bloccato
- Eventi dell'Anti-exploit avanzato
- Eventi di Network Attack Defense
- Rilevamento ransomware

Stato Security Server

Ti aiuta a valutare lo stato del bersaglio del Security Server. Puoi identificare i problemi che ogni Security Server potrebbe avere, con l'aiuto di diversi indicatori di stato, come:

- **Stato**: mostra lo stato generale del Security Server.
- **Stato della macchina**: indica quali appliance del Security Server sono state bloccate.
- **Stato AV**: segnala se il modulo Antimalware è stato attivato o disattivato.
- **Stato aggiornamento**: mostra se le appliance del Security Server sono aggiornato o se gli aggiornamenti sono stati disattivati.
- **Stato del carico**: indica il livello di carico della scansione di un Security Server, come descritto di seguito:
  - **Sottocarico**, quando viene usata meno del 5% della sua capacità di scansione.
  - **Normale**, quando il carico della scansione è bilanciato.
  - **Sovraccarico**, quando il carico della scansione supera il 90% della sua capacità. In tal caso, controlla le policy di sicurezza. Se tutti i Security Server assegnati in una policy sono sovraccaricati, dovrai aggiungere un altro Security Server all'elenco. Diversamente, controlla la connessione di rete tra i client e i Security Server senza problemi di carico.

Puoi anche visualizzare quanti agenti sono connessi al Security Server. Inoltre, cliccando sul numero di client connessi sarà mostrato l'elenco degli endpoint. Questi endpoint potrebbero essere vulnerabili se il Security Server ha problemi.

Top 10 malware rilevati

Ti mostra le 10 principali minacce malware rilevate in un determinato periodo di tempo sugli endpoint selezionati.

> **Nota**
> La tabella dei dettagli mostra tutti gli endpoint che sono stati infettati dai 10 principali malware rilevati.

Top 10 aziende infettate

Ti mostra le 10 aziende più infettate, in base alla tua selezione, tramite il numero di rilevamenti totali in un determinato periodo di tempo.

Top 10 endpoint infettati

Ti mostra i 10 endpoint più infettati in base al numero totale di rilevazioni in un determinato periodo di tempo tra gli endpoint selezionati.

> **Nota**
> La tabella dei dettagli mostra tutti i malware rilevati nei 10 principali endpoint infetti.

Stato dell'Aggiornamento

Ti mostra lo stato di aggiornamento dell'agente di sicurezza o del Security Server installati sui bersagli selezionati. Lo stato di aggiornamento si riferisce alle versioni del prodotto e del contenuto di sicurezza.

Utilizzando i filtri disponibili, puoi facilmente scoprire quali client sono stati aggiornati e quali no nelle ultime 24 ore.

In questo rapporto, puoi rapidamente portare gli agenti alla versione più recente. Per farlo, clicca sul pulsante **Aggiorna** dalla barra degli strumenti sopra la tabella dei dati.

Stato aggiornamento

Ti mostra gli agenti di sicurezza installati sui bersagli selezionati e se è disponibile oppure no una soluzione più recente.

Per gli endpoint con agenti di sicurezza più datati installati, puoi rapidamente installare l'agente di sicurezza supportato più recente cliccando sul pulsante

Aggiorna. Questa operazione è possibile solo se tutti i bersagli sono della stessa azienda.

> **Nota**
> Questo rapporto è disponibile solo quando è stato reso disponibile un upgrade della soluzione GravityZone.

Attività ransomware

Ti informa sugli attacchi ransomware che GravityZone ha rilevato sugli endpoint che gestisci e ti fornisce gli strumenti necessari per ripristinare i file interessati dagli attacchi.

Il rapporto è disponibile come una pagina in Control Center, distinto dalle altre segnalazioni e accessibile direttamente dal menu principale di GravityZone.

La pagina **Attività ransomware** è costituita da una griglia che, per ogni attacco ransomware, elenca i seguenti dati:

- Il nome, l'indirizzo IP e il FQDN dell'endpoint in cui è avvenuto l'attacco
- L'azienda a cui appartengono gli endpoint
- Il nome dell'utente che ha effettuato l'accesso durante l'attacco
- Il tipo di attacco, rispettivamente uno in locale o remoto
- Il processo in cui è stato eseguito il ransomware per gli attacchi locali o l'indirizzo IP da cui è stato avviato l'attacco per quelli remoti
- Data e ora del rilevamento
- Numero di file cifrati finché l'attacco è stato bloccato
- Lo stato dell'azione di ripristino per tutti i file sull'endpoint bersaglio

Di norma, alcuni dettagli sono nascosti. Clicca sul pulsante **Mostra/Nascondi colonne** nella parte in alto a destra della pagina per configurare i dettagli che vuoi visualizzare nella griglia. Se hai troppe voci nella griglia, puoi scegliere di nascondere i filtri usando il pulsante **Mostra/Nascondi filtri** nella parte in alto a destra della pagina.

Sono disponibili ulteriori informazioni cliccando sul numero per i file. Puoi visualizzare un elenco con l'intero percorso ai file originali e ripristinati, e lo stato di ripristino per tutti i file coinvolti nell'attacco ransomware selezionato.

Importante
Le copie di backup sono disponibili per un massimo di 30 giorni. Cerca di ricordarti la data e l'ora fino a cui i file potranno ancora essere ripristinati.

Per ripristinare i file dal ransomware:

1. Seleziona gli attacchi che desideri nella griglia.
2. Clicca sul pulsante **Ripristina file**. Comparirà una finestra di conferma.

   Sarà creata un'attività di ripristino. Puoi controllarne lo stato nella pagina **Attività**, proprio come per qualsiasi altra attività in GravityZone.

Se i rilevamenti sono il risultato dei processi legittimi, segui questi passaggi:

1. Seleziona le voci nella griglia.
2. Clicca sul pulsante **Aggiungi eccezione**.
3. Nella nuova finestra, seleziona le policy a cui applicare l'eccezione.
4. Clicca su **Add** (Aggiungi).

   applicherà tutte le possibili eccezioni: sulla cartella, sul processo e sull'indirizzo IP.

   Puoi controllarle o modificarle nella sezione della policy **Antimalware > Impostazioni > Eccezioni personali**.

Nota
Attività ransomware tiene traccia degli eventi per due anni.

11.1.2. Rapporti server Exchange

Si tratta dei tipi di rapporto disponibili per i server Exchange:

Exchange - Contenuti e allegati bloccati
Ti fornisce informazioni su email o allegati che il Controllo contenuti ha eliminato dai server selezionati durante un determinato intervallo di tempo. Le informazioni includono:

- Gli indirizzi email del mittente e dei destinatari.

  Quando l'email ha più destinatari, invece degli indirizzi email, il rapporto mostra il numero di destinatari con un link a una finestra contenente l'elenco degli indirizzi email.
- Oggetto e-mail.

- Il tipo di rilevamento, indicando quale filtro del Controllo contenuti ha rilevato la minaccia.
- L'azione intrapresa sul rilevamento.
- Il server in cui la minaccia è stata rilevata.
- L'azienda che possiede il server mail.

Exchange - Allegati non esaminabili bloccati

Ti fornisce informazioni sulle email contenenti allegati non esaminabili (super-compressi, protetti da password, ecc.), bloccati sui server mail Exchange in un determinato periodo di tempo. Le informazioni fanno riferimento a:

- Gli indirizzi email del mittente e dei destinatari.

  Quando l'email viene inviata a più destinatari, invece degli indirizzi email, il rapporto mostra il numero di destinatari con un link a una finestra contenente l'elenco degli indirizzi email.
- Oggetto e-mail.
- Le azioni intraprese per rimuovere gli allegati non esaminabili:
  - **Email eliminata**, indicando che l'intera email è stata rimossa.
  - **Allegati eliminati**, un termine generico per tutte le azioni che rimuovono allegati da un messaggio email, come eliminare l'allegato, metterlo in quarantena o sostituirlo con un avviso.

  Cliccando sul link nella colonna **Azione**, puoi visualizzare maggiori dettagli su ogni allegato bloccato e la corrispondente azione intrapresa.
- Data e ora di rilevamento.
- Il server in cui l'email è stata rilevata.
- L'azienda che possiede il server mail.

Exchange - Attività scansione e-mail

Mostra statistiche sulle azioni intraprese dal modulo Protezione Exchange in un determinato intervallo di tempo.

Le azioni sono raggruppate per tipo di rilevamento (malware, spam, allegato vietato e contenuti vietati) e server.

Le statistiche fanno riferimento ai seguenti stati dell'email:

- **In quarantena.** Queste email sono state messe nella cartella Quarantena.

- **Eliminate/Respinte.** Queste email sono state eliminate o respinte dal server.
- **Reindirizzate.** Queste e-mail sono state reindirizzate all'indirizzo e-mail indicato nella policy.
- **Pulite e consegnate.** Queste email sono state ripulite dalle minacce e successivamente passate attraverso i filtri.

  Un'email viene considerata come pulita quando tutti gli allegati rilevati sono stati disinfettati, messi in quarantena, eliminati o sostituiti con un testo.
- **Modificate e consegnate.** Le informazioni della scansione sono stati aggiunti alle intestazioni delle email, passando queste ultime tramite i filtri.
- **Consegnate senza nessun'altra azione.** Queste email sono state ignorate dalla Protezione Exchange e sono state analizzate dai filtri.

Exchange - Attività malware

Ti fornisce informazioni sulle email con minacce malware, rilevate sui server mail Exchange selezionati in un determinato periodo di tempo. Le informazioni fanno riferimento a:

- Gli indirizzi email del mittente e dei destinatari.

  Quando l'email viene inviata a più destinatari, invece degli indirizzi email, il rapporto mostra il numero di destinatari con un link a una finestra contenente l'elenco degli indirizzi email.
- Oggetto e-mail.
- Stato dell'email dopo la scansione antimalware.

  Cliccando sul link dello stato, puoi visualizzare maggiori dettagli sui malware eliminati e l'azione intrapresa.
- Data e ora di rilevamento.
- Il server in cui la minaccia è stata rilevata.
- L'azienda che possiede il server mail.

Exchange - Utilizzo licenza mensile

Fornisce informazioni dettagliate relative all'utilizzo della licenza Security for Exchange per le aziende da te gestite in un determinato periodo di tempo.

La tabella sotto il grafico fornisce dettagli relativi al nome dell'azienda, codici di licenza, mese e numero mailbox protette, appartenenti a ciascuna delle tue aziende gestite.

Il numero di utilizzo della licenza per un'azienda è collegato a una nuova finestra, in cui è possibile trovare informazioni dettagliate sull'uso, come domini in licenza in quella società e le relative mailbox.

Exchange - Top 10 malware rilevati

Ti informa sulle 10 minacce malware più rilevate negli allegati email. Puoi generare due visualizzazioni contenenti statistiche diverse. Una visualizzazione mostra il numero di rilevamenti dai destinatari interessati e una dai mittenti.

Per esempio, GravityZone ha rilevato un'email con un allegato infetto inviata a cinque destinatari.

- Nella visualizzazione dei destinatari:
  - Il rapporto mostra cinque rilevamenti.
  - I dettagli del rapporto mostrano solo i destinatari, non i mittenti.
- Nella visualizzazione dei mittenti:
  - Il rapporto mostra una rilevazione.
  - I dettagli del rapporto mostrano solo il mittente, non i destinatari.

Oltre alla combinazione mittente/destinatari e il nome del malware, il rapporto fornisce anche i seguenti dettagli:

- Il tipo di malware (virus, spyware, PUA, ecc.)
- Il server in cui la minaccia è stata rilevata.
- Le misure intraprese dal modulo antimalware.
- Data e ora dell'ultimo rilevamento.

Exchange - Top 10 destinatari malware

Ti mostra i 10 destinatari email più colpiti dai malware in un determinato intervallo di tempo.

I dettagli del rapporto ti forniscono l'intero elenco dei malware che hanno colpito tali destinatari, oltre alle azioni intraprese.

Exchange - Top 10 destinatari spam

Ti mostra i 10 destinatari email più colpiti per numero di email spam o phishing rilevate in un determinato intervallo di tempo. Il rapporto fornisce informazioni anche sulle azioni intraprese alle rispettive email.

11.2. Creare i rapporti

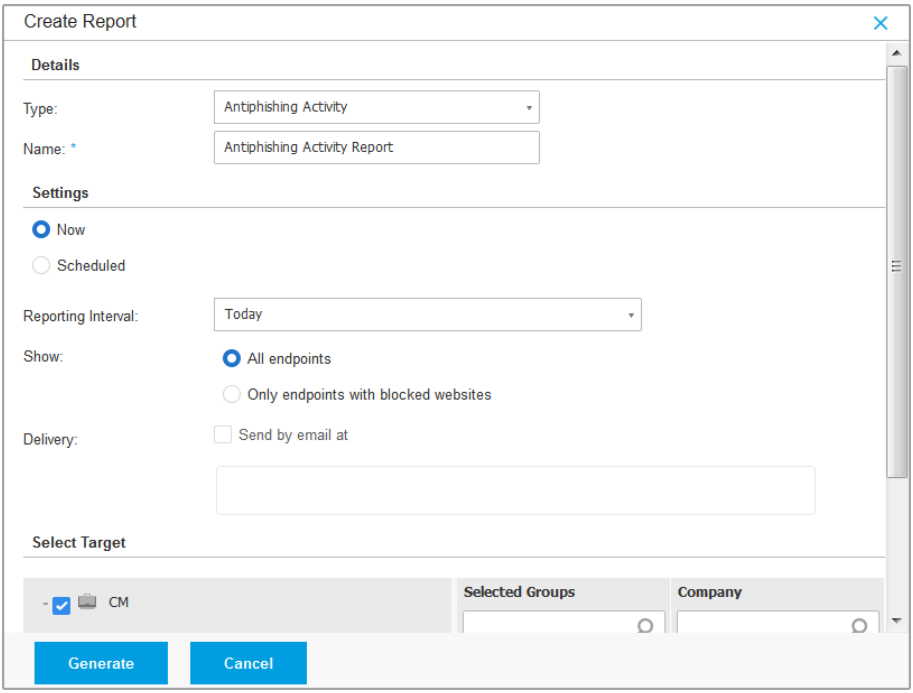
Puoi creare due categorie di rapporti:

- **Rapporti istantanei.** I rapporti istantanei vengono mostrati automaticamente dopo averli generati.
- **Rapporti programmati.** I rapporti programmati possono essere configurati per essere eseguiti periodicamente, in una determinata ora e data. Un elenco di tutti i rapporti programmati viene mostrato nella pagina **Rapporti**.

Importante
I rapporti istantanei vengono eliminati automaticamente alla chiusura della pagina del rapporto. I rapporti programmati vengono salvati e mostrati nella pagina **Rapporti**.

Per creare un rapporto:

1. Vai alla pagina **Rapporti**.
2. Clicca sul pulsante **Aggiungi** nel lato superiore della tabella. Apparirà una finestra di configurazione.



Opzioni rapporto

3. Seleziona il tipo di rapporto desiderato dal menu. Per maggiori informazioni, fai riferimento a «Tipo di rapporto» (p. 388)
4. Inserisci un nome specifico per il rapporto. Scegliendo un nome, considera il tipo e il bersaglio del rapporto, e possibilmente le opzioni del rapporto.
5. Configura la ricorrenza del rapporto:
   - Seleziona **Ora** per creare un rapporto istantaneo.
   - Seleziona **Programmato** per configurare la generazione automatica del rapporto nell'intervallo di tempo desiderato:
     - Orario, nell'intervallo specificato tra le ore.
     - Giornaliero. In questo caso, puoi anche impostare l'ora di inizio (ora e minuti).

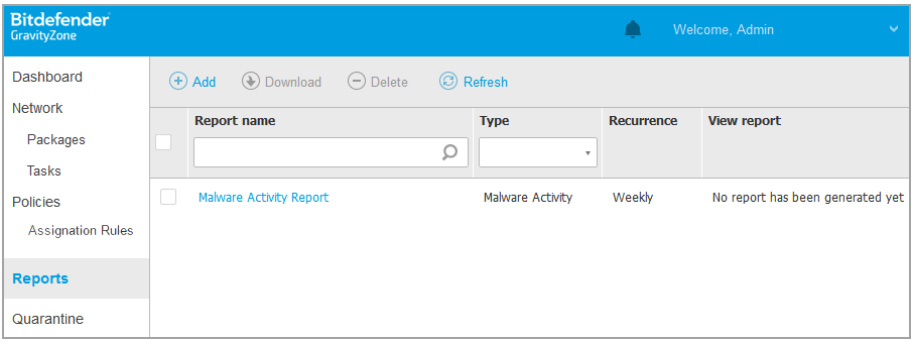
- Settimanale, nei giorni della settimana indicati e all'orario di inizio selezionato (ora e minuti).
- Mensile, nel giorno del mese indicato e all'orario di inizio selezionato (ora e minuti).

6. Per la maggior parte dei tipi di rapporto devi indicare l'intervallo di tempo a cui si riferiscono i dati contenuti. Il rapporto mostrerà solo i dati di quel periodo di tempo selezionato.
7. Diversi tipi di rapporto offrono opzioni di filtraggio per aiutarti a trovare facilmente le informazioni di tuo interesse. Usa le opzioni di filtraggio nella sezione **Mostra** per ottenere solo le informazioni desiderate.

   Per esempio, per un rapporto di **Stato aggiornamento**, puoi scegliere di visualizzare solo l'elenco degli elementi di rete che non sono stati aggiornati, o quelli che devono essere riavviati per completare l'aggiornamento.
8. **Consegna**. Per ricevere un rapporto programmato via email, seleziona la casella corrispondente. Inserisci gli indirizzi email desiderati nel campo sottostante. Di norma, l'email contiene un archivio con entrambi i file del rapporto (PDF e CSV). Usa le caselle nella sezione **Allega file** per personalizzare il tipo di file e come inviarli via email.
9. **Seleziona bersaglio**. Scorri in basso per configurare il bersaglio del rapporto. Seleziona uno o più gruppi di endpoint che vuoi includere nel rapporto.
10. In base alla ricorrenza selezionata, clicca su **Genera** per creare un rapporto istantaneo o **Salva** per creare un rapporto programmato.
    - Il rapporto istantaneo sarà visualizzato immediatamente dopo aver cliccato su **Genera**. Il tempo richiesto per la creazione dei rapporti potrebbe variare in base al numero di elementi di rete gestiti. Attendi la creazione del rapporto richiesto.
    - Il rapporto programmato sarà mostrato nell'elenco della pagina **Rapporti**. Una volta generata l'istanza del rapporto, puoi visualizzare il rapporto cliccando sul link corrispondente nella colonna **Vedi rapporto** nella pagina **Rapporti**.

11.3. Visualizzare e gestire i rapporti programmati

Per visualizzare e gestire i rapporti programmati, vai alla pagina **Rapporti**.



La pagina dei rapporti

Tutti i rapporti programmati vengono mostrati in una tabella con una serie di informazioni utili al riguardo:

- Nome e tipo del rapporto
- Ricorrenza del rapporto
- Ultima istanza generata.

Nota
I rapporti programmati sono disponibili solo per l'utente che li ha creati.

Per ordinare i rapporti in base a una determinata colonna, clicca semplicemente sull'intestazione della colonna. Clicca nuovamente sull'intestazione della colonna per modificare l'ordine selezionato.

Per trovare facilmente ciò che stai cercando, usa le caselle di ricerca o le opzioni di filtraggio sotto le intestazioni della colonna.

Per cancellare il contenuto di una casella di ricerca, posiziona il cursore su di essa e clicca sull'icona × **Elimina**.

Per assicurarsi che vengano visualizzate le informazioni più recenti, clicca sul pulsante **Aggiorna** nel lato superiore della tabella.

11.3.1. Visualizza rapporti

Per visualizzare un rapporto:

1. Vai alla pagina **Rapporti**.

2. Ordina i rapporti per nome, tipo o ricorrenza per trovare facilmente il rapporto che stai cercando.
3. Clicca sul link corrispondente nella colonna **Vedi rapporto** per mostrare il rapporto. Sarà mostrata l'istanza del rapporto più recente.

   Per visualizzare tutte le istanze di un rapporto, fai riferimento a«Salvare i rapporti» (p. 413)

Tutti i rapporti hanno una sezione di sommario (la metà superiore della pagina del rapporto) e una di dettagli (la metà inferiore della pagina del rapporto).

- La sezione del sommario fornisce dati statistici (grafici e diagrammi) per tutti gli elementi della rete bersaglio, oltre a informazioni generali sul rapporto, come il periodo interessato (ove applicabile), il bersaglio del rapporto, ecc.
- La sezione dei dettagli fornisce informazioni su ciascun elemento di rete bersaglio.

Nota

- Per configurare le informazioni mostrate dal grafico, clicca sui valori della legenda così da mostrare o nascondere i dati selezionati.
- Clicca sull'area grafica (sezione del diagramma, barra) di tuo interesse per visualizzare i relativi dettagli nella tabella.

11.3.2. Modificare i rapporti programmati

Nota
Quando si modifica un rapporto programmato, ogni aggiornamento sarà applicato a partire dalla prossima ricorrenza del rapporto. I rapporti generati in precedenza non saranno influenzati dalla modifica.

Per modificare le impostazioni di un rapporto programmato:

1. Vai alla pagina **Rapporti**.
2. Clicca sul nome del rapporto.
3. Modifica le impostazioni del rapporto in base alle esigenze. Puoi modificare:
   - **Nome del rapporto**. Seleziona un nome specifico per il rapporto, così da identificarne facilmente le caratteristiche. Scegliendo un nome, considera il tipo e il bersaglio del rapporto, e possibilmente le opzioni del rapporto. I

rapporti generati da un rapporto programmato vengono chiamati allo stesso modo.

- **Ricorrenza del rapporto (programma)**. Puoi programmare il rapporto per essere generato automaticamente a cadenza oraria (in un determinato intervallo orario), giornaliera (in una determinata ora di inizio), settimanale (in una determinata giornata della settimana e ora di inizio) o mensile (in una determinata giornata del mese e ora di inizio). In base al programma selezionato, il rapporto includerà dati rispettivamente solo dell'ultimo giorno, settimana o mese.
- **Impostazioni**
  - Puoi programmare il rapporto per essere generato automaticamente a cadenza oraria (in un determinato intervallo orario), giornaliera (in una determinata ora di inizio), settimanale (in una determinata giornata della settimana e ora di inizio) o mensile (in una determinata giornata del mese e ora di inizio). In base al programma selezionato, il rapporto includerà dati rispettivamente solo dell'ultimo giorno, settimana o mese.
  - Il rapporto includerà solo i dati dell'intervallo di tempo selezionato. Puoi modificare l'intervallo a partire dalla prossima ricorrenza.
  - La maggior parte dei rapporti forniscono opzioni di filtraggio per aiutarti a trovare facilmente le informazioni che ti interessano. Visualizzando il rapporto nella console, tutte le informazioni saranno disponibili, indipendentemente dalle opzioni selezionate. Tuttavia, se scarichi il rapporto o lo invii via email, nel file PDF saranno incluse solo le informazioni selezionate e il sommario del rapporto. I dettagli del rapporto saranno disponibili solo in formato CSV.
  - Puoi scegliere di ricevere il rapporto via email.
- **Seleziona bersaglio**. L'opzione selezionata indica il tipo di bersaglio del rapporto attuale (gruppi o singoli elementi della rete). Clicca sul link corrispondente per visualizzare il bersaglio del rapporto attuale. Per modificarlo, seleziona i gruppi o gli elementi di rete da includere nel rapporto.

4. Clicca su **Salva** per applicare le modifiche.

11.3.3. Eliminare i rapporti programmati

Quando un rapporto programmato non è più necessario, è meglio eliminarlo. Eliminare un rapporto programmato cancellerà tutte le istanze che ha generato automaticamente fino a quel momento.

Per eliminare un rapporto programmato:

1. Vai alla pagina **Rapporti**.
2. Seleziona il rapporto che vuoi eliminare.
3. Clicca sul pulsante ⊖ **Elimina** nel lato superiore della tabella.

11.4. Intraprendere azioni basate sul rapporto

Mentre la maggior parte dei rapporti evidenzia soltanto i problemi nella tua rete, alcuni di loro offrono anche diverse opzioni per risolvere i problemi cliccando su un solo pulsante.

Per risolvere i problemi mostrati nel rapporto, clicca sul pulsante appropriato nella barra degli strumenti sopra alla tabella dei dati.

Nota
Ti servono diritti di **Gestione rete** per eseguire tali azioni.

Queste sono le opzioni disponibili per ciascun rapporto:

Stato malware

- **Esamina bersagli infetti**. Esegui un'attività di scansione completa sui bersagli indicati come tuttora infetti.

Stato dell'Aggiornamento

- **Aggiornamento**. Aggiorna i client bersaglio alle versioni più recenti disponibili.

Stato aggiornamento

- **Upgrade**. Sostituisce i vecchi client endpoint con la nuova generazione di prodotti disponibili.

11.5. Salvare i rapporti

Di norma, i rapporti programmati vengono salvati automaticamente in Control Center.

Se hai bisogno di avere a disposizione i rapporti per periodi di tempo superiori, puoi salvarli nel computer. Il sommario del rapporto sarà disponibile in formato PDF, mentre i dettagli del rapporto saranno disponibili solo in formato CSV.

Hai due modi per salvare i rapporti:

- Esporta
- Download

11.5.1. Esportare i rapporti

Per esportare il rapporto sul tuo computer:

1. Seleziona un formato e clicca su **Esporta CSV** o **Esporta PDF**.
2. In base alle impostazioni del tuo browser, il file potrebbe essere scaricato automaticamente in un percorso di download predefinito, oppure si aprirà una finestra di download, in cui devi specificare la cartella di destinazione.

11.5.2. Scaricare i rapporti

Un archivio del rapporto include sia il sommario del rapporto che i suoi dettagli.

Per scaricare un archivio del rapporto:

1. Vai alla pagina **Rapporti**.
2. Seleziona il rapporto che vuoi salvare.
3. Clicca sul pulsante **Scarica** e seleziona **Ultima istanza** per scaricare l'ultima istanza generata dal rapporto o **Archivio completo** per scaricare un archivio contenente tutte le istanze.

   In base alle impostazioni del tuo browser, il file potrebbe essere scaricato automaticamente in un percorso di download predefinito, oppure si aprirà una finestra di download, in cui devi specificare la cartella di destinazione.

11.6. Inviare i rapporti via email

Puoi inviare i rapporti via email usando le seguenti opzioni:

1. Per inviare via e-mail il rapporto che stai visualizzando, clicca sul pulsante **E-mail**. Il rapporto sarà inviato all'indirizzo e-mail associato al tuo account.
2. Per configurare l'invio via email dei rapporti programmati desiderati:
   a. Vai alla pagina **Rapporti**.
   b. Clicca sul nome del rapporto desiderato.
   c. In **Impostazioni > Consegna**, seleziona **Invia per e-mail a**.
   d. Inserisci l'indirizzo e-mail desiderato nel campo sottostante. Puoi aggiungere quanti indirizzi e-mail desideri.
   e. Clicca su **Salva**.

> **Nota**
> Solo il sommario del rapporto e il grafico saranno inclusi nel file PDF inviato via email. I dettagli del rapporto saranno disponibili nel file CSV.

I rapporti vengono inviati via email come archivi .zip.

11.7. Stampare i rapporti

Control Center non supporta attualmente la funzionalità del pulsante Stampa. Per stampare un rapporto, prima è necessario salvarlo sul proprio computer.

12. QUARANTENA

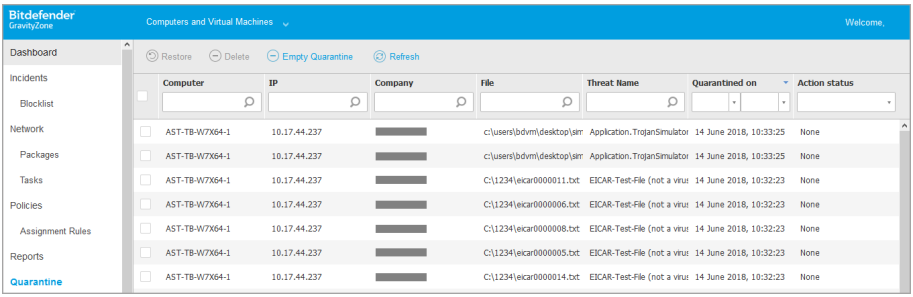
La quarantena è una cartella cifrata che include file potenzialmente dannosi, come sospetti malware, file infettati da malware o altri file indesiderati. Quando un virus o un'altra forma di malware sono in quarantena, non possono più arrecare alcun danno in quanto non possono essere eseguiti o letti.

GravityZone mette i file in quarantena in base alle policy assegnate agli endpoint. Di norma, i file che non possono essere disinfettati vengono messi in quarantena.

La quarantena viene salvata a livello locale su ciascun endpoint.

12.1. Esplorare la quarantena

La pagina **Quarantena** fornisce informazioni dettagliate sui file in quarantena da tutti gli endpoint gestiti.



La pagina Quarantena

La pagina Quarantena è formata da due parti:

- Computer e Virtual Machine, per file rilevati direttamente nel file system degli endpoint.
- Server Exchange, per email e file allegati a messaggi email, rilevati su server email Exchange.

Il selettore di visualizzazione nel lato superiore della pagina consente di alternarsi tra le due parti.

Le informazioni sui file messi in quarantena vengono mostrate in una tabella. In base al numero di endpoint gestiti e il grado dell'infezione, la tabella Quarantena

può includere un gran numero di valori. La tabella può spaziare per diverse pagine (di norma, vengono mostrate solo 20 voci per ciascuna pagina).

Per muoversi tra le pagine, usa i pulsanti di navigazione nella parte inferiore della tabella. Per cambiare il numero di valori mostrati in una pagina, seleziona un'opzione nel menu accanto ai pulsanti di navigazione.

Per una migliore visibilità dei dati di tuo interesse, puoi usare le caselle di ricerca nelle intestazioni della colonna per filtrare i dati mostrati. Per esempio, puoi cercare una determinata minaccia rilevata nella rete o un determinato elemento di rete. Puoi anche cliccare sulle intestazioni della colonna per ordinare i dati di una determinata colonna.

Per assicurarsi che vengano visualizzate le informazioni più recenti, clicca sul pulsante **Aggiorna** nel lato superiore della tabella. Potrebbe essere necessario se si trascorre molto tempo nella pagina.

12.2. Quarantena per computer e Virtual Machine

Di norma, i file in quarantena sono inviati automaticamente ai laboratori di Bitdefender per essere analizzati dai ricercatori antimalware di Bitdefender. Se viene confermata la presenza di malware, viene rilasciata una firma per consentirne la rimozione. Inoltre, i file in quarantena vengono esaminati dopo ogni aggiornamento delle firme dei malware. I file puliti vengono spostati automaticamente alla loro ubicazione originale. Queste funzionalità sono relative a ciascuna policy di sicurezza nella pagina **Policy** ed è possibile scegliere se tenerle o disattivarle. Per maggiori informazioni, fai riferimento a «Quarantena» (p. 180).

12.2.1. Visualizzare i dettagli della quarantena

La tabella quarantena ti fornisce le seguenti informazioni:

- Il nome dell'endpoint su cui è stata rilevata la minaccia.
- L'azienda in cui si trova l'endpoint.
- L'IP dell'endpoint su cui è stata rilevata la minaccia.
- Percorsi per il file infetto o sospetto sull'endpoint in cui è stato rilevato.
- Il nome assegnato alla minaccia malware dai ricercatori di sicurezza di Bitdefender.
- La data e l'ora in cui il file è stato messo in quarantena.
- Lo stato dell'azione da dover intraprendere sul file in quarantena.

12.2.2. Gestire i file in quarantena

Il comportamento della quarantena è diverso per ciascun ambiente:

- **Security for Endpoints** memorizza i file in quarantena su ogni computer gestito. Utilizzando la Control Center, hai la possibilità di eliminare o ripristinare determinati file in quarantena.
- **Security for Virtualized Environments (Multipiattaforma)** memorizza i file in quarantena su ciascuna virtual machine gestita. Utilizzando la Control Center, hai la possibilità di eliminare o ripristinare determinati file in quarantena.

Gestione dei file in quarantena

In determinate occasioni, potresti aver bisogno di ripristinare i file in quarantena nella loro posizione originale o in un'altra. Una simile situazione è quando intendi ripristinare alcuni file importanti memorizzati in un archivio infetto che è stato messo in quarantena.

Nota
Il ripristino di file in quarantena è possibile solo in ambienti protetti da Security for Endpoints e Security for Virtualized Environments (Multipiattaforma).

Per ripristinare uno o più file in quarantena:

1. Vai alla pagina **Quarantena**.
2. Seleziona le caselle corrispondenti ai file in quarantena che intendi ripristinare.
3. Clicca sul pulsante **Ripristina** nel lato superiore della tabella.
4. Seleziona la posizione in cui desideri vengano ripristinati i file selezionati (l'originale oppure una posizione personale sul computer bersaglio).

   Se scegli di ripristinarlo in una posizione personale, devi inserire il percorso nel campo corrispondente.
5. Seleziona **Aggiungi automaticamente esclusione nella policy** per escludere i file da ripristinare da scansioni future. L'esclusione si applica a tutte le policy, coinvolgendo i file selezionati, tranne che per la policy predefinita, che non è possibile modificare.
6. Clicca su **Salva** per richiedere l'azione di ripristino del file. Puoi notare lo stato in sospeso nella colonna **Azione**.
7. L'azione richiesta viene inviata agli endpoint bersaglio immediatamente o non appena tornano online.

Puoi visualizzare i dettagli relativi allo stato dell'azione nella pagina **Attività**. Una volta ripristinato un file, il valore corrispondente scomparirà dalla tabella Quarantena.

Eliminazione automatica dei file in quarantena

Di norma, i file in quarantena più vecchi di 30 giorni sono eliminati automaticamente. Questa impostazione può essere cambiata modificando la policy assegnata agli endpoint gestiti.

Per cambiare l'intervallo di eliminazione automatica per i file in quarantena:

1. Vai alla pagina **Policy**
2. Trova la policy assegnata agli endpoint su cui desideri modificare le impostazioni e clicca sul suo nome.
3. Vai alla pagina **Antimalware > Impostazioni**.
4. Nella sezione **Quarantena**, seleziona il numero di giorni dopo cui i file vengono eliminati.
5. Clicca su **Salva** per applicare le modifiche.

Eliminazione manuale dei file in quarantena

Se desideri eliminare manualmente i file in quarantena, dovresti prima assicurarti che i file che hai scelto di eliminare non siano necessari.

Un file stesso potrebbe essere un malware. Se la tua ricerca dovesse portare a tale esito, puoi cercare una determinata minaccia nella quarantena per poi eliminarla da essa.

Per eliminare uno o più file in quarantena:

1. Vai alla pagina **Quarantena**.
2. Seleziona le caselle corrispondenti ai file in quarantena che intendi eliminare.
3. Clicca sul pulsante ⊖ **Elimina** nel lato superiore della tabella. Dovrai confermare la tua azione cliccando su **Sì**.

   Puoi notare lo stato in sospeso nella colonna **Azione**.

   L'azione richiesta viene inviata agli elementi di rete bersaglio immediatamente o non appena tornano online. Una volta eliminato un file, il valore corrispondente scomparirà dalla tabella Quarantena.

Svuotare la quarantena

Per eliminare tutti gli elementi in quarantena:

1. Vai alla pagina **Quarantena**.
2. Clicca sul pulsante **Svuota quarantena**.

   Nella finestra di conferma, seleziona l'opzione **Includi quarantena sotto-aziende** per eliminare gli elementi in quarantena per le tue aziende figlio e clicca su **Sì**.

Verranno eliminate tutte le voci della tabella Quarantena. L'azione richiesta viene inviata agli elementi di rete bersaglio immediatamente o non appena tornano online.

12.3. Quarantena server Exchange

La quarantena Exchange include email e allegati. Il modulo Antimalware mette in quarantena allegati email, laddove Antispam e Filtro allegati e contenuti mettono in quarantena l'intera email.

Nota
Ti ricordiamo che la quarantena per Exchange Server richiede spazio su disco aggiuntivo nella partizione in cui l'agente di sicurezza viene installato. Lo spazio della quarantena dipende dal numero di oggetti memorizzati e dalla loro dimensione.

12.3.1. Visualizzare i dettagli della quarantena

La pagina **Quarantena** offre informazioni dettagliate sugli elementi in quarantena da tutti i server Exchange nella tua organizzazione. Le informazioni sono disponibili nella tabella Quarantena e nella finestra dei dettagli di ciascun elemento.

La tabella quarantena ti fornisce le seguenti informazioni:

- **Oggetto**. L'oggetto dell'email messa in quarantena.
- **Mittente**. L'indirizzo e-mail del mittente così come compare nel campo dell'intestazione dell'e-mail **Da**.
- **Destinatari**. L'elenco dei destinatari così come appaiono nei campi dell'intestazione dell'email **A** e **CC**.
- **Destinatari reali**. L'elenco degli indirizzi email dei singoli utenti a cui l'email era indirizzata prima di essere messa in quarantena.
- **Stato**. Lo stato dell'elemento dopo la scansione. Lo stato mostra se un'email è stata segnata come spam o se contiene contenuti indesiderati, oppure se un

allegato è un malware infetto, sospettato di essere infetto, indesiderato o non esaminabile.

- **Azienda**. L'azienda nel cui ambiente è stata rilevata e messa in quarantena l'email o l'allegato.
- **Nome del malware**. Il nome assegnato alla minaccia malware dai ricercatori di sicurezza di Bitdefender.
- **Nome del server**. L'hostname del server su cui la minaccia è stata rilevata.
- **Messo in quarantena il**. La data e l'ora in cui l'elemento è stato messo in quarantena.
- **Stato dell'azione**. Lo stato dell'azione intrapresa sull'elemento in quarantena. In questo modo puoi visualizzare rapidamente se un'azione è ancora in sospesa oppure se è fallita.

Nota

- Le colonne **Destinatari reali**, **Nome malware** e **Nome server** sono nascoste nella visualizzazione predefinita.
- Quando diversi allegati della stessa email vengono messi in quarantena, la tabella Quarantena mostra un valore separato per ogni allegato.

Per personalizzare i dettagli della quarantena mostrati nella tabella:

1. Clicca sul pulsante **Colonne** nel lato destro dell'intestazione della tabella.
2. Seleziona le colonne che vuoi visualizzare.

   Per tornare alla visualizzazione delle colonne predefinita, clicca sul pulsante **Reimposta**.

Puoi ottenere maggiori informazioni cliccando sul link **Oggetto** corrispondente per ogni elemento. Viene mostrata la finestra **Dettagli oggetto**, che ti fornisce le seguenti informazioni:

- **Elemento in quarantena**. Il tipo di elemento messo in quarantena, che può essere un'email o un allegato.
- **Messo in quarantena il**. La data e l'ora in cui l'elemento è stato messo in quarantena.
- **Stato**. Lo stato dell'elemento dopo la scansione. Lo stato mostra se un'email è stata segnata come spam o se contiene contenuti indesiderati, oppure se un

allegato è un malware infetto, sospettato di essere infetto, indesiderato o non esaminabile.

- **Nome allegato**. Il nome del file dell'allegato rilevato dal modulo antimalware o filtro allegati.
- **Nome del malware**. Il nome assegnato alla minaccia malware dai ricercatori di sicurezza di Bitdefender. Queste informazioni sono disponibili solo se l'oggetto è stato infettato.
- **Punto di rilevamento**. Un elemento viene rilevato a livello di trasporto o in una casella di posta, oppure una cartella pubblica dall'Exchange Store.
- **Regola associata**. La regola della policy a cui è stata associata la minaccia.
- **Server**. L'hostname del server su cui la minaccia è stata rilevata.
- **IP mittente**. L'indirizzo IP del mittente.
- **Mittente (Da)**. L'indirizzo e-mail del mittente così come compare nel campo dell'intestazione dell'e-mail **Da**.
- **Destinatari**. L'elenco dei destinatari così come appaiono nei campi dell'intestazione dell'email **A** e **CC**.
- **Destinatari reali**. L'elenco degli indirizzi email dei singoli utenti a cui l'email era indirizzata prima di essere messa in quarantena.
- **Oggetto**. L'oggetto dell'email messa in quarantena.

Nota
I puntini di sospensione al termine del testo indicano che una parte del testo manca. In questo caso, sposta il mouse sul testo per visualizzarlo in un suggerimento.

12.3.2. Elementi in quarantena

Email e file in quarantena del modulo Protezione Exchange vengono memorizzati localmente sul server come i file cifrati. Usando il Control Center hai la possibilità di ripristinare le email in quarantena, nonché di eliminare o salvare file o email in quarantena.

Ripristinare le email in quarantena

Se decidi che un'email in quarantena non rappresenta una minaccia, puoi toglierla dalla quarantena. Usando Exchange Web Services, la Protezione Exchange invia

l'email in quarantena ai destinatari previsti come allegato a un'email di notifica di Bitdefender.

Nota
Puoi ripristinare solo le email. Per ripristinare un allegato in quarantena, devi salvarlo in una cartella in locale su un server Exchange.

Per ripristinare una o più email:

1. Vai alla pagina **Quarantena**.
2. Scegli **Exchange** dal selettore di visualizzazione disponibile nella parte superiore della pagina.
3. Seleziona le caselle corrispondenti alle email che vuoi ripristinare.
4. Clicca sul pulsante **Ripristina** nel lato superiore della tabella. Comparirà la finestra **Ripristina credenziali**.
5. Seleziona le credenziali di un utente Exchange autorizzato per inviare le email da ripristinare. Se le credenziali che intendi usare sono nuove, prima devi aggiungerle al gestore delle credenziali.

   Per aggiungere le credenziali richieste:

   a. Inserisci le informazioni richieste nei campi corrispondenti nell'intestazione della tabella:
      - Il nome utente e la password dell'utente Exchange.

        Nota
        Il nome utente deve includere il nome del dominio, nel formato `user@domain` o `domain\user`.

      - L'indirizzo e-mail dell'utente Exchange, necessario solo quando l'indirizzo e-mail è diverso dal nome dell'utente.
      - L'URL dell'Exchange Web Services (EWS), necessario quando Exchange Autodiscovery non funziona. Questo di solito è il caso dei server Edge Transport in una DMZ.

   b. Clicca sul pulsante **Aggiungi** nel lato destro della tabella. Il nuovo set di credenziali viene aggiunto alla tabella.
6. Clicca sul pulsante **Ripristina**. Apparirà un messaggio di conferma.

L'azione richiesta viene inviata immediatamente ai server di destinazione. Una volta ripristinata l'email, viene anche eliminata dalla quarantena, così il valore corrispondente scomparirà dalla tabella Quarantena.

Puoi controllare lo stato dell'azione di ripristino in ognuna di queste posizioni:

- La colonna **Stato dell'Azione** della tabella Quarantena.
- **Rete e attività**.

Salvare i file in quarantena

Se vuoi esaminare o ripristinare dai file in quarantena, puoi salvare i file in una cartella locale sul Server Exchange. Bitdefender Endpoint Security Tools decifra i file, salvandoli in una determinata posizione.

Per salvare uno o più file in quarantena:

1. Vai alla pagina **Quarantena**.
2. Scegli **Exchange** dal selettore di visualizzazione disponibile nella parte superiore della pagina.
3. Filtra i dati della tabella per visualizzare tutti i file che vuoi salvare, inserendo i termini di ricerca negli appositi campi nelle intestazioni della colonna.
4. Seleziona le caselle corrispondenti ai file in quarantena che intendi ripristinare.
5. Clicca sul pulsante **Salva** nel lato superiore della tabella.
6. Inserisci il percorso per la cartella di destinazione sul Server Exchange. Se la cartella non esiste sul server, sarà creata.

   Importante
   Devi escludere questa cartella dalla scansione a livello di file system, altrimenti i file saranno spostati nella quarantena di computer e virtual machine. Per maggiori informazioni, fai riferimento a «Eccezioni» (p. 180).

7. Clicca su **Salva**. Apparirà un messaggio di conferma.

   Puoi notare lo stato in sospeso nella colonna **Stato dell'Azione**. Puoi anche visualizzare lo stato dell'azione nella pagina **Rete > Attività**.

Eliminazione automatica dei file in quarantena

Di norma, i file in quarantena più vecchi di 15 giorni vengono eliminati automaticamente. Puoi modificare questa impostazione modificando la policy assegnata al Server Exchange gestito.

Per cambiare l'intervallo di eliminazione automatica per i file in quarantena:

1. Vai alla pagina **Policy**
2. Clicca sul nome della policy assegnata al Server di Exchange di tuo interesse.
3. Vai alla pagina **Protezione Exchange > Generale**
4. Nella sezione **Impostazioni**, seleziona il numero di giorni dopo cui i file vengono eliminati.
5. Clicca su **Salva** per applicare le modifiche.

Eliminazione manuale dei file in quarantena

Per eliminare uno o più file in quarantena:

1. Vai alla pagina **Quarantena**.
2. Seleziona **Exchange** dal selettore di visualizzazione.
3. Seleziona le caselle corrispondenti ai file che vuoi eliminare.
4. Clicca sul pulsante ⊖ **Elimina** nel lato superiore della tabella. Dovrai confermare la tua azione cliccando su **Sì**.

   Puoi notare lo stato in sospeso nella colonna **Stato dell'Azione**.

   L'azione richiesta viene inviata immediatamente ai server di destinazione. Una volta eliminato un file, il valore corrispondente scomparirà dalla tabella Quarantena.

Svuotare la quarantena

Per eliminare tutti gli elementi in quarantena:

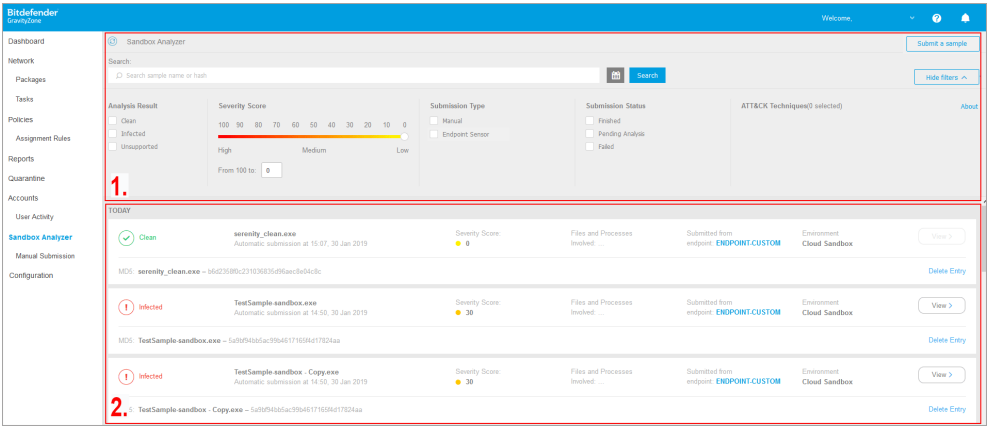
1. Vai alla pagina **Quarantena**.
2. Seleziona **Exchange** dal selettore di visualizzazione.
3. Clicca sul pulsante **Svuota quarantena**.

   Nella finestra di conferma, seleziona l'opzione **Includi quarantena sotto-aziende** per eliminare gli elementi in quarantena per le tue aziende figlio e clicca su **Sì**.

Verranno eliminate tutte le voci della tabella Quarantena. L'azione richiesta viene inviata immediatamente agli elementi di rete di destinazione.

13. USARE SANDBOX ANALYZER

La pagina **Sandbox Analyzer** fornisce un'interfaccia unificata per visualizzare, filtrare e cercare gli invii automatici e manuali per l'ambiente sandbox. La pagina **Sandbox Analyzer** è formata da due zone:



La pagina Sandbox Analyzer

1. La **zona del filtro** ti consente di cercare e filtrare gli invii in base a determinati criteri, come nome, hash, data, risultato dell'analisi, stato e tecniche di MITRE ATT&CK.
2. La **zona delle schede di invio** mostra tutti gli invii in un formato compatto con informazioni dettagliate su ciascuna di esse.

Nella pagina Sandbox Analyzer, è possibile:

- Filtra le schede di invio
- Visualizza l'elenco degli invii e i dettagli delle analisi
- Elimina le schede di invio
- Effettuare invii manuali

13.1. Filtrare le schede di invio

Questo è quello che puoi fare nell'area dei filtri:

- Filtrare gli invii in base a diversi criteri. La pagina caricherà automaticamente solo le schede degli eventi di sicurezza che corrispondono ai criteri selezionati.
- Azzera i filtri cliccando sul pulsante **Annulla filtri**.
- Nascondi l'area dei filtri cliccando sul pulsante **Nascondi filtri**. Puoi mostrare nuovamente le opzioni nascoste, cliccando su **Mostra filtri**.

Puoi filtrare gli invii di Sandbox Analyzer in base ai seguenti criteri:

- **Nome e hash del campione (MD5)**. Inserisci nel campo di ricerca una parte o l'intero nome, oppure l'hash del campione che stai cercando, poi clicca sul pulsante **Cerca** sul lato destro.
- **Data**. Per filtrare in base alla data:
  1. Clicca sull'icona del calendario per configurare l'intervallo di tempo della ricerca.
  2. Definisci l'intervallo. Clicca sui pulsanti **Da** e **A** nel lato superiore del calendario per selezionare le date che definiscono l'intervallo temporale. Puoi anche selezionare un periodo predeterminato dal lato destro dell'elenco delle opzioni, relativamente al momento attuale (ad esempio, gli ultimi 30 giorni).

     Puoi anche specificare l'ora e i minuti per ogni data dell'intervallo di tempo, usando le opzioni sotto il calendario.
  3. Clicca su **OK** per applicare il filtro.
- **Risultato analisi**. Seleziona una o più delle seguenti opzioni:
  - **Pulito** - Il campione è sicuro.
  - **Infetto** - Il campione è pericoloso.
  - **Non supportato** - Il campione ha un formato che Sandbox Analyzer non ha potuto detonare. Per visualizzare l'elenco completo delle estensioni e dei tipi di file supportati da Sandbox Analyzer, fai riferimento a «Estensioni e tipi di file supportati per l'invio manuale» (p. 461).
- **Punteggio di severità**. Il valore indica quanto un campione è pericoloso in una scala da 0 (zero) a 100. Più il punteggio è alto e più il campione è pericoloso. Il punteggio di severità si applica a tutti i campioni inviato, incluso quelli con stato **Pulito** o **Non supportato**.
- **Tipo di invio**. Seleziona una o più delle seguenti opzioni:

  - **Manuale**. Sandbox Analyzer ha ricevuto il campione tramite l'opzione **Invio manuale**.
  - **Sensore endpoint**. Bitdefender Endpoint Security Tools ha inviato il campione a Sandbox Analyzer in base alle impostazioni della policy.
- **Stato invio**. Seleziona una o più delle seguenti caselle:
  - **Finita** - Sandbox Analyzer ha consegnato il risultato dell'analisi.
  - **Analisi in corso** - Sandbox Analyzer sta eseguendo il campione.
  - **Fallita** - Sandbox Analyzer non ha potuto detonare il campione.
- **Tecniche di ATT&CK**. Questa opzione di filtro integra la knowledge base ATT&CK di MITRE, se applicabile. I valori delle tecniche ATT&CK cambiano in modo dinamico, in base agli eventi di sicurezza.

  Clicca sul link **Informazioni** per aprire la Matrice di ATT&CK in una nuova scheda.

13.2. Visualizzare i dettagli dell'analisi

La pagina **Sandbox Analyzer** mostra le schede di invio in base al giorno, in ordine cronologico inverso. Le schede di invio includono i seguenti dati:

- Risultato analisi
- Nome campione
- Tipo di invio
- Punteggio di severità
- File e processi coinvolti
- Ambiente di detonazione
- Valore hash (MD5)
- Tecniche di ATT&CK
- Lo stato dell'invio quando un risultato non è disponibile

Ogni scheda di invio include un link a un dettagliato rapporto HTML di analisi, se disponibile. Per aprire il rapporto, clicca sul pulsante **Vedi** nel lato destro della scheda.

Il rapporto HTML fornisce molte informazioni organizzate su più livelli, con testi descrittivi, grafici e schermate, che illustrano il comportamento del campione nell'ambiente di detonazione. Questo è ciò che puoi apprendere da un rapporto HTML di Sandbox Analyzer:

- Dati generali sul campione analizzato, come nome e classificazione del malware, dettagli dell'invio (nome del file, tipo e dimensione, hash, ora dell'invio e durata dell'analisi).
- Risultati dell'analisi comportamentale, che includono tutti gli eventi di sicurezza catturati durante la detonazione, organizzati in sezioni. Gli eventi di sicurezza si riferiscono a:
  - Scrittura / eliminazione / spostamento / duplicazione / sostituzione dei file sul sistema e su unità rimovibili.
  - Esecuzione di file appena creati.
  - Modifiche al file di sistema.
  - Modifiche alle applicazioni in esecuzione nella virtual machine.
  - Modifiche alla barra delle applicazioni di Windows e al menu Start.
  - Creazione / conclusione / inserimento processi.
  - Scrittura / eliminazione chiavi del registro.
  - Creazione di oggetti mutex.
  - Creazione / esecuzione / blocco / modifica / interrogazione / eliminazione di servizi.
  - Modificare le impostazioni di sicurezza del browser.
  - Modificare le impostazioni di visualizzazione di Windows Explorer.
  - Aggiungere file all'elenco delle eccezioni del firewall.
  - Modificare le impostazioni della rete.
  - Attivare l'esecuzione all'avvio del sistema.
  - Connessione a un host remoto.
  - Accesso a determinati domini.
  - Trasferimento dati a e da determinati domini.
  - Accesso a URL, IP e porte tramite diversi protocolli di comunicazione.
  - Verifica degli indicatori dell'ambiente virtuale.
  - Verifica degli indicatori degli strumenti di monitoraggio.
  - Creazione di istantanee
  - Hook SSDT, IDT, IRP.
  - Dump di memoria per processi sospetti.
  - Chiamate di funzioni API di Windows.
  - Disattivazione per un determinato periodo di tempo per ritardare l'esecuzione.
  - Creazione di file con azioni da eseguire in determinati intervalli di tempo.

Importante
I rapporti HTML sono disponibili solo in inglese, indipendentemente dalla lingua utilizzata in GravityZone Control Center.

13.3. Eliminare le schede di invio

Per eliminare una scheda di invio che non serve più:

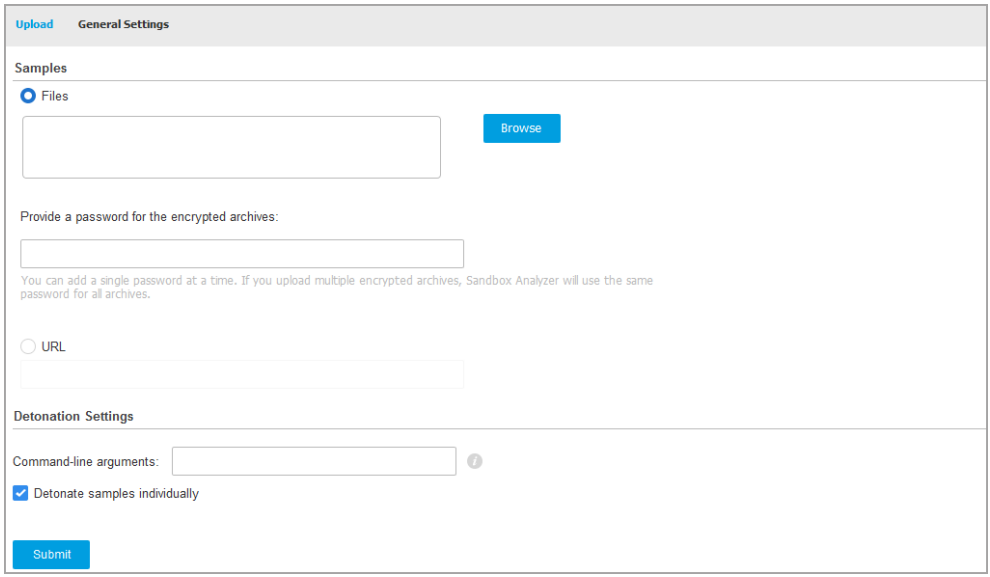
1. Vai alla scheda di invio che vuoi eliminare.
2. Clicca sull'opzione **Elimina valore** nel lato sinistro della scheda.
3. Clicca su **Sì** per confermare.

Nota
Seguendo questi passaggi, eliminerai solo la scheda di invio. Le informazioni relative all'invio continuano a essere disponibili nel rapporto **Risultati di Sandbox Analyzer (Deprecati)**. Tuttavia, questo rapporto continuerà a essere supportato solo per una quantità limitata di tempo.

13.4. Invio manuale

Da **Sandbox Analyzer > Invio manuale**, puoi inviare campioni di elementi sospetti a Sandbox Analyzer, per determinare se si tratta di minacce o file innocui. Puoi anche accedere alla pagina **Invio manuale**, cliccando sul pulsante **Invia un campione** nell'angolo in alto a destra della zona di filtro nella pagina Sandbox Analyzer.

Nota
L'invio manuale di Sandbox Analyzer è compatibile con tutti i browser richiesti dalla Control Center, tranne Internet Explorer 9. Per inviare gli elementi a Sandbox Analyzer, accedi a Control Center usando un qualsiasi altro browser web supportato e indicato in «Connessione a Control Center» (p. 16).



Sandbox Analyzer > Invio manuale

Per inviare i campioni a Sandbox Analyzer:

1. Nella pagina **Invio**, in **Campioni**, seleziona il tipo di elemento:
   a. **File**. Clicca sul pulsante **Esplora** per selezionare gli elementi che vuoi inviare all'analisi comportamentale. In caso di archivi protetti da password, puoi definire una password per sessione di upload in un campo dedicato. Durante la fase di analisi, Sandbox Analyzer applica la password specificata a tutti gli archivi inviati.
   b. **URL**. Compila il campo corrispondente con ogni URL che vuoi analizzare. Puoi inviare solo un URL per sessione.
2. In **Impostazioni detonazione**, configura i parametri dell'analisi per la sessione attuale:
   - **Argomenti linea di comando**. Puoi aggiungere quanti argomenti linea di comando desideri, separati da spazi, per alterare l'operatività di determinati programmi, come gli eseguibili. Gli argomenti linea di comando si applicano a tutti i campioni inviati durante l'analisi.

- **Detona i campioni individualmente**. Seleziona la casella per analizzare singolarmente i file di un pacchetto.

3. In **Profilo detonazione**, imposta il livello di complessità dell'analisi comportamentale, influenzando l'elaborazione di Sandbox Analyzer. Per esempio, se impostato su **Alto**, Sandbox Analyzer esegue un'analisi più accurata su meno campioni, nello stesso intervallo, rispetto a **Medio** o **Basso**.
4. Nella pagina **Impostazioni generali**, puoi impostare configurazioni che si applicano a tutti gli invii manuali, indipendentemente dalla sessione:
   a. **Limite di tempo per detonazione campione (minuti)**. Determina una quantità fissa di tempo per completare l'analisi del campione. Il valore predefinito è 4 minuti, ma a volte l'analisi potrebbe richiedere più tempo. Al termine dell'intervallo configurato, Sandbox Analyzer interrompe l'analisi e genera un rapporto basato sui dati raccolti fino a quel momento. Se interrotto quando incompleta, l'analisi potrebbe contenere risultati inaccurati.
   b. **Numero di repliche consentite**. In caso di errori inattesi, Sandbox Analyzer prova a detonare il campione come configurato fino al completamento dell'analisi. Il valore predefinito è 2. Ciò significa che Sandbox Analyzer proverà altre due volte a detonare il campione in caso di errore.
   c. **Prefiltraggio**. Seleziona questa opzione per escludere dalla detonazione i campioni già analizzati.
   d. **Accesso a Internet durante la detonazione**. Durante l'analisi, alcuni campioni richiedono la connessione a Internet per completare l'analisi. Per il miglior risultato, si consiglia di mantenere attivata questa opzione.
   e. Clicca su **Salva** per mantenere le modifiche.
5. Torna alla pagina **Invio**.
6. Clicca su **Invia**. Una barra dei progressi indica lo stato dell'invio.

   Dopo l'invio, la pagina **Sandbox Analyzer** mostra una nuova scheda. Quando l'analisi è completata, la scheda fornisce il verdetto e i relativi dettagli.

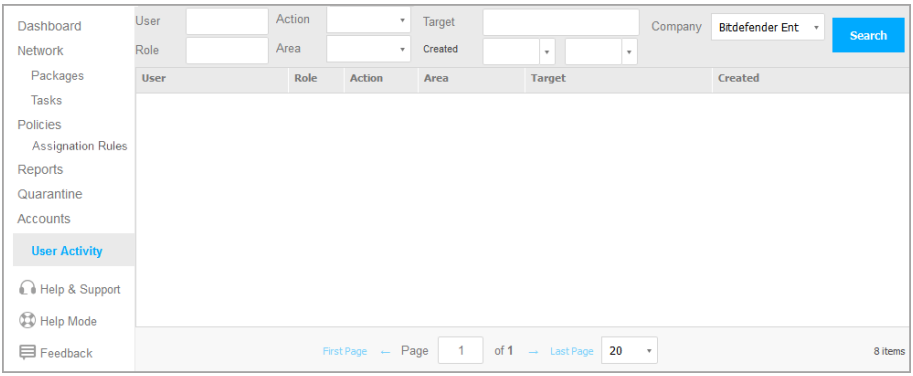
Nota
Per inviare manualmente il campione a Sandbox Analyzer, servono diritti di **Gestione reti**.

14. RAPPORTO ATTIVITÀ UTENTE

Control Center registra tutte le operazioni e azioni eseguite dagli utenti in un rapporto. L'elenco delle attività dell'utente include i seguenti eventi, in base al tuo livello di permesso amministrativo:

- Accedere e uscire
- Creare, modificare, rinominare ed eliminare i rapporti
- Aggiungere e rimuovere i portlet della dashboard
- Creare, modificare ed eliminare le credenziali
- Creare, modificare, scaricare ed eliminare i pacchetti di rete
- Creare attività di rete
- Avviare, terminare, annullare e bloccare processi di risoluzione dei problemi sulle macchine interessate
- Creare, modificare, rinominare ed eliminare gli account utente
- Eliminare o spostare gli endpoint tra i gruppi
- Creare, spostare, rinominare ed eliminare i gruppi
- Eliminare e ripristinare i file in quarantena
- Creare, modificare ed eliminare gli account utente
- Creare, modificare, rinominare, assegnare ed eliminare le policy
- Modificare le impostazioni di autenticazione per gli account di GravityZone.

Per esaminare i valori delle attività dell'utente, vai alla pagina**Account > Attività utente**.



La pagina attività utente

Per mostrare gli eventi registrati a cui sei interessato, devi definire una ricerca. Inserisci i criteri di ricerca nei campi disponibili e clicca sul pulsante **Cerca**. Tutte le voci che corrispondono ai tuoi criteri saranno mostrate nella tabella.

Le colonne della tabella di forniscono alcune informazioni utili sugli eventi elencati:

- Il nome utente di chi ha eseguito l'azione.
- Ruolo dell'utente.
- L'azione che ha causato l'evento.
- Il tipo di elemento della console influenzato dall'azione.
- Lo specifico elemento della console influenzato dall'azione.
- Il momento in cui si è verificato l'evento.

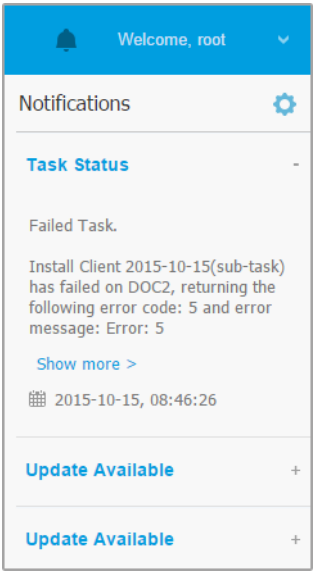
Per ordinare gli eventi in base a una determinata colonna, clicca semplicemente sull'intestazione di quella colonna. Cliccaci nuovamente per invertire l'ordine selezionato.

Per visualizzare informazioni dettagliate su un evento, selezionalo e controlla la sezione sotto la tabella.

15. USARE GLI STRUMENTI

16. NOTIFICHE

In base agli eventi che potrebbero verificarsi nella tua rete, Control Center mostrerà diverse notifiche per informarti dello stato di sicurezza del tuo ambiente. Le notifiche saranno mostrate nell'**Area notifiche**, localizzata nel lato destro di Control Center.



Area notifiche

Quando nella rete vengono rilevati nuovi eventi, l'icona 11 nell'angolo in alto a destra di Control Center mostrerà il numero di nuovi eventi rilevati. Cliccare sull'icona consente di mostrare l'Area notifiche contenente l'elenco degli eventi rilevati.

16.1. Tipi di notifiche

Questo è l'elenco dei tipi di notifica disponibili:

Epidemia malware

Questa notifica viene inviata agli utenti che hanno almeno il 5% di tutti i loro elementi di rete gestiti infettati dallo stesso malware.

Perciò, per le aziende partner, la notifica viene generata quando lo stesso malware viene rilevato in maniera cumulativa su endpoint della loro stessa rete e delle reti delle aziende figlie.

Puoi configurare la soglia di diffusione dei malware in base alle tue necessità nella finestra **Impostazioni notifiche**. Per maggiori informazioni, fai riferimento a «Configurare le impostazioni di scansione» (p. 443).

Le minacce rilevate da HyperDetect sono escluse da questa notifica.

Scadenza della licenza

Questa notifica viene inviata 30, 7 e 1 giorno prima della scadenza della licenza.

Devi avere il diritto **Gestione azienda** per visualizzare tale notifica.

Limite della licenza quasi raggiunto

Questa notifica viene inviata quando il 90% delle licenze disponibili è stato usato.

Devi avere il diritto **Gestione azienda** per visualizzare tale notifica.

Limite di utilizzo della licenza dei server è stato raggiunto

Questa notifica viene inviata quando il numero di server protetti raggiunge il limite specificato sul tuo codice di licenza.

Devi avere il diritto **Gestione azienda** per visualizzare tale notifica.

Il limite della licenza dei server sta per essere raggiunto

Questa notifica viene inviata quando è stato usato il 90% dei posti disponibili della licenza per i server.

Devi avere il diritto **Gestione azienda** per visualizzare tale notifica.

Limite di utilizzo licenza Exchange raggiunto

Questa notifica viene attivata ogni volta che il numero di caselle di posta protette dei tuoi server Exchange raggiunge il limite indicato nel tuo codice di licenza.

Devi avere il diritto **Gestione azienda** per visualizzare tale notifica.

Credenziali utente Exchange non valide

Questa notifica viene inviata quando non è stato possibile avviare un'attività di scansione a richiesta sul server Exchange bersaglio a causa di credenziali errate dell'utente Exchange.

Stato aggiornamento

Questa notifica viene attivata a cadenza settimanale, se nella rete vengono rilevate versioni del prodotto datato.

Anti-exploit avanzato

Questa notifica ti avvisa quando l'Anti-exploit avanzato ha rilevato tentativi di exploit nella tua rete.

Evento antiphishing

Questa notifica ti informa ogni volta che l'agente dell'endpoint impedisce l'accesso a una pagina web di phishing nota. Questa notifica fornisce anche dettagli come l'endpoint che ha tentato di accedere al sito web non sicuro (nome e IP), l'agente installato o l'URL bloccato.

Evento firewall

Con questa notifica vieni informato ogni volta che il modulo firewall di un agente installato ha impedito a un port scan o a un'applicazione di accedere alla rete, in base alla policy applicata.

Evento ATC/IDS

Questa notifica viene inviata ogni volta che un'applicazione potenzialmente pericolosa viene rilevata e bloccata su un endpoint nella rete. Troverai maggiori dettagli sul tipo di applicazione, il nome e il percorso così come il percorso e l'ID del processo parentale, e la linea di comando che ha avviato il processo, se è il caso.

Evento Controllo utenti

Questa notifica viene attivata ogni volta che un'attività dell'utente, come la navigazione web o un'applicazione software, viene bloccata dal client dell'endpoint in base alla policy in vigore.

Evento protezione dati

Questa notifica viene inviata ogni volta che il traffico dati viene bloccato su un endpoint in base alle regole di protezione dei dati.

Evento stato Security Server

Questo tipo di notifica fornisce informazioni su eventuali cambiamenti dello stato di un determinato Security Server installato nella tua rete. I cambiamenti dello stato del Security Server si riferiscono ai seguenti eventi: attivazione / disattivazione, aggiornamento del prodotto, aggiornamento del contenuto di sicurezza e necessità di riavvio.

Evento Security Server sovraccarico

Questa notifica viene inviata quando il carico della scansione su un Security Server nella rete supera la soglia definita.

Evento registrazione prodotto

Questa notifica ti informa quando lo stato di registrazione di un agente installato nella rete è cambiato.

Verifica autenticazione

Questa notifica ti informa quando un altro account GravityZone della tua azienda, tranne il tuo, è stato usato per accedere alla Control Center da un dispositivo non riconosciuto. Selezionando la casella **Ricevi una notifica per aziende figlie**, le notifiche saranno inviate anche per gli account GravityZone delle tue aziende gestite.

Accesso da nuovo dispositivo

Questa notifica ti informa che il tuo account GravityZone è stato usato per accedere a Control Center da un dispositivo che finora non hai mai utilizzato a tale scopo. La notifica viene configurata automaticamente per essere visibile sia in Control Center che via e-mail, e solo tu potrai visualizzarla.

Stato attività

Questa notifica ti informa ogni volta che uno stato di un'attività cambia o solo quando un'attività termina, in base alle tue preferenze.

Server di aggiornamento obsoleto

Questa notifica viene inviata quando un server d'aggiornamento nella rete ha contenuti di sicurezza datati.

Evento incidenti di rete

Questa notifica viene inviata ogni volta che il modulo Network Attack Defense rileva un tentativo di attacco nella tua rete. Questa notifica ti informa anche se il tentativo di attacco è stato condotto dall'esterno della rete o da un endpoint compromesso nella rete. Altri dettagli includono dati sull'endpoint, la tecnica di attacco, l'IP dell'aggressore e l'azione intrapresa da Network Attack Defense.

Rilevamento Sandbox Analyzer

Questa notifica ti avvisa ogni volta che Sandbox Analyzer rileva una nuova minaccia tra i campioni inviati. Ti vengono presentati dettagli come nome dell'azienda, hostname o IP dell'endpoint, ora e data del rilevamento, tipo di minaccia, percorso, nome, dimensione dei file e azione di risanamento intrapresa su ciascuno.

Nota
Non riceverai notifiche per i campioni puliti analizzati. Le informazioni sui campioni inviati dalla tua azienda e, se configurate, dalle tue aziende figlie, sono disponibili nel rapporto **Risultati di Sandbox Analyzer (Deprecati)** Le informazioni sui campioni inviate dalla tua azienda sono anche disponibili nella sezione di **Sandbox Analyzer**, nel menu principale di Control Center.

Attività HyperDetect

Questa notifica segnala quando HyperDetect trova qualsiasi antimalware o eventi non bloccati all'interno della rete. Viene inviata per ciascun evento di HyperDetect e contiene i seguenti dettagli:

- Informazioni sull'endpoint interessato (nome, IP, agente installato)
- Tipo e nome del malware
- Percorso del file infetto. Per gli attacchi privi di file, viene indicato il nome dell'eseguibile usato nell'attacco.
- Stato dell'infezione
- L'hash SHA256 dell'eseguibile malware
- Il tipo di attacco previsto (attacco mirato, grayware, exploit, ransomware, file sospetti e traffico di rete)
- Grado di rilevazione (Permissivo, Normale, Aggressivo)
- Ora e data della rilevazione

Puoi visualizzare maggiori dettagli sull'infezione e investigare ulteriormente sui problemi generando un rapporto **Attività HyperDetect** direttamente dalla pagina **Notifiche**. Per farlo:

1. In Control Center, clicca sul pulsante **Notifiche** per visualizzare l'area delle notifiche.
2. Clicca sul link **Mostra altro** al termine della notifica per aprire la pagina **Notifiche**.
3. Clicca sul pulsante **Vedi rapporto** nei dettagli della notifica. In questo modo si aprirà la finestra di configurazione.
4. Se necessario, configura il rapporto. Per maggiori informazioni, fai riferimento a «Creare i rapporti» (p. 406).
5. Clicca su **Genera**.

Nota
Per evitare di creare spam, riceverai un massimo di una notifica ogni ora.

Problema integrazione Active Directory
Questa notifica ti informa sui problemi che influenzano la sincronizzazione con Active Directory.

Problema patch mancante
Questa notifica si verifica quando gli endpoint nella tua rete non hanno una o più patch disponibili.

GravityZone invia automaticamente una notifica contenente tutto ciò che ha rilevato nelle ultime 24 ore fino alla data di notifica. La notifica viene inviata a tutti i tuoi account utente.

Puoi visualizzare quali endpoint sono in questa situazione cliccando sul pulsante **Vedi rapporto** nei dettagli della notifica.

Di norma, la notifica fa riferimento a patch di sicurezza, ma potresti configurarla per informarti anche sulle patch di non sicurezza.

Nuovo incidente
Questa notifica ti informa ogni volta che si verifica un nuovo incidente. Una volta attivata, la notifica viene generata ogni volta che un nuovo incidente viene mostrato nella sezione **Incidenti** del Control Center. Per maggiori dettagli, clicca sul **Nome dell'incidente**.

Rilevamento ransomware
Questa notifica ti informa quando GravityZone rileva un attacco ransomware nella tua rete. Ti vengono forniti i dettagli relativi all'endpoint colpito, all'utente che ha effettuato l'accesso, all'origine dell'attacco, al numero di file cifrati e alla data e all'ora dell'attacco.

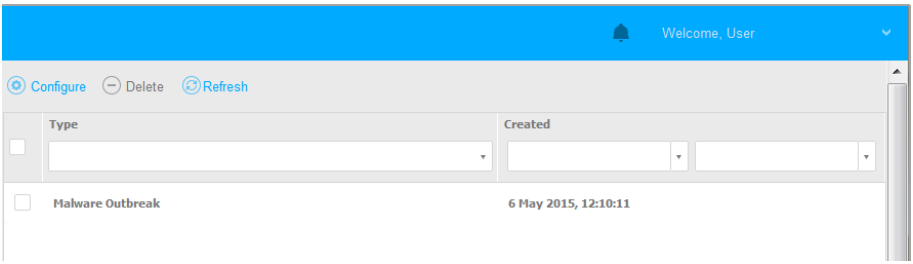
Nel momento in cui ricevi la notifica, l'attacco è già stato bloccato.

Il link nella notifica ti reindirizzerà alla pagina **Attività ransomware**, in cui potrai visualizzare l'elenco dei file cifrati e ripristinarli, se necessari.

Disponibilità formato syslog: JSON, CEF

16.2. Visualizzare le notifiche

Per visualizzare le notifiche, clicca sul pulsante **Notifiche** e clicca su **Vedi tutte le notifiche**. Viene mostrata una tabella contenente tutte le notifiche.



La pagina Notifiche

In base al numero di notifiche, la tabella può essere formata da diverse pagine (di norma, per ogni pagina sono presenti solo 20 voci).

Per muoversi tra le pagine, usa i pulsanti di navigazione nella parte inferiore della tabella.

Per cambiare il numero di valori mostrati in una pagina, seleziona un'opzione nel menu accanto ai pulsanti di navigazione.

Nel caso ci fossero troppi valori, puoi usare le caselle di ricerca sotto le intestazioni delle colonne o il menu filtro nel lato superiore della tabella per filtrare i dati mostrati.

- Per filtrare le notifiche, seleziona il tipo di notifica che vuoi visualizzare nel menu **Tipo**. In alternativa, puoi selezionare l'intervallo di tempo durante il quale è stata generata la notifica, per ridurre il numero di valori nella tabella, specialmente se è stato generato un numero elevato di notifiche.
- Per visualizzare i dettagli della notifica, clicca sul nome della notifica nella tabella. Sotto la tabella viene mostrata una sezione **Dettagli**, in cui puoi visualizzare l'evento che ha generato la notifica.

16.3. Eliminare le notifiche

Per eliminare le notifiche:

1. Clicca sul pulsante **Notifiche** sul lato destro della barra dei menu e clicca su **Vedi tutte le notifiche**. Viene mostrata una tabella contenente tutte le notifiche.
2. Seleziona le notifiche che vuoi eliminare.
3. Clicca sul pulsante **Elimina** nel lato superiore della tabella.

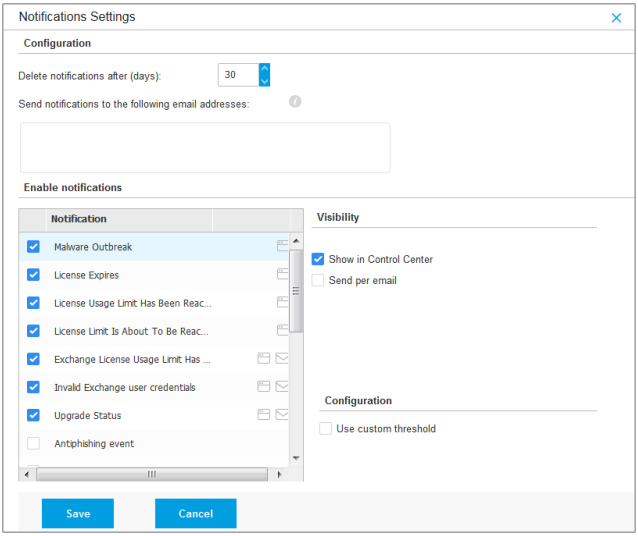
Puoi anche configurare le notifiche per essere eliminate automaticamente dopo un determinato numero di giri. Per maggiori informazioni, fai riferimento a «Configurare le impostazioni di scansione» (p. 443).

16.4. Configurare le impostazioni di scansione

Il tipo di notifiche da inviare e gli indirizzi email a cui vengono inviate possono essere configurati per ciascun utente.

Per configurare le impostazioni delle notifiche:

1. Clicca sul pulsante **Notifiche** sul lato destro della barra dei menu e clicca su **Vedi tutte le notifiche**. Viene mostrata una tabella contenente tutte le notifiche.
2. Clicca sul pulsante **Configura** nel lato superiore della tabella. Viene mostrata la finestra **Impostazioni delle notifiche**.



Impostazioni notifiche

Nota
Puoi anche accedere direttamente alla finestra **Impostazioni delle notifiche** usando l'icona **Configura** nell'angolo in alto a destra della finestra **Area notifiche**.

3. Nella sezione **Configurazione**, puoi definire le seguenti impostazioni:
   - Eliminare automaticamente le notifiche dopo un determinato periodo di tempo. Impostare il valore desiderato tra 1 e 365 nel campo **Elimina le notifiche dopo (days)**.
   - Inoltre, puoi inviare le notifiche via email a determinati destinatari. Inserisci gli indirizzi email nel campo dedicato, premendo il tasto `Invio` dopo ogni indirizzo.
4. Nella sezione **Attiva notifiche** puoi selezionare il tipo di notifiche che vuoi ricevere da GravityZone. Puoi anche configurare individualmente visibilità e opzioni di invio per ciascun tipo di notifica.

   Seleziona il tipo di notifica che desideri dall'elenco. Per maggiori informazioni, fai riferimento a «Tipi di notifiche» (p. 436). Una volta selezionato un tipo di notifica, puoi configurare le sue opzioni specifiche (se disponibili) nell'area a destra:

Visibilità

- **Mostra in Control Center** indica che questo tipo di evento viene mostrato in Control Center, con l'aiuto del pulsante **Notifiche**.
- **Invia per e-mail** indica che questo tipo di evento viene inviato anche a determinati indirizzi e-mail. In questo caso, è necessario inserire gli indirizzi e-mail nel campo dedicato, premendo `Invio` dopo ogni indirizzo.

Configurazione

- **Usa soglia personalizzata** - Ti consente di definire una soglia per gli eventi che si verificano, da cui viene inviata la notifica selezionata.

  Per esempio, la notifica Epidemia malware viene inviata di norma agli utenti che hanno almeno il 5% dei loro elementi di rete gestiti infettati dallo stesso malware. Per modifica il valore della soglia di un'epidemia malware, attiva l'opzione **Usa soglia personalizzata** e inserisci il valore che desideri nel campo **Soglia epidemia malware**.
- Per **Evento stato Security Server**, puoi selezionare gli eventi del Security Server che attiveranno questo tipo di notifica:

- **Datato** - Notifica ogni volta in cui un Security Server nella tua rete è datato.
- **Riavvio richiesto** - Notifica ogni volta in cui un Security Server nella tua rete richiede un riavvio.

- Per **Stato attività**, puoi selezionare il tipo di stato che attiverà questo tipo di notifica:
  - **Ogni stato** - Notifica ogni volta che un'attività inviata da Control Center viene eseguita con uno stato qualsiasi.
  - **Solo fallite** - Notifica ogni volta che un'attività inviata da Control Center è fallita.

5. Clicca su **Salva**.

17. OTTENERE AIUTO

Bitdefender si sforza di fornire ai suoi clienti un supporto veloce e preciso assolutamente senza pari. Se riscontri un problema o in caso di domande sul tuo prodotto di Bitdefender, visita il nostro Centro di supporto online. Fornisce diverse risorse che puoi utilizzare per trovare rapidamente una soluzione o una risposta. O, se preferisci, puoi contattare il Servizio clienti di Bitdefender. Gli operatori del nostro supporto risponderanno alle tue domande in modo tempestivo e ti forniranno l'assistenza necessaria.

Nota
Puoi trovare informazioni sui nostri servizi e la politica di supporto nel Centro di supporto.

17.1. Centro di supporto di Bitdefender

Centro di supporto di Bitdefender è il luogo in cui troverai tutta l'assistenza necessaria con il tuo prodotto di Bitdefender.

Puoi usare varie risorse per trovare rapidamente una soluzione o una risposta:

- Articoli della Knowledge Base
- Forum supporto di Bitdefender
- Documentazione del prodotto

Puoi anche usare il tuo motore di ricerca preferito per trovare più informazioni sulla sicurezza del computer, i prodotti Bitdefender e la società.

Articoli della Knowledge Base

La Knowledge Base di Bitdefender è un archivio online di informazioni sui prodotti di Bitdefender. Conserva, in un formato facilmente accessibile, le notifiche sui risultati delle attività di risoluzioni bug e problemi del supporto tecnico di Bitdefender e dei team di sviluppo, oltre ad articoli più generali sulla prevenzione antivirus, la gestione delle soluzioni di Bitdefender, con spiegazioni dettagliate, e molti altri articoli.

La Knowledge Base di Bitdefender è aperta al pubblico e liberamente esplorabile. Le molte informazioni contenute sono un altro mezzo per fornire ai clienti di Bitdefender le conoscenze tecniche che gli servono. Tutte le richieste di informazioni o segnalazioni di bug dai clienti di Bitdefender arrivano alla Knowledge Base di

Bitdefender, così come segnalazioni e informazioni su bug risolti o articoli tecnici per integrare i file di supporto del prodotto.

La Knowledge Base di Bitdefender per i prodotti aziendali è disponibile in qualsiasi momento presso http://www.bitdefender.com/support/business.html.

Forum supporto di Bitdefender

Il forum del supporto di Bitdefender fornisce agli utenti di Bitdefender un modo semplice per ottenere aiuto e aiutare gli altri. Puoi pubblicare ogni problema o domanda relativa al tuo prodotto Bitdefender.

I tecnici del supporto di Bitdefender controllano le nuove discussioni sul forum per poterti assistere. Potresti ricevere una risposta o una soluzione anche da un utente di Bitdefender più esperto.

Prima di postare il tuo problema o la tua domanda, cerca nel forum un'eventuale discussione simile o collegata.

Il forum del supporto di Bitdefender è disponibile all'indirizzo http://forum.bitdefender.com in 5 lingue diverse: inglese, tedesco, francese, spagnolo e rumeno. Clicca sul link **Protezione Business** per accedere alla sezione dedicata ai prodotti per utenti aziendali.

Documentazione del prodotto

La documentazione del prodotto è la fonte di informazioni più completa sul tuo prodotto.

Clicca sul tuo nome utente nell'angolo in alto a destra della console, seleziona **Aiuto e Supporto** e poi il link della guida a cui sei interessato. La guida si aprirà in una nuova scheda del tuo browser.

17.2. Necessiti di assistenza

Puoi chiederci assistenza attraverso il nostro Centro di supporto online. Compila il modulo di contatto e invialo.

17.3. Usare lo strumento di supporto

Lo Strumento di supporto di GravityZone è stato progettato per aiutare gli utenti e supportare i tecnici a ottenere facilmente le informazioni necessarie per risolvere eventuali problemi. Esegui lo Strumento di supporto nei computer interessati e

invia l'archivio risultante con le informazioni sulla risoluzione dei problemi al rappresentante del supporto di Bitdefender.

17.3.1. Utilizzare lo Strumento di supporto sui sistemi operativi Windows

Eseguire l'applicazione dello strumento di supporto

Per generare il rapporto sul computer interessato, utilizza uno dei seguenti metodi:

- Linea di comando

  Per qualsiasi altro problema con BEST, installato sul computer.

- Problema di installazione

  Per situazioni in cui BEST non è stato installato sul computer e l'installazione non è avvenuta.

Metodo a linea di comando

Usando una linea di comando puoi ottenere i rapporti direttamente dal computer interessato. Questo metodo è utile in situazioni in cui non hai accesso a GravityZone Control Center o se il computer non comunica con la console.

1. Apri il prompt dei comandi con privilegi di amministratore.
2. Vai alla cartella di installazione del prodotto. Il percorso predefinito è:

   `C:\Programmi\Bitdefender\Endpoint Security`
3. Raccogli e salva i registri eseguendo il seguente comando:

   ```
   Product.Support.Tool.exe collect
   ```

   Per impostazione predefinita, i registri vengono salvati in `C:\Windows\Temp`.

   Facoltativamente, se desideri salvare il rapporto dello strumento di supporto in una posizione personalizzata, utilizza il percorso opzionale:

   ```
   Product.Support.Tool.exe collect [path="<path-to-file>"]
   ```

   Esempio:

```
Product.Support.Tool.exe collect path="D:\Test"
```

Mentre il comando è in esecuzione, sullo schermo apparirà una barra di avanzamento. Una volta completato il processo, vengono mostrati il nome e la posizione dell'archivio che contiene i registri.

Per inviare i rapporti al supporto aziendale di Bitdefender, accedi a `C:\Windows\Temp` o al percorso personalizzato e trova il file di archivio chiamato `ST_[computername]_[currentdate]`. Allega l'archivio al tuo ticket di supporto per ricevere ulteriore assistenza.

Problema di installazione

1. Per scaricare lo Strumento di supporto di BEST, clicca qui.
2. Esegui il file eseguibile come amministratore. Comparirà una finestra.
3. Scegli una posizione per salvare l'archivio dei rapporti.

   Mentre i rapporti vengono ottenuti, sullo schermo potrai visualizzare una barra indicante i progressi. Una volta completato il processo, vengono mostrati il nome e la posizione dell'archivio.

Per inviare i rapporti al Supporto aziendale di Bitdefender, accedi alla posizione selezionata e trova il file di archivio chiamato `ST_[computername]_[currentdate]`. Allega l'archivio al tuo ticket di supporto per ricevere ulteriore assistenza.

17.3.2. Utilizzare lo Strumento di supporto su sistemi operativi Linux

Per i sistemi operativi Linux, lo Strumento di supporto è integrato nell'agente di sicurezza di Bitdefender.

Per raccogliere informazioni sul sistema Linux utilizzando lo Strumento di supporto, esegui il seguente comando:

```
# /opt/BitDefender/bin/bdconfigure
```

usando le seguenti opzioni disponibili:

- `--help` per elencare tutti i comandi dello Strumento di supporto

- `enablelogs` per attivare i registri dei moduli prodotto e comunicazione (tutti i servizi saranno riavviati automaticamente)
- `disablelogs` per disattivare i registri dei moduli prodotto e comunicazione (tutti i servizi saranno riavviati automaticamente)
- `deliverall` per creare:
  - Un archivio contenente i registri dei moduli prodotto e comunicazioni, forniti alla cartella `/tmp` nel seguente formato: `bitdefender_machineName_timeStamp.tar.gz`.

    Una volta creato l'archivio:

    1. Ti sarà chiesto se desideri disattivare i registri. Se necessario, i servizi vengono riavviati automaticamente.
    2. Ti sarà chiesto se desideri eliminare i registri.
- `deliverall -default` fornisce le stesse informazioni dell'opzione precedente, ma le azioni predefinite saranno prese nei registri, senza che venga chiesto nulla all'utente (i registri vengono disattivati ed eliminati).

Puoi anche eseguire il comando `/bdconfigure` direttamente dal pacchetto BEST (completo o downloader) senza aver installato il prodotto.

Per segnalare un problema di GravityZone che riguarda i tuoi sistemi Linux, segui questi passaggi, usando le opzioni descritte in precedenza:

1. Attiva i registri dei moduli prodotto e comunicazione.
2. Prova a riprodurre il problema.
3. Disattiva i registri.
4. Crea l'archivio dei registri.
5. Apri un ticket di supporto via e-mail utilizzando il modulo disponibile nella pagina **Aiuto e supporto** della Control Center, con una descrizione del problema e allegando l'archivio dei registri.

Lo Strumento di supporto per Linux fornisce le seguenti informazioni:

- Le cartelle `etc`, `var/log`, `/var/crash` (se disponibili) e `var/epag` da `/opt/BitDefender`, contenenti i registri e le impostazioni di Bitdefender.
- Il file `/var/log/BitDefender/bdinstall.log`, contenente le informazioni di installazione

- Il file `network.txt`, contenente informazioni su impostazioni di rete / connettività della macchina
- Il file `product.txt`, incluso i contenuti di tutti i file `update.txt` da `/opt/BitDefender/var/lib/scan` e un elenco completo ricorrente di tutti i file da `/opt/BitDefender`
- Il file `system.txt`, contenente informazioni generali sul sistema (distribuzione e versione del kernel, RAM disponibile e spazio libero su disco rigido)
- Il file `users.txt`, contenente le informazioni dell'utente
- Altre informazioni sul prodotto e relative al sistema, come connessioni esterne di processi e utilizzo della CPU.
- Registri di sistema

17.3.3. Utilizzare lo Strumento di supporto sui sistemi operativi Mac

Inviando una richiesta al supporto tecnico di Bitdefender, devi fornire le seguenti informazioni:

- Una descrizione dettagliata del problema che stai riscontrando.
- Un'immagine (se possibile) dell'esatto messaggio di errore che compare.
- Il registro dello Strumento di supporto.

Per raccogliere informazioni sul sistema Mac con lo Strumento di supporto:

1. Scarica l'archivio ZIP contenente lo Strumento di supporto.
2. Estrai il file **BDProfiler.tool** dall'archivio.
3. Apri una finestra del Terminale.
4. Raggiungi la posizione del file **BDProfiler.tool**.

   Per esempio:

   ```
   cd /Users/Bitdefender/Desktop;
   ```

5. Aggiungi i permessi di esecuzione al file:

```
chmod +x BDProfiler.tool;
```

6. Esegui lo strumento.

   Per esempio:

   ```
   /Users/Bitdefender/Desktop/BDProfiler.tool;
   ```

7. Premi `Y` e inserisci la password quando ti verrà chiesto di indicare la password dell'amministratore.

   Attendi un paio di minuti finché lo strumento non finisce di generare il registro. Troverai il file di archivio risultante (**Bitdefenderprofile_output.zip**) sul desktop.

17.4. Informazioni di contatto

Una comunicazione efficiente è la chiave di un business di successo. Negli ultimi 18 anni Bitdefender ha acquisito una reputazione inestimabile superando le aspettative di clienti e partner, e sforzandosi costantemente per una comunicazione sempre più efficiente. Se hai delle domande o richieste, non esitare a contattarci.

17.4.1. Indirizzi Web

Dipartimento vendite: enterprisesales@bitdefender.com
Centro di supporto:http://www.bitdefender.com/support/business.html
Documentazione: gravityzone-docs@bitdefender.com
Distributori locali:http://www.bitdefender.it/partners
Programma partner: partners@bitdefender.com
Rapporti con i Media: pr@bitdefender.com
Invio virus: virus_submission@bitdefender.com
Invio spam: spam_submission@bitdefender.com
Segnala abuso: abuse@bitdefender.com
Sito web: http://www.bitdefender.com

17.4.2. Distributori locali

I distributori locali di Bitdefender sono pronti a rispondere a ogni richiesta inerente le loro zone operative, sia in ambito commerciale sia generale.

Per trovare un distributore di Bitdefender nel tuo paese:

1. Visitare http://www.bitdefender.it/partners.
2. Vai a **Trova partner**.
3. Le informazioni di contatto dei distributori locali di Bitdefender dovrebbero essere visualizzate automaticamente. Se non fosse così, seleziona il paese in cui risiedi per visualizzare le informazioni.
4. Se non dovessi trovare un distributore di Bitdefender nel tuo paese, contattaci via e-mail all'indirizzo enterprisesales@bitdefender.com.

17.4.3. Uffici di Bitdefender

Gli uffici di Bitdefender sono sempre pronti a rispondere a ogni richiesta inerente le loro competenze, sia in ambito commerciale sia generale. I loro rispettivi indirizzi e contatti sono elencati sotto.

Stati Uniti

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Telefono (supporto tecnico e vendite): 1-954-776-6262
Vendite: sales@bitdefender.com
Web: http://www.bitdefender.com
Centro di supporto: http://www.bitdefender.com/support/business.html

Francia

Bitdefender
49, Rue de la Vanne
92120 Montrouge
Fax: +33 (0)1 47 35 07 09
Telefono: +33 (0)1 47 35 72 73
E-mail: b2b@bitdefender.fr
Sito web: http://www.bitdefender.fr
Centro di supporto: http://www.bitdefender.fr/support/business.html

Spagna

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª

08037 Barcelona
España
Fax: (+34) 93 217 91 28
Telefono (ufficio e vendite): (+34) 93 218 96 15
Telefono (supporto tecnico): (+34) 93 502 69 10
Vendite: comercial@bitdefender.es
Sito web: http://www.bitdefender.es
Centro di supporto: http://www.bitdefender.es/support/business.html

Germania

Bitdefender GmbH
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Telefono (ufficio e vendite): +49 (0) 2304 94 51 60
Telefono (supporto tecnico): +49 (0) 2304 99 93 004
Vendite: firmenkunden@bitdefender.de
Sito web: http://www.bitdefender.de
Centro di supporto: http://www.bitdefender.de/support/business.html

Regno Unito e Irlanda

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Telefono (supporto tecnico e vendite): (+44) 203 695 3415
E-mail: info@bitdefender.co.uk
Vendite: sales@bitdefender.co.uk
Sito web: http://www.bitdefender.co.uk
Centro di supporto: http://www.bitdefender.co.uk/support/business.html

Romania

BITDEFENDER SRL
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6

Fax: +40 21 2641799
Telefono (supporto tecnico e vendite): +40 21 2063470
Vendite: sales@bitdefender.ro
Sito web: http://www.bitdefender.ro
Centro di supporto: http://www.bitdefender.ro/support/business.html

Emirati Arabi Uniti

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Telefono (supporto tecnico e vendite): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Vendite: sales@bitdefender.com
Web: http://www.bitdefender.com
Centro di supporto: http://www.bitdefender.com/support/business.html

A. Appendici

A.1. Tipi di file supportati

I motori di scansione antimalware inclusi nelle soluzioni di sicurezza di Bitdefender possono esaminare tutti i tipi di file che potrebbero contenere minacce. L'elenco sottostante include i tipi di file più comuni che vengono analizzati.

{*; 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. Tipi di elementi di rete e stati

A.2.1. Tipi elementi di rete

Ogni tipo di elemento disponibile nella pagina **Rete** viene rappresentato da una determinata icona.

Nella tabella presentata di seguito puoi trovare l'icona e la descrizione per tutti i tipi di elemento disponibili.

Icona	Tipo
	Azienda partner
	Azienda cliente
	Insieme aziende
	Rete azienda
	Gruppo rete
	Computer
	Compute relay
	Computer integratore Active Directory
	Computer Server Exchange
	Computer Server Exchange Relay
	Macchina virtuale
	Virtual machine Relay
	Golden image
	Virtual machine Server Exchange
	Virtual machine Server Exchange relay
	Security Server

A.2.2. Stati elementi rete

Ogni elemento di rete può avere diversi stati, relativi allo stato di gestione, problemi di sicurezza, connettività e così via. Nella prossima tabella trovi tutte le icone di stato disponibili e la loro descrizione.

Nota
La tabella sottostante contiene alcuni esempi di stato generici. Gli stessi stati possono applicarsi, singolarmente o combinati, a tutti i tipi di elementi di rete, come gruppi, computer di rete e così via.

Icona	Stato
	Azienda cliente, attiva, autogestita
	Azienda cliente, attiva, gestita da partner
	Azienda cliente, sospesa, autogestita
	Virtual machine, offline, non gestita
	Virtual machine, online, non gestita
	Virtual machine, online, gestita
	Virtual machine, online, gestita, con problemi
	Virtual machine, riavvio in sospeso
	Virtual machine, sospesa
	Virtual machine, eliminata

A.3. Tipi di file applicazioni

I motori di scansione antimalware inclusi nelle soluzioni di sicurezza di Bitdefender possono essere configurati per limitare la scansione solo ai file delle applicazioni (o programmi). I file delle applicazioni sono più vulnerabili agli attacchi dei malware rispetto ad altri tipi di file.

Questa categoria include file con le seguenti estensioni:

```
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. Tipi di file filtro allegati

Il modulo Controllo contenuti offerto da Security for Exchange può filtrare gli allegati e-mail in base al tipo di file. I tipi disponibili nella Control Center includono le seguenti estensioni:

File eseguibili

386; acm; ax; com; cpl; dll; drv; exe; flt; fon; lrc; ocx; scr; sys; vxd; x32

Immagini

bmp; cal; dcx; drw; ds4; eps; gif; gx2; ico; img; jfif; jpe; jpeg; jpg; pat; pcx; pgm; png; psd; psp; rgb; sdr; sh3; shw; sym; tif; tiff; wpg

Multimedia

3g2; 3gg; asf; au; avi; mid; mmf; mov; mp3; mpeg; mpg; ogg; qt; ra; ram; rm; swf; wav; wpl

Archivi

7z; ain; arc; arj; bz; bz2; cab; cpio; cru; crush; gz; hap; img; jar; lha; lzh; pak; ppz; rar; rpm; sit; snp; tar; tar.z; tb2; tbz2; tgz; ufa; z; zip; zoo

Fogli di calcolo

`fm3; ods; wk1; wk3; wks; xls; xlsx`

Presentazioni

`odp; pps; ppt; pptx`

Documenti

`doc; docx; dtd; htm; html; odt; pcx; pdf; qxd; rtf; wks; wpf; ws; ws2; xml`

A.5. Variabili di sistema

Alcune delle impostazioni disponibili nella console richiedono di indicare il percorso dei computer bersaglio. È consigliabile utilizzare variabili di sistema (laddove appropriato) per assicurarsi che il percorso sia valido su tutti i computer di destinazione.

Ecco l'elenco delle variabili di sistema predefinite:

`%ALLUSERSPROFILE%`

La cartella del profilo Tutti gli utenti. Percorso tipico:

`C:\Documents and Settings\All Users`

`%APPDATA%`

La cartella Application Data dell'utente che ha eseguito l'accesso. Percorso tipico:

`C:\Users\{username}\AppData\Roaming`

`%LOCALAPPDATA%`

I file temporanei delle applicazioni. Percorso tipico:

`C:\Users\{username}\AppData\Local`

`%PROGRAMFILES%`

La cartella Program Files. Un percorso tipico è `C:\Program Files`.

`%PROGRAMFILES(X86)%`

La cartella Program Files per le applicazioni a 32 bit (su sistemi a 64 bit). Percorso tipico:

`C:\Program Files (x86)`

`%COMMONPROGRAMFILES%`
La cartella Common Files. Percorso tipico:
`C:\Program Files\Common Files`

`%COMMONPROGRAMFILES(X86)%`
La cartella Common Files per le applicazioni a 32 bit (su sistemi a 64 bit). Percorso tipico:
`C:\Program Files (x86)\Common Files`

`%WINDIR%`
La cartella Windows o SYSROOT. Un percorso tipico è `C:\Windows`.

`%USERPROFILE%`
Il percorso della cartella del profilo utente. Percorso tipico:
`C:\Users\{username}`
Su macOS, la cartella del profilo dell'utente corrisponde alla cartella Home. Usare `$HOME` o `~` quando si configurano le eccezioni.

A.6. Oggetti Sandbox Analyzer

A.6.1. Estensioni e tipi di file supportati per l'invio manuale

Le seguenti estensioni di file sono supportate e possono essere detonate manualmente in Sandbox Analyzer:

`Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archivio), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, file MZ/PE (eseguibile), PDF, PEF (eseguibile), PIF (eseguibile), RTF, SCR, URL (binario), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.`

Sandbox Analyzer è in grado di rilevare i suddetti tipi di file anche se sono inclusi nei seguenti tipi di archivio: `7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.`

A.6.2. Tipi di file supportati da Pre-filtro contenuti per l'invio automatico

Pre-filtro contenuti determinerà un particolare tipo di file, attraverso una combinazione che include il contenuto e l'estensione dell'oggetto. Ciò significa che un eseguibile con estensione `.tmp` verrà riconosciuto come un'applicazione e, se ritenuto sospetto, verrà inviato a Sandbox Analyzer.

- Applicazioni - file in formato PE32, incluse, a titolo esemplificativo, le seguenti estensioni: `exe, dll, com`.
- Documenti - file in formato documento, incluse, a titolo esemplificativo, le seguenti estensioni: `xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm, dotm, potm, potx, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf, pdf`.
- Script: `ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe`.
- Archivi: `zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00`.
- E-mail (salvate nel file system): `eml, tnef`.

A.6.3. Eccezioni predefinite all'invio automatico

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

A.7. Raccolta dati rischio umano

Ci assicuriamo di raccogliere e archiviare temporaneamente i dati sensibili, esclusivamente a livello locale, sulla workstation dell'utente, al solo scopo di generare avvisi su potenziali minacce a cui la tua azienda potrebbe essere esposta dal comportamento dell'utente. Non salviamo dati personali come nome utenti e password in testo semplice in qualsiasi database cloud.

I dati locali che raccogliamo vengono eliminati periodicamente e possono includere solo hash di nomi utenti e password, il numero totale di siti web rischiosi a cui hanno avuto accesso in un determinato periodo di tempo e gli URL di alcuni di questi siti web sospetti, oltre agli IP dei loro domini.

La seguente tabella descrive quali comportamenti dell'utente ERA sta monitorando e il modo in cui elabora e raccoglie i dati dell'utente.

Nome regola	Descrizione	Tipo	Dati raccolti
Credenziali plain HTTP	Verifica se l'utente ha inviato o no le credenziali su connessioni HTTP non sicure dall'ultima scansione.	password	Verifica se l'utente utilizza le stesse password su diversi siti esterni. Questo scenario viene attivato quando rileviamo almeno due siti web esterni con la stessa password.
Password HTTP condivisa esternamente	Controlliamo per vedere se l'utente accede a siti web non sicuri (HTTP) e memorizza il numero di siti web a cui si accede, e i relativi timestamp.	password	Memorizziamo localmente l'hash delle password (formato CRC32) immesse in siti esterni, oltre agli URL a cui si accede, gli IP dei domini e il nome utente.
Password HTTP interna condivisa esternamente	Verifica se l'utente utilizza le stesse password condivise tra siti web interni ed esterni.	password	Memorizziamo localmente l'hash delle password (formato CRC32) immesse in siti interni ed esterni, oltre agli URL a cui si accede e gli IP dei domini.
Navigazione ad alto rischio	Verifica se l'utente ha visitato i siti indicati come phishing o fraudolenti dall'ultima scansione. Questo scenario si attiva quando il numero di siti web insicuri a cui si accede supera la soglia attuale.	navigazione	Memorizziamo solo localmente il numero di siti web ad alto rischio a cui si accede e i loro URL, durante un determinato intervallo di tempo.
Conteggio di rilevamento elevato	Verifica se l'utente è stato esposto a un numero elevato di minacce	rilevamenti	Memorizziamo localmente il numero di rilevamenti attivati durante un

Nome regola	Descrizione	Tipo	Dati raccolti
	dall'ultima scansione. Lo scenario si attiva quando il numero di rilevamenti per utente supera la soglia predefinita.		determinato intervallo di tempo.
Infezione dispositivo rimovibile	Verifica se l'utente è stato esposto a una minaccia da un dispositivo rimovibile (ad esempio chiavette USB e hard disk esterni) dall'ultima scansione.	rilevamenti	Memorizziamo localmente i rilevamenti attivati durante un determinato intervallo di tempo con la fonte dell'infezione (USB/CD/file ISO).
Infezione SMB	Verifica se l'utente ha effettuato l'accesso a file dannosi su una cartella condivisa di rete dall'ultima scansione.	rilevamenti	Memorizziamo localmente gli eventi di accesso al file che si originano da cartelle di rete condivise o punti di condivisione.
Infezione navigazione	Verifica se l'utente ha avuto accesso a URL dannosi dall'ultima scansione.	rilevamenti	Memorizziamo localmente gli URL dannosi/sospetti e li conteggiamo.
Elevato numero di rilevamenti nel tempo	Verifica se l'utente è esposto a un elevato numero di minacce durante un determinato intervallo di tempo.	rilevamenti	Memorizziamo localmente il numero di infezioni durante un determinato intervallo di tempo.
Password HTTP condivisa esternamente	Verifica se l'utente non ha modificato periodicamente le password per siti web esterni.	password	Memorizziamo localmente: hash delle password (formato CRC32), hash del nome utente e gli URL dei siti web esterni che hanno attivato questo comportamento, oltre agli IP del dominio.

Nome regola	Descrizione	Tipo	Dati raccolti
Vecchia password utente	Verifica se l'utente non ha modificato la password di accesso per l'account (locale o dominio) per più di 30 giorni.	password	Non memorizziamo nulla localmente. Eseguiamo una query su una funzione di Active Directory che indica l'ultima volta in cui la password di un utente è stata modificata.

Glossario

Adware

La modalità adware è spesso combinata con un'applicazione che viene fornita gratuitamente se l'utente accetta l'adware. Considerando che le applicazioni adware vengono di solito installate dopo che l'utente ha accettato l'accordo di licenza, dove viene spiegato il proposito dell'applicazione, non viene commessa alcuna infrazione.

Comunque, le finestre pop-up di avvertimento possono essere fastidiose e in alcuni casi ridurre le prestazioni del sistema. Inoltre, le informazioni che vengono raccolte da alcune di queste applicazioni possono causare inconvenienti riguardo la privacy degli utenti, non sempre completamente informati sui termini dell'accordo di licenza.

Aggiornamento

Una nuova versione di un prodotto software o hardware creato per sostituire la versione precedente. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul computer, diversamente non sarà possibile installare l'aggiornamento.

Bitdefender ha un proprio modulo di aggiornamento che consente la verifica manuale degli aggiornamenti oppure l'aggiornamento automatico del prodotto.

Archivio

Un Disco, un nastro o una cartella che contiene file memorizzati.

Un file che contiene uno o più file in forma compressa.

Area di notifica

Introdotta con Windows 95, l'area di notifica è situata nella barra delle applicazioni di Windows (in genere in basso vicino all'orologio) e contiene icone miniaturizzate per un accesso veloce a funzioni di sistema come fax, stampante, modem, volume e molto altro. Clicca due volte o clicca con il pulsante destro su un'icona per visualizzare e accedere ai dettagli e i controlli.

Attacchi mirati

Gli attacchi informatici che puntano principalmente a guadagni finanziari o a rovinare una reputazione. Il bersaglio può essere un individuo, un'azienda, un

software o un sistema, ben studiato prima che l'attacco avvenga. Questi attacchi vengono eseguiti per un lungo periodo di tempo e per fasi, usando uno o più punti d'infiltrazione. Vengono notati difficilmente, e la maggior parte delle volte quando il danno è già stato fatto.

Backdoor

Una breccia nella sicurezza di un sistema deliberatamente lasciata dal programmatore o dal manutentore. La presenza di tali "brecce" non sempre è dolosa: su alcuni sistemi operativi, ad esempio, vengono utilizzate per l'accesso con utenze privilegiate per servizi tecnici o per i programmatori del produttore a scopo di manutenzione.

Bootkit

Un bootkit è un programma dannoso che ha la capacità di infettare il master boot record (MBR), il volume boot record (VBR) o il settore di boot. Il bootkit resta attivo anche dopo un riavvio del sistema.

Browser

Abbreviazione di browser web, un'applicazione software utilizzata per localizzare e visualizzare pagine web.

Cookie

Nell'industria di Internet, i cookie vengono descritti come piccoli file contenenti informazioni relative ai computer individuali che possono essere analizzate e utilizzate dai pubblicitari per tenere traccia di interessi e gusti online degli utenti. In questo settore, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di fornire offerte pubblicitarie personalizzate in base agli interessi degli utenti. Per molte persone è una lama a doppio taglio, poiché da una parte è efficace e consente di far vedere solo ciò che viene dichiarato interessante. Ma dall'altra, implica in effetti un "tracciamento" di dove si va e di cosa si seleziona. In considerazione di questo è in atto un dibattito relativo alla riservatezza e molte persone si sentono offese all'idea di essere visti come un "codice SKU" (il codice a barre sul retro delle confezioni che viene letto dalle casse). Se questo punto di vista può essere considerato estremo, in alcuni casi può essere corretto.

Estensione del nome di un file

Porzione del nome di un file che segue il punto finale e che indica il tipo di dati inclusi nel file.

Molti sistemi operativi utilizzano estensioni di file, come Unix, VMS e MS-DOS. Sono normalmente composti da una a tre lettere (alcuni vecchi sistemi operativi non ne supportano più di tre). Esempi: "c" per codici sorgente C, "ps" per PostScript, "txt" per testi semplici.

Euristico

Un metodo basato su regole per l'identificazione di nuovi virus. Questo metodo di scansione non si basa su specifiche firme dei virus. Il vantaggio della scansione euristica è di non essere ingannata dalle nuove varianti dei virus esistenti. Tuttavia, può occasionalmente segnalare una parte di codice sospetto in programmi normali, generando i cosiddetti "falsi positivi".

Eventi

Un'azione oppure un evento segnalato da un programma. Gli eventi possono essere azioni dell'utente, come cliccare con il mouse o premere un tasto sulla tastiera, oppure del sistema, come l'esaurimento della memoria.

Exploit

In genere, un exploit è un qualsiasi metodo usato per ottenere accesso non autorizzato ai computer o una vulnerabilità nella sicurezza di un sistema che rende vulnerabile il sistema a un attacco.

Falso positivo

Appare quando un prodotto di analisi antivirus individua un documento come infettato quando di fatto non lo è.

File di rapporto

Un file che elenca le azioni avvenute. Bitdefender crea un rapporto che elenca i percorsi controllati, le cartelle, il numero di archivi e file esaminati, oltre a quanti file infetti e sospetti sono stati trovati.

File sospetti e traffico di rete

I file sospetti sono quelli con una reputazione piuttosto dubbia. Questa classifica è data da molti fattori, tra cui: l'esistenza della firma digitale, il numero di occorrenze nelle reti di computer, il packer usato, ecc. Il traffico di rete viene considerato sospetto quando si discosta dal modello. Per esempio, una sorgente inaffidabile, richieste di connessione a porte insolite, un maggiore uso della banda, tempi di connessione casuali, ecc.

Firma malware

Le firme malware sono frammenti di codice estratti da campioni attuali di malware. Sono usate dai programmi antivirus per eseguire confronti di esempi e rilevare i malware. Le firme vengono usate anche per rimuovere il codice malware dai file infetti.

Il database di firme malware di Bitdefender è una raccolta di firme malware aggiornato continuamente dai ricercatori malware di Bitdefender.

Grayware

Una classe di applicazioni software tra software legittimi e malware. Anche se non sono dannosi come i malware che possono influenzare l'integrità del sistema, il loro comportamento è comunque fastidioso, portando a situazioni non desiderate, come furto di dati, uso non autorizzato e pubblicità non gradita. Le applicazioni grayware più comuni sono spyware e adware.

IOR

Indicatore di rischio - si riferisce a un valore di chiave di registro o ai dati di una specifica impostazione del sistema, o una vulnerabilità nota di un'applicazione.

IP

Internet Protocol – protocollo di instradamento nella suite di protocollo TCP/IP, responsabile dell'indirizzamento IP, dell'instradamento, della frammentazione e della ricomposizione dei pacchetti IP.

Keylogger

Un keylogger è un'applicazione che registra ogni informazione digitata.

I keylogger non sono dannosi di natura. Possono essere usati anche per scopi legittimi, come monitorare le attività di dipendenti o bambini. Tuttavia, sono utilizzati anche dai criminali informatici per scopi dannosi (per esempio, ottenere dati personali, come credenziali o codici di accesso).

Linea di comando

In un'interfaccia a linea di comando, l'utente digita i comandi nello spazio previsto direttamente sullo schermo, utilizzando il linguaggio di comando.

Livelli di protezione

GravityZone fornisce protezione attraverso una serie di moduli e ruoli, collettivamente denominati livelli di protezione, suddivisi in Protezione per Endpoint (EPP) o protezione principale, e vari componenti aggiuntivi. La

Protezione per Endpoint include Antimalware, Advanced Threat Control, Advanced Anti-Exploit, Firewall, Controllo contenuti, Controllo dispositivi, Network Attack Defense, Utente esperto e Relay. Gli add-on includono diversi livelli di protezione come Security for Exchange e Sandbox Analyzer.

Per maggiori dettagli sui livelli di protezione disponibili con la tua soluzione GravityZone, fai riferimento a «Livelli di protezione di GravityZone» (p. 2).

Macro virus

Un tipo di virus informatico, codificato come macro all'interno di un documento. Molte applicazioni, come ad esempio Microsoft Word ed Excel, supportano potenti linguaggi macro.

Queste applicazioni consentono di codificare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Malware

Malware è un termine generico per software progettati appositamente per essere dannosi, un'abbreviazione di "software dannoso" (in inglese "malicious software"). Non è ancora usato in maniera universale, ma la sua popolarità come termine generale per indicare virus, Trojan, worm e codice mobile dannoso sta aumentando.

Malware

Un programma o parte di codice caricato sul computer a propria insaputa e che viene eseguito contro la propria volontà. La maggior parte dei virus è anche in grado di auto replicarsi. Tutti i virus informatici sono creati dall'uomo. È relativamente facile produrre un semplice virus in grado di copiare sé stesso innumerevoli volte. Persino un virus così semplice è pericoloso in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di virus ancora più pericoloso è quello in grado di trasmettere sé stesso attraverso le reti superando i sistemi di sicurezza.

Non euristico

Questo metodo di scansione si basa su specifiche firme di virus. Il vantaggio della scansione non-euristica è di non essere ingannata da ciò che potrebbe sembrare un virus, e quindi non genera falsi allarmi.

Phishing

L'atto d'inviare un'e-mail a un utente fingendo di essere una società legittima e affermata, nel tentativo di truffarlo, facendogli cedere informazioni private

che saranno usate per furti d'identità. L'e-mail invita gli utenti a visitare un sito web, dove gli sarà chiesto di aggiornare determinate informazioni personali, come password e numero di carta di credito, codice fiscale o coordinate bancarie, che l'azienda legittima ovviamente possiede già. In ogni caso, la pagina web è falsa e creata solo per rubare i dati personali dell'utente.

Porta

Un'interfaccia su un computer dalla quale è possibile connettere un dispositivo. I personal computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, monitor e tastiere. Esternamente i personal computer hanno porte per la connessione di modem, stampanti, mouse e altre periferiche.

Nelle reti TCP/IP e UDP, un endpoint per una connessione logica. Il numero della porta ne identifica il tipo. Ad esempio, la porta 80 viene usata per il traffico HTTP.

Programma di download Windows

È il nome generico di un programma che ha come funzionalità principale quella di scaricare contenuti a scopi indesiderati o dannosi.

Ransomware

Un malware che ti isola dal tuo computer o blocca l'accesso ai tuoi file e applicazioni. Un ransomware ti chiederà di pagare un determinato costo (riscatto), in cambio di una chiave di decifrazione che ti consente di riottenere l'accesso al tuo computer o ai tuoi file.

Rootkit

Un rootkit è una serie di strumenti software che consente di accedere a un sistema come amministratore. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la propria presenza, in modo da non essere visti dagli amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, gli accessi e i registri. Se incorporano il software adeguato, possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche.

I rootkit non sono dannosi per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando i rootkit. Comunque, vengono principalmente utilizzati per nascondere malware o per celare la presenza di

un intruso nel sistema. Se combinati ai malware, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e registri, ed evitare il rilevamento.

Script
Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Settore di avvio:
Un settore all'inizio di ogni disco che ne identifica l'architettura (dimensione del settore, dimensione del cluster, ecc.). Nei dischi di avvio, il settore di boot contiene anche un programma che carica il sistema operativo.

Sottrazione di password
Un password stealer raccoglie parti di dati che possono essere nomi di account e le relative password. Tali credenziali rubate vengono poi usate per scopi dannosi, come il furto di account.

Spam
Messaggi di posta elettronica o newsgroup indesiderati. Generalmente conosciuto come e-mail non desiderate.

Spyware
Qualsiasi software che raccoglie segretamente informazioni dell'utente tramite la sua connessone a Internet, senza che questo se ne accorga, di solito per scopi pubblicitari. Le applicazioni spyware in genere sono incluse come componente nascosta di programmi freeware o shareware, che possono essere scaricati da Internet. Tuttavia, occorre segnalare che la maggioranza delle applicazioni shareware o freeware non includono alcun programma spyware. Una volta installato, uno spyware monitora le attività dell'utente su Internet e trasmette di nascosto tali informazioni a qualcun altro. Gli spyware possono anche raccogliere informazioni su indirizzi e-mail o addirittura password e numeri di carta di credito.

Gli spyware sono simili a un cavallo di Troia che gli utenti installano inconsapevolmente con altre applicazioni. Un modo comune per diventare vittima degli spyware è utilizzare i programmi peer-to-peer attuali per condividere e scaricare file.

Oltre a questioni di etica e privacy, gli spyware sottraggono risorse di memoria al computer, "mangiandosi" larghezza di banda poiché inviano informazioni alla propria "base" usando la connessione internet dell'utente. Poiché gli spyware utilizzano memoria e risorse del sistema, le applicazioni eseguite in background possono provocare instabilità o blocchi del sistema.

Storm di scansione antimalware

Un intenso uso delle risorse del sistema che si verifica quando un software antivirus esamina contemporaneamente più virtual machine su un solo host fisico.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di rete largamente utilizzati su Internet, che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il relativo traffico.

Trojan

Un programma distruttivo che si maschera da applicazione benevola. Diversamente dai virus, i cavalli di Trojan non si replicano ma possono comunque essere altrettanto distruttivi. Un tipo di cavallo di Troia particolarmente insidioso è un programma che dichiara di pulire i virus dal computer, ma al contrario li introduce.

Il termine deriva da una storia dell'Iliade di Omero, in cui i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e conquistare Troia.

Virus di boot

Un virus che infetta il settore di avvio di un disco rigido oppure di un'unità floppy. Qualsiasi tentativo di effettuare il boot da un disco floppy infettato con un virus di boot, farà sì che il virus venga attivato in memoria. Da quel momento in poi, ogni volta che si esegue il boot del sistema, il virus sarà attivo in memoria.

Virus polimorfico

Un virus che modifica la propria forma con ogni file che infetta. Non avendo caratteristiche binarie costanti, questi virus sono difficili da identificare.

Worm

Un programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.