Bitdefender

GravityZone

INSTALLAZIONE

Bitdefender GravityZone
Installazione

Data di pubblicazione 2021.01.12

Avvertenze legali

Bitdefender

Indice

Prefazione

Questa guida è rivolta agli amministratori IT responsabili dell'impiego della protezione di GravityZone nelle sedi della propria organizzazione. In questa guida, i responsabili IT in cerca di informazioni su GravityZone possono trovare i requisiti di GravityZone e i moduli di protezione disponibili.

Questo documento intende spiegare come impiegare gli agenti di sicurezza di Bitdefender in tutti i tipi di endpoint nella propria azienda, e come configurare la soluzione di GravityZone.

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. v)	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 una soluzione di sicurezza aziendale sviluppata da zero per il cloud e la virtualizzazione con l'obiettivo di offrire servizi di sicurezza a endpoint fisici, macchine virtuali in cloud pubblici e privati e mail server Exchange.

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.

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.
Oltre alla protezione di Microsoft Exchange, la licenza copre anche i moduli di protezione endpoint installati sul server.

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.

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.

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. Security for Storage

GravityZone Security for Storage offre la migliore protezione in tempo reale per i principali sistemi di condivisione di file e archiviazione in rete. Sia il sistema che gli algoritmi di rilevazione delle minacce si aggiornano automaticamente, senza richiedere alcun intervento da parte tua e interrompere l'attività dei tuoi utenti finali.

Due o più Security Server di GravityZone multipiattaforma svolgono il ruolo di server ICAP fornendo servizi antimalware ai dispositivi Network-Attached Storage (NAS) e sistemi di condivisione dei file conformi al protocollo ICAP (Internet Content Adaptation Protocol, come definito in RFC 3507).

Quando un utente chiede di aprire, leggere, scrivere o chiudere un file da un portatile, una postazione di lavoro, una piattaforma mobile o un altro dispositivo, il client ICAP (un NAS o un sistema di condivisione di file) invia una richiesta di scansione al Security Server e riceve un verdetto relativo al file. In base al risultato, il Security Server consente l'accesso, nega l'accesso o elimina il file.

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

2.17. 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.

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
- 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 a «Sistemi operativi supportati» (p. 20).

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

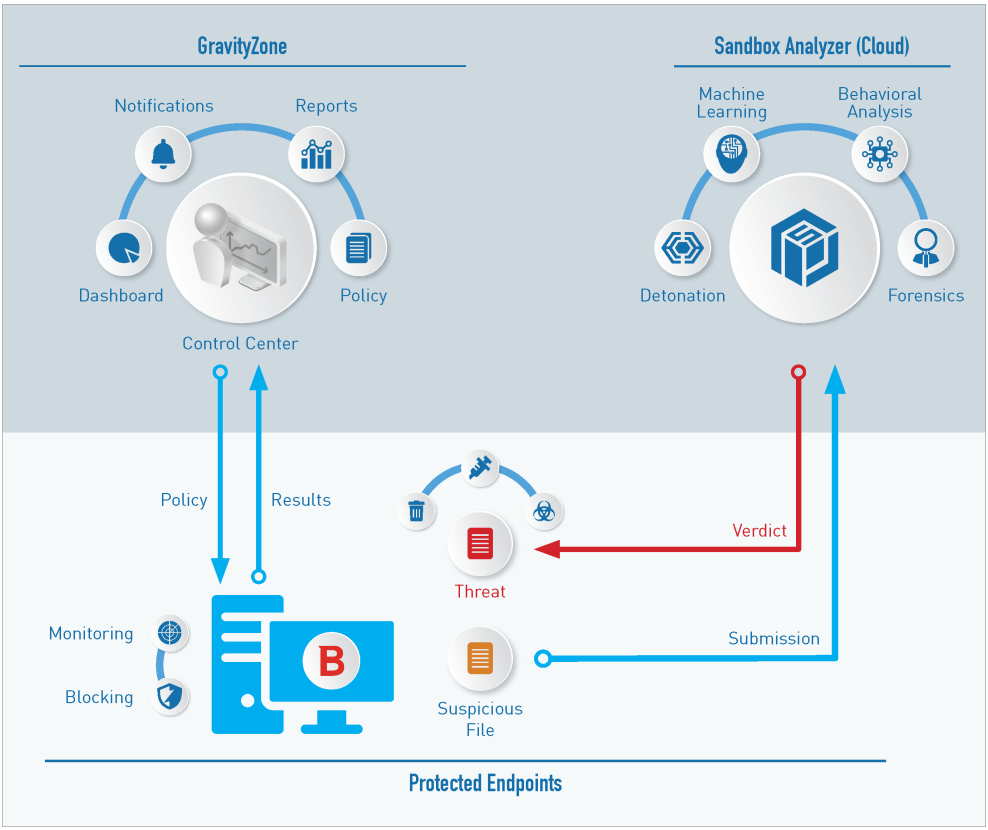
Bitdefender Sandbox Analyzer fornisce un potente livello di protezione dalle minacce avanzate, eseguendo un'analisi automatica e approfondita dei file sospetti non ancora firmati dai motori antimalware di Bitdefender.

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.

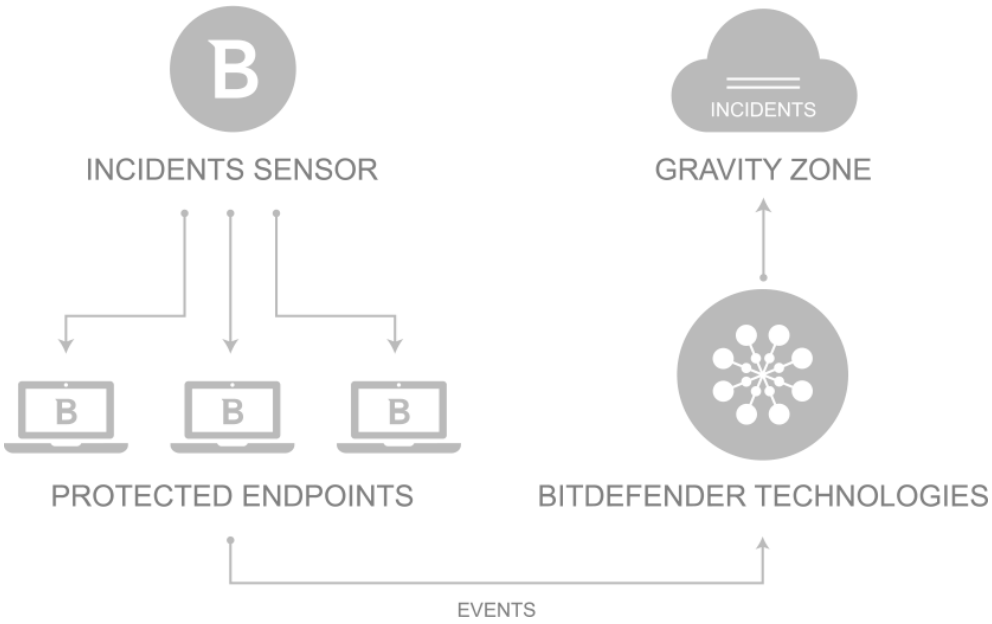
I risultati delle analisi sono conservati tramite un valore di hash del file nel database di Sandbox Analyzer. Quando un file analizzato in precedenza viene inviato da un altro endpoint, si ottiene una risposta immediata, perché i risultati sono già disponibili nel database.

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. REQUISITI

Tutte le soluzioni di GravityZone sono installate e gestite tramite la Control Center.

4.1. Control Center

Per accedere alla console web Control Center, serve:

- 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.

4.2. Protezione degli endpoint

Per proteggere la tua rete con Bitdefender, devi installare gli agenti di sicurezza di GravityZone negli endpoint della rete. Per una protezione ottimizzata, puoi installare anche Security Server.A tale scopo, ti serve un utente Control Center con privilegi di amministratore sui servizi che devi installare e gli endpoint di rete sotto la tua gestione.

I requisiti per l'agente di sicurezza sono diversi, in base alla presenza di eventuali ruoli server aggiuntivi, come Relay, Protezione Exchange o Patch Caching Server. Per maggiori informazioni sui ruoli dell'agente, fai riferimento a «Agenti di sicurezza» (p. 9).

4.2.1. Hardware

Agente di sicurezza senza ruoli

Uso CPU

Sistemi bersaglio	Tipo CPU	Sistemi operativi supportati (OS)
Workstation	Processori compatibili Intel® Pentium, 2 GHz o superiori	Sistemi operativi desktop di Microsoft Windows
	Intel® Core 2 Duo, 2 GHz o superiore	macOS
Dispositivi smart	Processori compatibili Intel® Pentium, 800 MHz o superiori	Sistemi operativi Microsoft Windows embedded
Server	Requisiti minimi: processori compatibili Intel® Pentium a 2,4 GHz	Sistemi operativi Microsoft Windows server e Linux
	Requisiti consigliati: processore Intel® Xeon multi-core, 1.86 GHz o superiore	

Avvertimento
Al momento i processori ARM non sono supportati.

Memoria RAM libera

All'installazione (MB)

SO	SINGOLO MOTORE					
	Scansione locale		Scansione ibrida		Scansione centralizzata	
	Solo AV	Tutte le opzioni	Solo AV	Tutte le opzioni	Solo AV	Tutte le opzioni
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
macOS	1024	1024	N/D	N/D	N/D	N/D

Per uso giornaliero (MB)*

SO	Antivirus (singolo motore)			Moduli di protezione				
	Locale	Ibrida	Centralizzata	Scans. comportamentale	Firewall	Controllo contenuti	Utente esperto	ag
Windows	75	55	30	+13	+17	+41	+29	
Linux	200	180	90	-	-	-	-	
macOS	650	-	-	+100	-	+50	-	

* I valori si riferiscono a un utilizzo del client endpoint giornaliero, senza considerare eventuali attività aggiuntive, come scansioni a richiesta o aggiornamenti del prodotto.

Spazio libero su disco rigido

All'installazione (MB)

SO	SINGOLO MOTORE						DOPPIO MOTORE			
	Scansione locale		Scansione ibrida		Scansione centralizzata		Centralizzata + Scansione locale		Centralizzata + Scansione ibrida	
	Solo AV	Tutte le opzioni	Solo AV	Tutte le opzioni	Solo AV	Tutte le opzioni	Solo AV	Tutte le opzioni	Solo AV	Tutte le opzioni
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1600	1600	1100	1100	600	600	1600	1600	1100	1100
macOS	1024	1024	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D

Per uso giornaliero (MB)*

SO	Antivirus (singolo motore)			Moduli di protezione				
	Locale	Ibrida	Centralizzata	Scans. comportamentale	Firewall	Controllo contenuti	Utente esperto	a
Windows	410	190	140	+12	+5	+60	+80	
Linux	500	200	110	-	-	-	-	
macOS	1700	-	-	+20	-	+0	-	

* I valori si riferiscono a un utilizzo del client endpoint giornaliero, senza considerare eventuali attività aggiuntive, come scansioni a richiesta o aggiornamenti del prodotto.

Agente di sicurezza con ruolo di relay

Il ruolo di relay richiede risorse hardware aggiuntive alla configurazione dell'agente di sicurezza base. Questi requisiti sono per supportare il server di aggiornamento e i pacchetti di installazione ospitati dall'endpoint:

Numero di endpoint connessi	Processore per supportare il server di aggiornamento	RAM	Spazio libero su disco per il server di aggiornamento
1-300	Minimo processore Intel® Core™ i3 o equivalente, 2 vCPU per core	1,0 GB	10 GB
300-1000	Minimo processore Intel® Core™ i5 o equivalente, 4 vCPU per core	1,0 GB	10 GB

Avvertimento

- Al momento i processori ARM non sono supportati.
- Gli agenti relay richiedono dischi SSD per supportare l'elevato ammontare di operazioni di lettura/scrittura.

Importante

- Se vuoi salvare i pacchetti di installazione e gli aggiornamenti per un'altra partizione rispetto a quella in cui è stato installato l'agente, assicurati che entrambe le partizioni abbiano sufficiente spazio libero sul disco (10 GB), altrimenti l'agente annullerà l'installazione. Ciò è richiesto solo all'installazione.
- Sugli endpoint Windows, è necessario attivare i collegamenti simbolici da locale a locale.

Agente di sicurezza con ruolo di protezione Exchange

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.

Di norma, l'agente viene installato sulla partizione del sistema.

Agente di sicurezza con ruolo Patch Caching Server

L'agente con ruolo Patch Caching Server deve soddisfare i seguenti requisiti cumulativi:

- Tutti i requisiti hardware dell'agente di sicurezza semplice (senza ruoli)
- Tutti i requisiti hardware del ruolo relay
- In aggiunta 100 GB di spazio libero su disco per memorizzare le patch scaricate

Importante
Se vuoi salvare le patch per un'altra partizione rispetto a quella in cui è stato installato l'agente, assicurati che entrambe le partizioni abbiano sufficiente spazio libero sul disco (100 GB), altrimenti l'agente annullerà l'installazione. Ciò è richiesto solo all'installazione.

4.2.2. Sistemi operativi supportati

Windows Desktop

- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 November 2019 Update (19H2)
- Windows 10 May 2019 Update (19H1)
- Windows 10 October 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1
- Windows 8

- Windows 7

Avvertimento
Bitdefender non supporta build del Programma Windows Insider.

Windows Tablet e Embedded

- Windows 10 IoT Enterprise
- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7

Windows Server

- Windows Server 2019
- Windows Server 2019 Core
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

Linux

Importante
Gli endpoint Linux usano set di licenze provenienti dai pool di licenze per sistemi operativi dei server.

- Ubuntu 14.04 LTS o superiore
- Red Hat Enterprise Linux / CentOS 6.0 o superiore(2)
- SUSE Linux Enterprise Server 11 SP4 o superiore

- OpenSUSE Leap 42.x
- Fedora 25 o superiore(1)
- Debian 8.0 o superiore
- Oracle Linux 6.3 o più recente
- Amazon Linux AMI 2016.09 o superiore
- Amazon Linux 2

Avvertimento

(1) Su Fedora 28 e versioni successive, Bitdefender Endpoint Security Tools richiede l'installazione manuale del pacchetto `libnsl`, eseguendo il seguente comando:

```
sudo dnf install libnsl -y
```

(2) Per le installazioni minime di CentOS, Bitdefender Endpoint Security Tools richiede l'installazione manuale del pacchetto `libnsl`, eseguendo il seguente comando:

```
sudo yum install libnsl
```

Prerequisiti Active Directory

Integrando gli endpoint Linux con un dominio Active Directory tramite il System Security Services Daemon (SSSD), assicurati che gli strumenti **ldbsearch, krb5-user** e **krb5-config** siano installati e che kerberos sia configurato correttamente.

```
/etc/krb5.conf

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
        default_realm = DOMAIN.NAME
        dns_lookup_realm = true
        dns_lookup_kdc = true
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
```

```
        proxiable = true
        fcc-mit-ticketflags = true
        default_keytab_name = FILE:/etc/krb5.keytab

[realms]
        DOMAIN.NAME = {
                        kdc = dc1.domain.name
                        kdc = dc2.domain.name
                        admin_server = dc.domain.com
                        default_domain = domain.com
        }

[domain_realm]
 domain.name = DOMAIN.NAME
 .domain.name = DOMAIN.NAME

[appdefaults]
 pam = {
        debug = false
        ticket_lifetime = 36000
        renew_lifetime = 36000
        forwardable = true
        krb4_convert = false
        }
```

Nota
Tutti i valori sono sensibili alle lettere maiuscole/minuscole.

Supporto scansione a richiesta

La scansione a richiesta è disponibile per tutti i sistemi operativi guest supportati. Nei sistemi Linux, il supporto per la scansione a richiesta viene fornito nelle seguenti situazioni:

Versioni kernel	Distribuzioni Linux	Requisiti all'accesso
2.6.38 o superiore*	Red Hat Enterprise Linux / CentOS 6.0 o superiore Ubuntu 14.04 o superiore	**Fanotify** (opzione kernel) deve essere attivata.

Versioni kernel	Distribuzioni Linux	Requisiti all'accesso
	SUSE Linux Enterprise Server 11 SP4 o superiore OpenSUSE Leap 42.x Fedora 25 o superiore Debian 9.0 o superiore Oracle Linux 6.3 o più recente Amazon Linux AMI 2016.09 o superiore	
2.6.38 o superiore	Debian 8	**Fanotify** deve essere attivata e impostata in modalità enforcing. Inoltre, il pacchetto del kernel deve essere ricostruito. Per maggiori dettagli, fai riferimento a questo articolo della KB.
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender fornisce supporto via **DazukoFS** con moduli kernel predefiniti.
Tutti gli altri kernel	Tutti gli altri sistemi supportati	Il modulo **DazukoFS** deve essere compilato manualmente. Per maggiori dettagli, fai riferimento a «Compila manualmente il modulo DazukoFS» (p. 57).

* Con determinate limitazioni descritte in basso.

Limitazioni scansione all'accesso

Versioni kernel	Distribuzioni Linux	Dettagli
2.6.38 o superiore	Tutti i sistemi supportati	La scansione a richiesta monitora le condivisioni di rete installate solo in queste condizioni: • **Fanotify** è attivato sia su sistemi locali che remoti. • La condivisione è basata sui file system CIFS e NFS. **Nota** La scansione a richiesta non esamina le condivisioni di rete installate utilizzando SSH o FTP.
Tutti i kernel	Tutti i sistemi supportati	La scansione all'accesso non è supportata su sistemi con **DazukoFS** per condivisioni di rete montate su percorsi già protetti dal modulo All'accesso.

Supporto Endpoint Detection and Response (EDR)

Vai a questa pagina web per un elenco completo e aggiornato delle versioni del kernel e delle distribuzioni Linux che supportano il sensore EDR.

macOS

- macOS Big Sur (11.0)*
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

Controllo contenuti non è supportato in macOS Big Sur (11.0).

4.2.3. File system supportati

Bitdefender si installa e protegge i seguenti file system:

AFS, BTRFS, ext2, ext3, ext4, FAT, FAT16, FAT32, VFAT, exFAT, NTFS, UFS, ISO 9660 / UDF, NFS, CIFS/SMB, VXFS, XFS.

Nota
Il supporto per la scansione a richiesta non è fornito per NFS e CIFS/SMB.

4.2.4. Browser supportati

La sicurezza per i browser degli endpoint risulta funzionante con i seguenti browser:

- Internet Explorer 8+
- Mozilla Firefox 30+
- Google Chrome 34+
- Safari 4+
- Microsoft Edge 20+
- Opera 21+

4.2.5. Security Server

Security Server è una macchina virtuale preconfigurata che funziona su un Server Ubuntu 12.04 LTS (3.2 kernel).

Piattaforme di virtualizzazione

Bitdefender Security Server può essere installato sulle seguenti piattaforme di virtualizzazione:

- VMware vSphere & vCenter Server 7.0, 6.7 update 3, update 2a, 6.7 update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0

  Nota
  La funzionalità Workload Management in vSphere 7.0 non è supportata.

- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6

- VMware Player 7.x, 6.x, 5.x
- Citrix XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (incluso Xen Hypervisor)
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp e XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 o Windows Server 2008 R2, 2012, 2012 R2 (incluso Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (incluso KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism con AOS 5.5, 5.10, 5.15 LTS
- Nutanix Prism con AOS 5.6, 5.11 STS
- Nutanix Prism con AHV 20170830.115, 20170830.301 e 20170830.395 Community Edition
- Nutanix Prism versione 2018.01.31 (Community Edition)

Nota
Il supporto per altre piattaforme di virtualizzazione può essere fornito su richiesta.

Memoria e CPU

L'assegnazione delle risorse di memoria e CPU per il Security Server dipende dal numero e dal tipo di VM in esecuzione sull'host. La seguente tabella elenca le risorse consigliate da assegnare:

Numero di VM protette	RAM	CPU
1-50 VM	2 GB	2 CPU
51-100 VM	2 GB	4 CPU
101-200 VM	4 GB	6 CPU

Spazio su disco rigido

Occorre mantenere 8 GB di spazio sul disco su ciascun host di Security Server.

Distribuzione di Security Server su host

Anche se non è obbligatorio, Bitdefender consiglia di installare Security Server su ogni host fisico per ottenere prestazioni migliori.

Latenza di rete

La latenza delle comunicazioni tra Security Server e gli endpoint protetti deve essere inferiore a 50 ms.

Carico di Protezione archiviazione

L'impatto della Protezione archiviazione sul Security Server durante la scansione di 20 GB è il seguente:

Stato Protezione archiviazione	Risorse del Security Server	Caricamento Security Server	Tempo di trasferimento (mm:ss)
Disattivato (riferimento)	N/A	N/A	10:10
Attivato	4 vCPU 4 GB RAM	Normale	10:30
Attivato	2 vCPU 2 GB RAM	Pesante	11:23

Nota
Questi risultati sono stati ottenuti con un campione di diversi tipi di file (.exe, .txt, .doc, .eml, .pdf, .zip etc.), che spaziano da 10 KB a 200 MB. La durata del trasferimento corrisponde a 20 GB di dati contenuti in 46.500 file.

4.2.6. Uso del traffico

- **Traffico dell'aggiornamento dei prodotti tra il client endpoint e il server di aggiornamento**

  Ogni aggiornamento periodico del prodotto Bitdefender Endpoint Security Tools genera il seguente traffico di download in ciascun client endpoint:

  - Su SO Windows: ~20 MB
  - Su SO Linux: ~26 MB

- Su macOS: ~25 MB

- **Traffico degli aggiornamenti del contenuto di sicurezza scaricati tra il client endpoint e il server di aggiornamento (MB / giorno)**

Tipo di server di aggiornamento	Tipo di motore di scansione		
	Locale	Ibrida	Centralizzata
Relay	65	58	55
Server di aggiornamento pubblico di Bitdefender	3	3.5	3

- **Traffico della scansione centralizzata tra il client endpoint e Security Server**

Oggetti esaminati	Tipo di traffico		Download (MB)	Upload (MB)
File*	Prima scansione		27	841
	Scansione nella cache		13	382
Siti web**	Prima scansione	Traffico web	621	N/A
		Security Server	54	1050
	Scansione nella cache	Traffico web	654	N/A
		Security Server	0.2	0.5

* I dati forniti sono stati misurati per file di 3,49 GB (6.658 file) di cui 1,16 GB sono file Portable Executable (PE).

** I dati forniti sono stati misurati per i migliori 500 siti web.

- **Traffico della scansione ibrida tra il client endpoint e i servizi cloud di Bitdefender**

Oggetti esaminati	Tipo di traffico	Download (MB)	Upload (MB)
File*	Prima scansione	1.7	0.6
	Scansione nella cache	0.6	0.3
Traffico web**	Traffico web	650	N/A
	Servizi Cloud di Bitdefender	2.6	2.7

* I dati forniti sono stati misurati per file di 3,49 GB (6.658 file) di cui 1,16 GB sono file Portable Executable (PE).

** I dati forniti sono stati misurati per i migliori 500 siti web.

Nota
La latenza della rete tra il client endpoint e il server cloud di Bitdefender deve essere inferiore a 1 secondo.

- **Traffico tra i client Bitdefender Endpoint Security Tools Relay e il server di aggiornamento per il download del contenuto di sicurezza**

  I client con ruolo Bitdefender Endpoint Security Tools Relay scaricano circa 16 MB / giorno* dal server di aggiornamento.

  * Disponibile con client Bitdefender Endpoint Security Tools a partire dalla versione 6.2.3.569.

- **Traffico tra i client endpoint e la console web Control Center**

  Tra i client endpoint e la console web Control Center viene generato un traffico medio di 618 KB / giorno.

4.3. Exchange Protection

Security for Exchange viene fornito attraverso Bitdefender Endpoint Security Tools, che è in grado di proteggere sia il file system che il mail server di Microsoft Exchange.

4.3.1. xxx

Security for Exchange supporta i seguenti ruoli e le seguenti versioni di Microsoft Exchange:

- Exchange Server 2019 con ruolo Edge Transport o mailbox
- Exchange Server 2016 con ruolo Edge Transport o mailbox
- Exchange Server 2013 con Edge Transport o ruolo Mailbox
- Exchange Server 2010 con ruolo Edge Transport, Hub Transport o mailbox
- Exchange Server 2007 con ruolo Edge Transport, Hub Transport o mailbox

Security for Exchange è compatibile con Microsoft Exchange Database Availability Groups (DAGs).

4.3.2. Requisiti di sistema

Security for Exchange è compatibile con ogni server fisico o virtuale a 64 bit (Intel o AMD) che esegue un ruolo o una versione supportata di Microsoft Exchange Server. Per maggiori dettagli sui requisiti di sistema di Bitdefender Endpoint Security Tools, fai riferimento a «Agente di sicurezza senza ruoli» (p. 17).

Disponibilità risorse server consigliato:

- Memoria RAM libera: 1 GB
- Spazio libero su disco rigido: 1 GB

4.3.3. Altri requisiti software

- Per Microsoft Exchange Server 2013 con Service Pack 1: KB2938053 di Microsoft.
- Per Microsoft Exchange Server 2007: .NET Framework 3.5 Service Pack 1 o superiore

4.4. Full Disk Encryption

GravityZone Full Disk Encryption ti consente di usare BitLocker su endpoint Windows e FileVault e l'utility con linea di comando diskutil su endpoint macOS tramite Control Center.

Per garantire la protezione dei dati, questo modulo fornisce una crittografia completa del disco per volumi di avvio e non su dischi fissi, e memorizza le chiavi di recupero nel caso gli utenti dimenticassero le proprie password.

Il modulo Cifratura utilizza le risorse hardware esistenti nel tuo ambiente di GravityZone.

Da un punto di vista software, i requisiti sono quasi gli stessi di BitLocker, FileVault e l'utility con linea di comando diskutil, e la maggior parte delle limitazioni si riferisce a questi strumenti.

Su Windows

GravityZone Encryption supporta BitLocker, a partire dalla versione 1.2 su macchine con e senza un chip Trusted Platform Module (TPM).

GravityZone supporta BitLocker sugli endpoint con i seguenti sistemi operativi:

- Windows 10 Education

- Windows 10 Enterprise
- Windows 10 Pro
- Windows 8.1 Enterprise
- Windows 8.1 Pro
- Windows 8 Enterprise
- Windows 8 Pro
- Windows 7 Ultimate (con TPM)
- Windows 7 Enterprise (con TPM)
- Windows Server 2019*
- Windows Server 2016*
- Windows Server 2012 R2*
- Windows Server 2012*
- Windows Server 2008 R2* (con TPM)

*BitLocker non è incluso sui seguenti sistemi operativi e deve essere installato separatamente. Per maggiori informazioni sull'impiego di BitLocker su Windows Server, fai riferimento a questi articoli della KB forniti da Microsoft:

- https://technet.microsoft.com/en-us/itpro/bitlocker-how-to-deploy-on-windows-server
- https://technet.microsoft.com/en-us/library/cc732725(v=ws.10).aspx

Importante
GravityZone non supporta la cifratura su Windows 7 e Windows 2008 R2 senza TPM.

Per i requisiti dettagliati di BitLocker, fai riferimento a questo articolo della KB fornito da Microsoft: https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx

Su Mac

GravityZone supporta FileVault e diskutil su endpoint macOS con i seguenti sistemi operativi:

- macOS Big Sur (11.0)
- macOS Catalina (10.15)

- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

4.5. Protezione archiviazione

Soluzioni di archiviazione e condivisione file supportate:

- Sistemi ICAP-compatible network-attached storage (NAS) e storage-area network (SAN) di Dell®, EMC®, IBM®, Hitachi®, HPE®, Oracle® e altri
- Nutanix® Files 3.x fino al 3.6.2
- Citrix® ShareFile

4.6. Porte di comunicazione di GravityZone

GravityZone è una soluzione distribuita, in altre parole i suoi componenti comunicano tra loro attraverso l'utilizzo della rete locale o Internet. Ogni componente utilizza una serie di porte per comunicare con gli altri. Devi assicurarti che queste porte siano aperte per GravityZone.

Per maggiori informazioni sulle porte di GravityZone, fai riferimento a questo articolo della KB.

5. INSTALLARE LA PROTEZIONE

Per proteggere la tua rete con Bitdefender, devi installare gli agenti di sicurezza di GravityZone sugli endpoint. A tal fine, hai bisogno di un account utente GravityZone Control Center con privilegi di amministratore sugli endpoint sotto la tua gestione.

5.1. Amministrazione licenza

GravityZone è concesso in licenza con un solo codice per tutti i servizi di sicurezza, tranne Full Disk Encryption, che per una licenza annuale richiede un codice separato.

Puoi provare GravityZone gratuitamente per un periodo di 30 giorni. Durante il periodo di prova, saranno disponibili tutte le funzionalità e potrai utilizzare il servizio su qualsiasi numero di computer. Prima del termine del periodo di prova, se vuoi continuare a utilizzare i servizi, devi selezionare un piano di abbonamento a pagamento ed effettuare l'acquisto.

Per acquistare una licenza, contatta un rivenditore Bitdefender o contattaci via e-mail all'indirizzo enterprisesales@bitdefender.com.

5.1.1. Trovare un rivenditore

I nostri rivenditori ti forniranno tutte le informazioni che ti servono, aiutandoti a scegliere la migliore opzione di licenza per te.

Per trovare un rivenditore di Bitdefender nel tuo paese:

1. Visita la pagina Trova un partner sul sito web di Bitdefender.
2. Seleziona il paese in cui risiedi per visualizzare le informazioni di contatto dei partner di Bitdefender disponibili.
3. Se non dovessi trovare un rivenditore di Bitdefender nel tuo paese, contattaci via e-mail all'indirizzo enterprisesales@bitdefender.com.

5.1.2. Attivare la tua licenza

Quando acquisti per la prima volta un piano di abbonamento a pagamento, ti sarà inviato un codice di licenza. L'abbonamento a GravityZone viene attivato utilizzando questo codice di licenza.

Avvertimento
Attivare una licenza NON consente di aggiungere le sue funzionalità alla licenza attualmente attiva. Invece, la nuova licenza sostituisce la precedente. Per esempio, attivando una licenza di 10 endpoint su una licenza di 100 endpoint NON si otterrà

un abbonamento per 110 endpoint. Al contrario, ridurrà il numero di endpoint inclusi da 100 a 10.

Il codice di licenza ti viene inviato via e-mail quando lo acquisti. In base al tuo contratto di servizio, una volta rilasciato il codice di licenza, il tuo fornitore di servizi può attivarlo per te. In alternativa, puoi attivare la tua licenza manualmente, seguendo questi passaggi:

1. Accedi alla Control Center usando il tuo account.
2. Clicca sul tuo nome utente nell'angolo in alto a destra della console e seleziona **La mia azienda**.
3. Verifica i dettagli sulla licenza attuale nella sezione **Licenza**.
4. Nella sezione **Licenza**, seleziona il tipo di **Licenza**.
5. Alla voce **Codice di licenza**, inserisci il tuo codice di licenza.
6. Clicca sul pulsante **Controlla** e attendi che la Control Center recuperi le informazioni sul codice di licenza inserito.
7. Nel campo **Codice add-on**, inserisci il codice per un determinato add-on, come la Cifratura.
8. Clicca su **Add** (Aggiungi). In una tabella compaiono tutti i dettagli dell'add-on: tipo, codice di licenza e un'opzione per rimuovere il codice.
9. Clicca su **Salva**.
10. Per poter utilizzare l'add-on, devi uscire dalla Control Center e poi riaccedere. Ciò renderà le funzionalità dell'add-on visibili in GravityZone.

5.1.3. Verificare i dettagli della licenza attuale

Per visualizzare i dettagli della tua licenza:

1. Accedi alla Control Center usando il tuo indirizzo e-mail e la password ricevuta via e-mail.

5.2. Installare la protezione per endpoint

In base alla configurazione delle macchine e all'ambiente di rete, puoi scegliere di installare solo gli agenti di sicurezza o anche utilizzare un Security Server. In quest'ultimo caso, devi prima installare il Security Server e poi gli agenti di sicurezza.

Si consiglia di utilizzare il Security Server, se le macchine hanno poche risorse hardware.

Importante
Solo Bitdefender Endpoint Security Tools supporta la connessione a un Security Server. Per maggiori informazioni, fai riferimento a «Architettura di GravityZone» (p. 9).

5.2.1. Installare Security Server

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

Devi installare Security Server su uno o più host in modo da accogliere il numero di macchine virtuale da proteggere.

Devi considerare il numero di macchine virtuali protette, le risorse disponibili per il Security Server sugli host, oltre alla connettività di rete tra il Security Server e le macchine virtuali protette.

L'agente di sicurezza installato sulle macchine virtuali si connette al Security Server su TCP/IP, utilizzando i dettagli configurati all'installazione o tramite una policy.

Scaricare i pacchetti di installazione di Security Server

Per scaricare i pacchetti di installazione di Security Server:

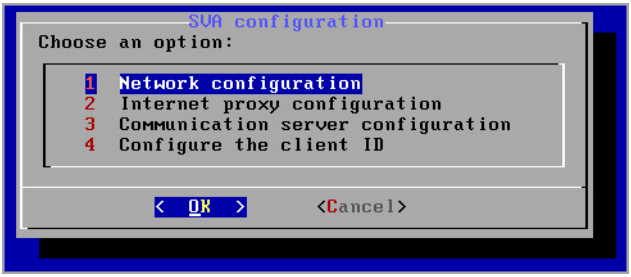
1. Vai alla pagina **Rete e Pacchetti**.
2. Seleziona il pacchetto Security Server standard.
3. Clicca sul pulsante **Scarica** nel lato superiore della tabella e seleziona il tipo di pacchetto nel menu.
4. Salva il pacchetto selezionato nella posizione desiderata.

Impiegare i pacchetti di installazione di Security Server

Una volta ottenuto il pacchetto di installazione, impiegalo nell'host utilizzando lo strumento di impiego di virtual machine preferito.

Dopo l'impiego, configura il Security Server come segue:

1. Accedi alla console della appliance dal tuo strumento di gestione della virtualizzazione (per esempio, vSphere Client). In alternativa, puoi anche connetterti alla appliance via SSH.
2. Accedi utilizzando le credenziali predefinite.
   - Nome utente: `root`
   - Password: `sve`
3. Esegui il comando `sva-setup`. Accederai all'interfaccia di configurazione della appliance.



Interfaccia configurazione di Security Server (menu principale)

Per esplorare i menu e le opzioni, usa il tasto `Tab` e le frecce. Per selezionare un'opzione specifica, premi `Invio`.

4. Configura le impostazioni di rete.

   Il Security Server utilizza il protocollo TCP/IP per comunicare con gli altri componenti di GravityZone. Puoi configurare la appliance per ottenere automaticamente le impostazioni di rete dal server DHCP oppure puoi configurare le impostazioni di rete manualmente, come descritto qui:

   a. Dal menu principale, seleziona **Configurazione di rete**.
   b. Seleziona l'interfaccia di rete.
   c. Seleziona la modalità di configurazione IP:
      - **DHCP**, se vuoi che il Security Server ottenga automaticamente le impostazioni di rete dal server DHCP.

- **Statico**, se un server DHCP è assente o se è stata fatta una prenotazione IP da parte della appliance sul server DHCP. In questo caso, devi configurare manualmente le impostazioni di rete.
  i. Inserisci l'hostname, l'indirizzo IP, la maschera di rete, il gateway, i server DND nei campi corrispondenti.
  ii. Seleziona **OK** per salvare le modifiche.

Nota
Se sei connesso a una appliance tramite un client SSH, modificando le impostazioni di rete la tua sessione sarà conclusa immediatamente.

5. Configura le impostazioni del proxy.

   Se nella rete viene usato un server proxy, devi fornire le sue informazioni, in modo che Security Server possa comunicare con GravityZone Control Center.

   Nota
   Sono supportati solo proxy con autenticazione base.

   a. Dal menu principale, seleziona **Configurazione proxy Internet**.
   b. Inserisci l'hostname, il nome utente, la password e il dominio nei campi corrispondenti.
   c. Seleziona **OK** per salvare le modifiche.
6. Configura l'indirizzo del server di comunicazione.
   a. Dal menu principale, seleziona **Configurazione server di comunicazione**.
   b. Inserisci uno dei seguenti indirizzi per il server di comunicazione:
      - `https://cloud-ecs.gravityzone.bitdefender.com:443`
      - `https://cloudgz-ecs.gravityzone.bitdefender.com:443`

      Importante
      Questo indirizzo deve essere lo stesso di quello che compare nelle impostazioni della policy della Control Center. Per verificare il link, vai alla pagina **Policy**, aggiungi o apri una policy personalizzata, esplora la sezione **Generale > Comunicazione > Assegnazione comunicazione endpoint** e inserisci il nome del server di comunicazione nell'intestazione della colonna. Il server corretto sarà mostrato nei risultati della ricerca.

c. Seleziona **OK** per salvare le modifiche.

7. Configura l'ID del client.
   a. Dal menu principale, seleziona **Configura l'ID del client**.
   b. Inserisci l'ID dell'azienda.

      L'ID è una stringa di 32 caratteri, che puoi trovare accedendo alla pagina informativa dell'azienda nella Control Center.
   c. Seleziona **OK** per salvare le modifiche.

5.2.2. Installare gli agenti di sicurezza

Per proteggere i tuoi endpoint fisici e virtuali, devi installare un agente di sicurezza in ciascuno di loro. Oltre a gestire la protezione sull'endpoint locale, l'agente di sicurezza comunica anche con la Control Center per ricevere i comandi dell'amministratore e inviare i risultati delle sue azioni.

Per ulteriori informazioni sugli agenti di sicurezza, fai riferimento a «Agenti di sicurezza» (p. 9).

Su macchine Windows e Linux, l'agente di sicurezza può avere due ruoli e puoi installarlo come segue:

1. Come un semplice agente di sicurezza per i tuoi endpoint.
2. Come un relay, agendo come un agente di sicurezza e anche come server di comunicazione, aggiornamento e proxy per altri endpoint nella rete.

Avvertimento

- Il primo endpoint su cui installi la protezione deve avere il ruolo di relay, altrimenti non potrai installare in remoto l'agente di sicurezza su altri endpoint nella stessa rete.
- L'endpoint relay deve essere alimentato e online in modo che gli agenti connessi possano comunicare con la Control Center.

Puoi installare gli agenti di sicurezza su endpoint fisici e virtuali eseguendo i pacchetti di installazione in locale o eseguendo le attività di installazione in remoto dalla Control Center.

È molto importante leggere e seguire con attenzione le istruzioni per preparare l'installazione.

In modalità normale, gli agenti di sicurezza hanno un'interfaccia utente minimale. Consente solo agli utenti di verificare lo stato della protezione ed eseguire attività di sicurezza base (aggiornamenti e scansioni), senza fornire accesso alle impostazioni.

Se attivato dall'amministratore di rete tramite pacchetto di installazione e policy di sicurezza, l'agente di sicurezza può anche essere eseguito in modalità utente esperto sugli endpoint Windows, consentendo all'utente dell'endpoint di visualizzare e modificare le impostazioni della policy. Tuttavia, l'amministratore della Control Center può sempre controllare quali impostazioni della policy applicare, prevalendo sulla modalità utente esperto.

Di norma, la lingua dell'interfaccia utente sugli endpoint protetti è impostata al momento dell'installazione in base a quella del proprio account di GravityZone.

Su Mac, la lingua dell'interfaccia utente è impostata al momento dell'installazione in base a quella del sistema operativo dell'endpoint. Su Linux, l'agente di sicurezza non ha un'interfaccia utente localizzata.

Per installare l'interfaccia utente in un'altra lingua su determinati endpoint Windows, puoi creare un pacchetto di installazione e impostare la lingua preferita nelle sue opzioni di configurazione. Questa opzione non è disponibile per endpoint Mac e Linux. Per maggiori informazioni sulla creazione dei pacchetti di installazione, fai riferimento a «Creare i pacchetti di installazione» (p. 43).

Preparazione all'installazione

Prima dell'installazione, segui questi passaggi preparatori per assicurarti che tutto vada bene:

1. Assicurati che gli endpoint di destinazione soddisfino i requisiti di sistema minimi. Per alcuni endpoint, potresti dover installare l'ultimo pacchetto di servizio del sistema operativo disponibile oppure liberare spazio sul disco rigido. Compila un elenco di endpoint che non soddisfano i requisiti necessari in modo da escluderli dalla gestione.
2. Disinstalla (non solo disattiva) ogni antimalware o software di sicurezza Internet esistente dagli endpoint di destinazione. Eseguire l'agente di sicurezza in contemporanea con un altro software di sicurezza su un endpoint potrebbe influenzare il suo funzionamento e causare parecchi problemi al sistema.

   Molti programmi di sicurezza incompatibili vengono rilevati e rimossi automaticamente al momento dell'installazione.

Per maggiori informazioni e per controllare l'elenco dei software di sicurezza rilevati da Bitdefender Endpoint Security Tools per gli attuali sistemi operativi Windows, fai riferimento a questo articolo della KB.

Importante
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.

3. L'installazione richiede privilegi di amministratore e accesso a Internet. Se gli endpoint di destinazione sono nel dominio di Active Directory, devi usare le credenziali di amministratore del dominio per un'installazione in remoto. Altrimenti, assicurati di avere le credenziali necessarie a portata di mano per tutti gli endpoint.
4. Gli endpoint deve avere una connettività con la Control Center.
5. Si consiglia di usare un indirizzo IP statico per il server relay. Se non imposti un IP statico, utilizza l'hostname della macchina.
6. Impiegando l'agente tramite un relay Linux, devono essere soddisfatte le seguenti condizioni aggiuntive:
   - 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.

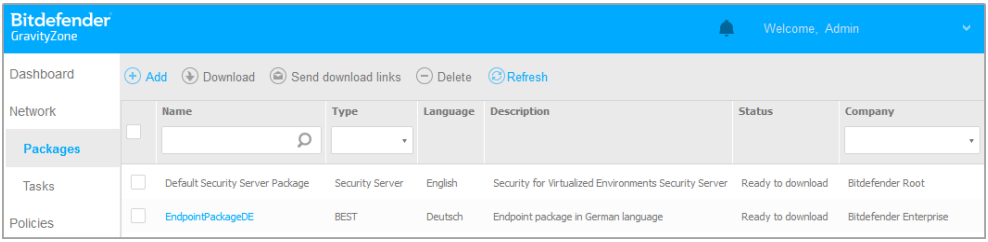
   - Gli endpoint Windows bersaglio devono avere le opzioni Condivisione amministrativa e Condivisione rete attivate.
   - Gli endpoint Linux e Mac di destinazione devono avere SSH attivato.
7. A partire da macOS High Sierra (10.13), dopo aver installato Endpoint Security for Mac manualmente o in remoto, agli utenti viene chiesto di approvare le estensioni del kernel di Bitdefender sui propri computer. Fin quando l'utente non approva le estensioni del kernel di Bitdefender, alcune funzionalità di Endpoint Security for Mac non funzioneranno. Per eliminare l'intervento

dell'utente, puoi pre-approvare le estensioni del kernel di Bitdefender inserendole nella whitelist usando uno strumento di Mobile Device Management.

Installazione locale

Un modo per installare l'agente di sicurezza su un endpoint è eseguire localmente un pacchetto di installazione.

Puoi creare e gestire i pacchetti di installazione nella pagina **Rete > Pacchetti**.



La pagina dei pacchetti

Avvertimento

- La prima macchina su cui installi la protezione deve avere il ruolo di relay, altrimenti non potrai impiegare l'agente di sicurezza su altri endpoint nella rete.
- La macchina relay deve essere alimentata e online in modo che i client possano comunicare con la Control Center.

Una volta che il primo client è stato installato, sarà utilizzato per rilevare altri endpoint nella stessa rete, basati sul meccanismo di Network Discovery. Per maggiori informazioni su Network Discovery, fai riferimento a «Come funziona Network Discovery» (p. 59).

Per installare localmente l'agente di sicurezza su un endpoint, segui questi passaggi:

1. Crea un pacchetto di installazione in base alle tue necessità.

   Nota
   Questo passaggio non è obbligatorio se nel tuo account è già stato creato un pacchetto di installazione per la rete.

2. Scarica il pacchetto di installazione sull'endpoint di destinazione.

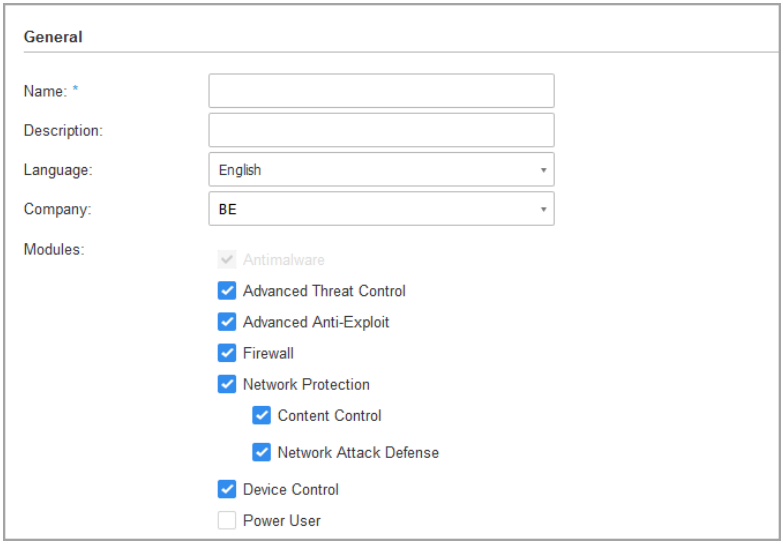
In alternativa puoi inviare i link per scaricare il pacchetto di installazione via e-mail a diversi utenti nella tua rete.

3. Esegui il pacchetto di installazione sull'endpoint di destinazione.

Creare i pacchetti di installazione

Per creare un pacchetto di installazione:

1. Connettiti e accedi alla Control Center.
2. Vai alla pagina **Rete e Pacchetti**.
3. Clicca sul pulsante ⊕**Aggiungi** nel lato superiore della tabella. Apparirà la finestra di configurazione.



Crea pacchetti - Opzioni

4. Inserisci un nome indicativo e una descrizione per il pacchetto di installazione che vuoi creare.
5. Dal campo **Lingua**, seleziona la lingua desiderata per l'interfaccia del client.

Nota
Questa opzione è disponibile solo per i sistemi operativi Windows.

6. Seleziona i moduli della protezione che desideri installare.

   Nota
   Saranno installati solo i moduli supportati per ciascun sistema operativo. Per maggiori informazioni, fai riferimento a «Agenti di sicurezza» (p. 9).

7. Seleziona il ruolo dell'endpoint di destinazione:
   - **Relay**, per creare il pacchetto per un endpoint con ruolo di relay. Per maggiori informazioni, fai riferimento a «Relay» (p. 11)
   - **Server cache gestione patch**, per rendere il Relay un server interno per la distribuzione delle patch dei software. Questo ruolo viene mostrato quando si seleziona il ruolo Relay. Per maggiori informazioni, fai riferimento a «Server caching patch» (p. 11)
   - **Protezione Exchange**, per installare i moduli di protezione per i Microsoft Exchange Server, tra cui antimalware, antispam, filtro di contenuti e allegati per il traffico e-mail di Exchange e scansione antimalware a richiesta dei database di Exchange. Per maggiori informazioni, fai riferimento a «Installare la protezione di Exchange» (p. 63).
8. **Rimuovi concorrenti**. Si consiglia di mantenere selezionata questa casella per rimuovere automaticamente ogni software di sicurezza incompatibile mentre l'agente di Bitdefender viene installato sull'endpoint. Deselezionando questa opzione, l'agente di Bitdefender si installerà accanto alla soluzione di sicurezza esistente. Puoi rimuovere manualmente la soluzione di sicurezza installata precedentemente in un secondo momento, a tuo rischio e pericolo.

   Importante
   Eseguire l'agente di Bitdefender in contemporanea con un altro software di sicurezza su un endpoint potrebbe influenzare il suo funzionamento e causare parecchi problemi al sistema.

9. **Mod. di scansione**. Seleziona la tecnologia di scansione che si adatta meglio all'ambiente della tua rete e alle risorse dei tuoi endpoint. Puoi definire la modalità di scansione scegliendo una delle seguenti tipologie:
   - **Automatica**. In questo caso, l'agente di sicurezza rileverà automaticamente la configurazione dell'endpoint e adatterà la tecnologia di scansione di conseguenza:

- Scansione centrale nel cloud pubblico o privato (con Security Server) e fallback su scansione ibrida (motori leggeri), per computer fisici con prestazioni hardware limitate e macchine virtuali. Questo caso richiede almeno un Security Server impiegato nella rete.
- Scansione locale (con motori completi) per computer fisici con prestazioni hardware elevate.

Nota
I computer con prestazioni limitate sono sistemi con una frequenza della CPU inferiore a 1,5 GHz o meno di 1 GB di memoria RAM.

- **Personalizzata**. In questo caso, puoi configurare la modalità di scansione scegliendo tra diverse tecnologie di scansione per macchine fisiche e virtuali:
  - Scansione centrale in cloud pubblico o privato (con Security Server), che può passare* a una scansione ibrida (con motori leggeri) o una scansione locale (con motori completi)
  - Scansione ibrida (con motori leggeri)
  - Scansione locale (con motori completi)

  La modalità di scansione predefinita per le istanze EC2 è la Scansione locale (tutti contenuti di sicurezza vengono memorizzati sull'agente di sicurezza installato e la scansione viene eseguita localmente sulla macchina). Se vuoi esaminare le tue istanze EC2 con un Security Server, devi configurare il pacchetto di installazione dell'agente di sicurezza e la policy applicata di conseguenza.

  La modalità di scansione predefinita per le virtual machine di Microsoft Azure è la Scansione locale (tutti contenuti di sicurezza vengono memorizzati sull'agente di sicurezza installato e la scansione viene eseguita localmente sulla macchina). Se vuoi esaminare le tue virtual machine di Microsoft Azure con un Security Server, devi configurare il pacchetto di installazione dell'agente di sicurezza e la policy applicata di conseguenza.

  * 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 sarà basato sui motori utilizzati.

  Per maggiori informazioni sulle tecnologie di scansione disponibili, fai riferimento a «Motori di scansione» (p. 3)

10. Personalizzando i motori di scansione, usando una scansione in cloud pubblico o privato (Security Server), ti sarà richiesto di selezionare i Security Server installati in locale, se desideri usare e configurare la loro priorità nella sezione **Assegnazione Security Server**:

    a. Clicca sull'elenco Security Server) nell'intestazione della tabella. Viene mostrato l'elenco dei Security Server rilevati.

    b. Seleziona un'entità.

    c. Clicca sul pulsante ⊕ **Aggiungi** dall'intestazione della colonna **Azioni**.

    Il Security Server viene aggiunto all'elenco.

    d. Segui gli stessi passaggi per aggiungere i server di sicurezza, se disponibili. In questo caso, puoi configurare la loro priorità utilizzando le frecce ⌃ su e ⌄ giù, disponibili sul lato destro di ciascuna entità. Quando il primo Security Server non è disponibile, sarà usato il successivo e così via.

    e. Per eliminare un'entità dall'elenco, clicca sul pulsante ⊗ **Elimina** corrispondente nel lato superiore della tabella.

    Puoi scegliere di cifrare la connessione al Security Server selezionando l'opzione **Usa SSL**.

11. Seleziona **Esamina prima dell'installazione**, se vuoi assicurarti che le macchine siano pulite prima di installarci il client. Una scansione veloce nel cloud sarà eseguita sulle macchine bersaglio prima di iniziare l'installazione.

12. Bitdefender Endpoint Security Tools viene installato nella cartella di installazione predefinita. Seleziona **Usa percorso di installazione personalizzato**, se vuoi installare Bitdefender in un'altra posizione. Se la cartella indicata non esiste, sarà creata durante l'installazione.

    - Su Windows, il percorso predefinito è `C:\Program Files\`. Per installare Bitdefender Endpoint Security Tools in un percorso personale, usa le convenzioni di Windows quando inserisci il percorso. Per esempio, `D:\folder`.

    - Su Linux, Bitdefender Endpoint Security Tools viene installato in maniera predefinita nella cartella `/opt`. Per installare l'agente di Bitdefender in un percorso personale, usa le convenzioni di Linux quando inserisci il percorso. Per esempio, `/folder`.

Bitdefender Endpoint Security Tools non supporta l'installazione nei seguenti percorsi personali:

- Qualsiasi percorso che non inizia con la barra (/). L'unica eccezione è la posizione di Windows `%PROGRAMFILES%`, che l'agente di sicurezza interpreta come la cartella predefinita di Linux `opt`.
- Qualsiasi percorso che sia in `/tmp` o `/proc`.
- Qualsiasi percorso che contenga i seguenti caratteri speciali: `$, !, *, ?, ", ', `, \, (,), [,], {, }`.
- L'indicatore `systemd` (%).

Su Linux, l'installazione in un percorso predefinito richiede glibc 2.21 o superiore.

Importante
Nell'usare un percorso personalizzato, assicurati di avere il giusto pacchetto di installazione per ciascun sistema operativo.

13. Se lo desideri, puoi impostare una password per impedire agli utenti di rimuovere la protezione. Seleziona **Imposta password di disinstallazione** e inserisci la password desiderata nei campi corrispondenti.
14. Se gli endpoint di destinazione sono nell'inventario di rete nei **Gruppi personalizzati**, puoi scegliere di spostarli subito in una cartella specifica, subito dopo il completamento dell'impiego dell'agente di sicurezza.

    Seleziona **Usa cartella personalizzata** e scegli una cartella nella tabella corrispondente.
15. Nella sezione **Gestore**, scegli l'entità a cui gli endpoint di destinazione si connettono per installare e aggiornare il client:

    - **Cloud di Bitdefender**. Se desideri aggiornare i client direttamente da Internet.

      In questo caso, puoi anche definire le impostazioni del proxy, se gli endpoint di destinazione si connettono a Internet tramite proxy. Seleziona **Usa proxy per la comunicazione** e inserisci le impostazioni proxy richieste nei campi sottostanti.
    - **Relay di sicurezza endpoint**, se vuoi connettere gli endpoint a un client relay installato nella tua rete. Tutte le macchine con ruolo di relay rilevate nella tua rete compariranno nella tabella mostrata sotto. Seleziona la macchina

relay che desideri. Gli endpoint connessi comunicheranno con la Control Center solo tramite il relay specificato.

Importante
Per funzionare, la porta 7074 deve essere aperta per l'impiego tramite Bitdefender Endpoint Security Tools Relay.

16. Clicca su **Salva**.

Il pacchetto appena creato sarà aggiunto all'elenco dei pacchetti.

Nota
Le impostazioni configurate in un pacchetto di installazione saranno applicate agli endpoint subito dopo l'installazione. Non appena la policy viene applicata al client, le impostazioni configurate nella policy vengono applicate, sostituendo alcune impostazioni del pacchetto di installazione (come i server di comunicazione o le impostazioni del proxy).

Scaricare i pacchetti di installazione

Per scaricare i pacchetti di installazione degli agenti di sicurezza:

1. Accedi alla Control Center dall'endpoint su cui vuoi installare la protezione.
2. Vai alla pagina **Rete e Pacchetti**.
3. Seleziona il pacchetto di installazione che desideri scaricare.
4. Clicca sul pulsante **Scarica** nel lato superiore della tabella e seleziona il tipo di installer che vuoi utilizzare. Sono disponibili due tipi di file di installazione:
   - **Downloader**. Il downloader scarica prima il kit di installazione completo dai server cloud di Bitdefender e poi avvia l'installazione. È di piccole dimensioni e può essere eseguito su sistemi a 32 e 64 bit (il che ne facilita la distribuzione). Il lato negativo, è che richiede una connessione a Internet attiva.
   - **Kit completo**. I kit di installazione completi sono di maggiori dimensioni e devono essere eseguiti su un determinato tipo di sistema operativo.

     Il kit completo deve essere utilizzato per installare la protezione sugli endpoint con una connessione a Internet lenta o assente del tutto. Scarica questo file in un endpoint connesso a Internet e poi distribuiscilo sugli altri endpoint utilizzando un supporto di archiviazione esterno o una rete condivisa.

Nota
Versioni dei kit completi disponibili:

- **SO Windows:** sistemi a 32 e 64 bit
- **SO Linux:** sistemi a 32 e 64 bit
- **macOS:** solo sistemi a 64 bit

Assicurati di utilizzare la versione corretta per il sistema in cui vuoi installarlo.

5. Salva il file nell'endpoint.

Avvertimento

- L'eseguibile del downloader non deve essere rinominato, altrimenti non sarà possibile scaricare i file di installazione dal server di Bitdefender.

6. Inoltre, se hai selezionato il Downloader, puoi creare un pacchetto MSI per gli endpoint Windows. Per maggiori informazioni, fai riferimento a questo articolo della KB.

Invia i link per scaricare i pacchetti di installazione via e-mail.

Potrebbe essere necessario informare rapidamente gli altri utenti che è un pacchetto di installazione è disponibile per il download. In questo caso, segui i passaggi descritti di seguito:

1. Vai alla pagina **Rete e Pacchetti**.
2. Seleziona il pacchetto di installazione che desideri.
3. Clicca sul pulsante **Invia link di download** nel lato superiore della tabella. Apparirà la finestra di configurazione.
4. Inserisci l'e-mail di ogni utente che vuole ricevere il link per il download del pacchetto di installazione. Premi `Invio` dopo ogni indirizzo e-mail.

   Assicurati che ogni indirizzo e-mail inserito sia valido.
5. Se vuoi visualizzare i link di download prima di inviarli via e-mail, clicca sul pulsante **Link di installazione**.
6. Clicca su **Invia**. A ciascun indirizzo e-mail indicato viene inviata un'e-mail contenente il link di installazione.

Eseguire i pacchetti di installazione

Affinché l'installazione funzioni, il pacchetto di installazione deve essere eseguito utilizzando i privilegi di amministratore.

Il pacchetto si installa in modo diverso su ciascun sistema operativo, come segue:

- Su sistemi operativi Windows e macOS:
  1. Sull'endpoint di destinazione, scarica il file di installazione dalla Control Center o copialo da una rete condivisa.
  2. Se hai scaricato il kit completo, estrai i file dall'archivio.
  3. Esegui il file eseguibile.
  4. Seguire le istruzioni sullo schermo.

  Nota
  Su macOS, dopo aver installato Endpoint Security for Mac, agli utenti viene chiesto di approvare le estensioni del kernel di Bitdefender sui propri computer. Finché gli utenti non approvano le estensioni del kernel di Bitdefender, alcune funzionalità dell'agente di sicurezza non funzioneranno. Per maggiori dettagli, fai riferimento a questo articolo della KB.

- Sui sistemi operativi Linux:
  1. Connettiti e accedi alla Control Center.
  2. Scarica o copia il file di installazione sull'endpoint di destinazione.
  3. Se hai scaricato il kit completo, estrai i file dall'archivio.
  4. Ottieni privilegi di root eseguendo il comando `sudo su`.
  5. Modifica i permessi per il file di installazione in modo da eseguirlo:

     ```
     # chmod +x installer
     ```

  6. Lanciare il file di installazione:

     ```
     # ./installer
     ```

7. Per verificare se l'agente è stato installato sull'endpoint, esegui questo comando:

```
$ service bd status
```

Una volta che l'agente di sicurezza è stato installato, l'endpoint comparirà come gestito nella Control Center (pagina **Rete**) in pochi minuti.

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.

Installazione remota

Control Center ti consente di installare in remoto l'agente di sicurezza sugli endpoint rilevati nella rete, utilizzando le attività di installazione.

Una volta installato in locale il primo client con il ruolo di relay, potrebbero volerci alcuni minuti affinché il resto degli endpoint della rete sia visibile in Control Center. Da questo punto, puoi installare in remoto l'agente di sicurezza sugli endpoint da te gestiti, utilizzando le attività di installazione dalla Control Center.

Bitdefender Endpoint Security Tools include un meccanismo di Network Discovery automatico che consente di rilevare altri endpoint nella stessa rete. Gli endpoint rilevati vengono mostrati come **non gestiti** nella pagina **Rete**.

Per consentire Network Discovery, devi avere Bitdefender Endpoint Security Tools già installato su almeno un endpoint nella rete. Questo endpoint sarà utilizzato per

esaminare la rete e installare Bitdefender Endpoint Security Tools sugli endpoint non protetti.

Per maggiori informazioni su Network Discovery, fai riferimento a «Come funziona Network Discovery» (p. 59).

Requisiti per l'installazione in remoto

Affinché l'installazione in remoto funzioni:

- Bitdefender Endpoint Security Tools Relay deve essere installato nella tua rete.
- Su Windows:
  - La condivisione amministrativa `admin$` deve essere attivata. Configura ogni workstation bersaglio per non usare la condivisione file avanzata.
  - Configura User Account Control (UAC) in base al sistema operativo in esecuzione sugli endpoint di destinazione. Se gli endpoint sono in un dominio di Active Directory, puoi usare una policy di gruppo per configurare User Account Control. Per maggiori dettagli, fai riferimento a questo articolo della KB.
  - Disattiva Windows Firewall o configuralo per consentire il traffico tramite il protocollo di condivisione di file e stampanti.

  Nota
  L'impiego remoto funziona solo sui sistemi operativi moderni, a partire con Windows 7 / Windows Server 2008 R2, per cui Bitdefender fornisce supporto completo. Per maggiori informazioni, fai riferimento a «Sistemi operativi supportati» (p. 20).

- Su Linux: SSH deve essere attivato.
- Su macOS: l'accesso remoto e la condivisione file devono essere attivati.

Eseguire attività di installazione in remoto

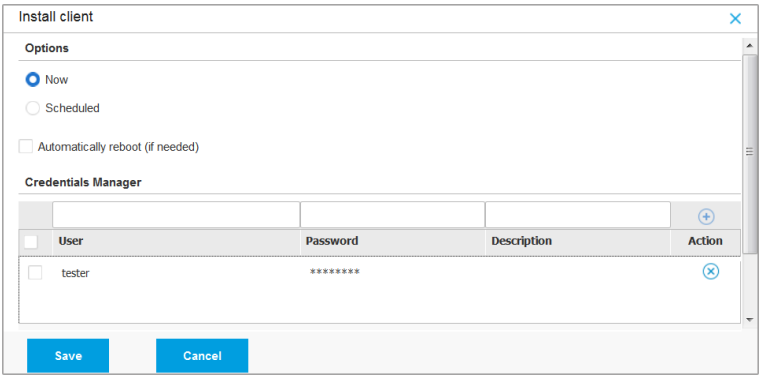
Per eseguire un'attività di installazione in remoto:

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.

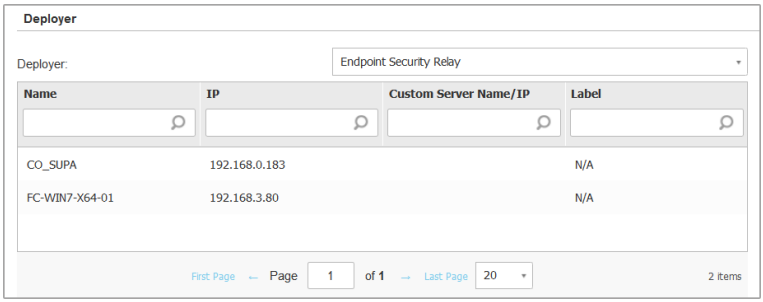
Importante
Se le credenziali fornite non sono valide, l'impiego del client sugli endpoint corrispondenti non funzionerà. Assicurati di aggiornare le credenziali SO inserite nel Credentials Manager quando queste vengono modificate negli endpoint di destinazione.

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:
    - Tutte le macchine con ruolo di relay rilevate nella tua rete compariranno nella tabella disponibile nella sezione **Gestore**. Ogni nuovo client deve essere connesso ad almeno un client relay della stessa rete, che servirà come server di aggiornamento e comunicazione. Seleziona il relay che vuoi collegare con gli endpoint bersagli. Gli endpoint connessi comunicheranno con la Control Center solo tramite il relay specificato.

Importante
Per funzionare, la porta 7074 deve essere aperta per l'impiego tramite l'agente relay.



- Se gli endpoint bersaglio comunicano con l'agente relay tramite il proxy, devi definire anche le impostazioni del proxy. In questo caso, seleziona **Usa proxy per la comunicazione** e inserisci le impostazioni proxy richieste nei campi sottostanti.

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 maggiori informazioni su come modificare i pacchetti di installazione, fai riferimento a «Creare i pacchetti di installazione» (p. 43).

    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.

Preparare i sistemi Linux per la scansione all'accesso

Bitdefender Endpoint Security Tools per Linux include capacità di scansione all'accesso che funzionano con determinate distribuzioni Linux e versioni kernel. Per maggiori informazioni, fai riferimento ai requisiti di sistema.

Poi scoprirai come compilare manualmente il modulo DazukoFS.

Compila manualmente il modulo DazukoFS

Segui i passaggi sottostanti per compilare DazukoFS per la versione del kernel del sistema e poi carica il modulo:

1. Scaricare le corrette intestazioni kernel.
   - Sui sistemi **Ubuntu**, esegui questo comando:

     ```
     $ sudo apt-get install linux-headers-`uname -r`
     ```

   - Sui sistemi **RHEL/CentOS**, esegui questo comando:

     ```
     $ sudo yum install kernel-devel kernel-headers-`uname -r`
     ```

2. Sui sistemi **Ubuntu**, ti serve `build-essential`:

   ```
   $ sudo apt-get install build-essential
   ```

3. Copia ed estrai il codice sorgente di DazukoFS in una cartella preferita:

   ```
   # mkdir temp
   # cd temp
   # cp /opt/BitDefender/share/modules/dazukofs/dazukofs-source.tar.gz
   # tar -xzvf dazukofs-source.tar.gz
   # cd dazukofs-3.1.4
   ```

4. Compila il modulo:

```
# make
```

5. Installa e carica il modulo:

```
# make dazukofs_install
```

Requisiti per utilizzare la scansione a richiesta con DazukoFS

Affinché DazukoFS e la scansione a richiesta lavorino insieme, devono essere soddisfatte alcune condizioni. Controlla se una delle seguenti indicazioni si applica al tuo sistema Linux e segui le linee guida per evitare problemi.

- La policy SELinux deve essere disattivata o impostata su **permissivo**. Per controllare e impostare l'impostazione della policy di SELinux, modifica il file `/etc/selinux/config`.
- Bitdefender Endpoint Security Tools è compatibile esclusivamente con la versione DazukoFS inclusa nel pacchetto di installazione. Se DazukoFS è già stato installato sul sistema, rimuovilo prima di installare Bitdefender Endpoint Security Tools.
- DazukoFS supporta determinate versioni del kernel. Se il pacchetto DazukoFS fornito con Bitdefender Endpoint Security Tools non è compatibile con la versione kernel del sistema, il modulo non potrà essere caricato. In tal caso, puoi aggiornare il kernel alla versione supportata o ricompila il modulo DazukoFS per la tua versione del kernel. Puoi trovare il pacchetto DazukoFS nella cartella di installazione di Bitdefender Endpoint Security Tools:

  `/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz`
- Condividendo i file usando server dedicati come NFS, UNFSv3 o Samba, devi avviare i servizi nel seguente ordine:

  1. Attiva la scansione all'accesso tramite la policy dalla Control Center.

     Per maggiori informazioni, fai riferimento alla Guida dell'amministratore di GravityZone.

  2. Avvia il servizio di condivisione della rete.

     Per NFS:

```
# service nfs start
```

Per UNFSv3:

```
# service unfs3 start
```

Per Samba:

```
# service smbd start
```

Importante
Per il servizio NFS, DazukoFS è compatibile solo con NFS User Server.

Come funziona Network Discovery

Oltre all'integrazione con Active Directory, GravityZone include anche un meccanismo automatico di network discovery inteso a rilevare i computer del gruppo di lavoro.

GravityZone si basa sul servizio **Microsoft Computer Browser** e lo strumento **NBTscan** per eseguire Network Discovery.

Il servizio Computer Browser è una tecnologia di rete utilizzata da computer Windows per mantenere aggiornati gli elenchi di domini, workgroup e computer in essi e fornire tali elenchi ai computer client a richiesta. I computer rilevati nella rete dal servizio Computer Browser possono essere visualizzati eseguendo il comando **net view** in una finestra di comando.

Il comando Net view

Lo strumento NBTscan esamina le reti dei computer utilizzando NetBIOS. Interroga ogni endpoint nella rete e recupera informazioni come indirizzo IP, nome computer NetBIOS e indirizzo MAC.

Per consentire automaticamente Network Discovery, devi avere già installato Bitdefender Endpoint Security Tools Relay su almeno un computer nella rete. Questo computer sarà utilizzato per esaminare la rete.

Importante

Control Center non usa le informazioni di rete da Active Directory o dalla funzionalità mappa di rete. La mappa di rete si affida a una diversa tecnologia di Network Discovery: il protocollo Link Layer Topology Discovery (LLTD).

Control Center non è attivamente coinvolto nell'operatività del servizio Computer Browser. Bitdefender Endpoint Security Tools interroga solo il servizio Computer Browser per l'elenco delle workstation e dei server attualmente visibili nella rete (conosciuto come elenco di navigazione) e quindi lo invia alla Control Center. Control Center elabora l'elenco di navigazione, aggiungendo i nuovi computer rilevati al suo elenco **Computer non gestiti**. I computer rilevati in precedenza non vengono eliminati dopo una nuova query di Network Discovery, quindi dovrai escludere ed eliminare direttamente i computer che non appartengono più alla rete.

La query iniziale per la lista di navigazione viene eseguita dal primo Bitdefender Endpoint Security Tools installato nella rete.

- Se il relay è installato su un computer workgroup, solo i computer di quel workgroup saranno visibili in Control Center.
- Se il relay è installato su un computer dominio, solo i computer di quel dominio saranno visibili in Control Center. I computer da altri domini possono essere rilevati se c'è un rapporto di fiducia con il dominio dove è stato installato il relay.

Le richieste successive di Network Discovery vengono eseguite regolarmente ogni ora. Per ogni nuova query, Control Center divide lo spazio dei computer gestiti in aree di visibilità e successivamente designa un relay in ciascuna area per eseguire un'attività. Un'area di visibilità è un gruppo di computer che si rilevano a vicenda. In genere, un'area di visibilità viene definita da un workgroup o un dominio, ma dipende dalla topologia e la configurazione della rete. In alcuni casi, un'area di visibilità può consistere in più domini e workgroup.

Se un relay selezionato non riesce a eseguire la query, Control Center attende per la prossima query programmata, senza selezionare un altro relay per riprovare.

Per una completa visibilità della rete, il relay deve essere installato in almeno un computer in ogni workgroup o dominio nella rete. Idealmente, Bitdefender Endpoint Security Tools deve essere installato su almeno un computer in ogni sottorete.

Maggiori informazioni sul servizio Microsoft Computer Browser

Alcune informazioni sul servizio Computer Browser:

- Funziona in modo indipendente da Active Directory.
- Funziona esclusivamente su reti IPv4 e opera autonomamente nei confini di un gruppo LAN (workgroup o dominio). Per ciascun gruppo LAN viene compilata e mantenuta una lista di navigazione.
- Utilizza tipicamente trasmissioni server senza connessione per comunicare tra i nodi.
- Utilizza NetBIOS su TCP/IP (NetBT).
- Richiede la risoluzione dei nomi NetBIOS. Si consiglia di avere un'infrastruttura Windows Internet Name Service (WINS) attiva e in esecuzione nella rete.
- Di norma non è attivata in Windows Server 2008 e 2008 R2.

Per maggiori informazioni sul servizio Computer Browser, consulta Computer Browser Service Technical Reference su Microsoft Technet.

Requisiti di Network Discovery

Per scoprire con successo tutti i computer (server e workstation) che saranno gestiti dalla Control Center, servono i seguenti requisiti:

- I computer devono essere uniti in un workgroup o un dominio e connessi tramite una rete locale IPv4. Il servizio Computer Browser non funziona su reti IPv6.
- Diversi computer in ogni gruppo LAN (workgroup o dominio) devono eseguire il servizio Computer Browser. Anche i Primary Domain Controller devono eseguire il servizio.
- NetBIOS su TCP/IP (NetBT) deve essere attivato sui computer. Il firewall locale deve consentire il traffico NetBT.
- Se si utilizza un relay Linux per scoprire altri endpoint Linux o Mac, è necessario installare Samba sugli endpoint bersaglio, oppure associarli in Active Directory

e usare DHCP. In questo modo, NetBIOS sarà configurato automaticamente su di essi.

- Sui computer deve essere attiva la condivisione dei file. Il firewall locale deve consentire la condivisione dei file.
- Un'infrastruttura Windows Internet Name Service (WINS) deve essere attivata e deve funzionare correttamente.
- Network Discovery deve essere attivato (**Pannello di controllo > Centro connessioni di rete e condivisione > Modifica impostazioni di condivisione avanzate**).

  Per attivare questa funzionalità, i seguenti servizi devono essere attivati:
  - Client DNS
  - Function Discovery Resource Publication
  - SSDP Discovery
  - UPnP Device Host
- Negli ambienti con più domini, si consiglia di impostare relazioni affidabili tra i domini, in modo che i computer possano accedere a liste di navigazione da altri domini.

I computer da cui Bitdefender Endpoint Security Tools interroga il servizio Computer Browser devono essere in grado di risolvere i nomi NetBIOS.

Nota
Il meccanismo di Network Discovery funziona per tutti i sistemi operativi supportati, tra cui versioni di Windows Embedded, a condizione che i requisiti siano soddisfatti.

5.3. Installare EDR

Questo modulo viene fornito in modo predefinito di un kit d'installazione di Bitdefender Endpoint Security Tools e richiede l'attivazione del sensore Incidenti una volta inserito il codice di licenza per la prima volta.

Prima dell'installazione, assicurati che gli endpoint bersaglio soddisfino i requisiti minimi. I requisiti minimi degli Incidenti soddisfano i requisiti dell'agente di sicurezza.

Per proteggere i tuoi endpoint con EDR puoi scegliere fra due opzioni:

- Installa gli agenti di sicurezza con il sensore EDR quando inserisci il codice di licenza. Fai riferimento alla sezione Attivare la tua licenza.

- Usa l'attività **Riconfigura**.

Importante
The Incidents Sensor no longer provides support for Internet Explorer.

Per maggiori informazioni, fai riferimento alla Guida dell'amministratore di GravityZone.

5.4. Installare Full Disk Encryption

Full Disk Encryption richiede l'attivazione basata su un codice di licenza.

Per maggiori informazioni sui codici di licenza, fai riferimento a «Amministrazione licenza» (p. 34).

Gli agenti di sicurezza di Bitdefender supportano Full Disk Encryption a partire dalla versione 6.2.22.916 su Windows e 4.0.0173876 su Mac. Per assicurarsi che gli agenti siano pienamente compatibili con questo modulo, hai due opzioni:

- Installa gli agenti di sicurezza con il modulo Cifratura incluso.
- Usa l'attività **Riconfigura**.

Per maggiori informazioni sull'utilizzo di Full Disk Encryption nella tua rete, fai riferimento al capitolo **Policy di sicurezza > Cifratura** nella Guida dell'amministratore di GravityZone.

5.5. Installare la protezione di Exchange

Security for Exchange si integra automaticamente con i server Exchange, in base al ruolo del server. Per ciascun ruolo, vengono installate solo le funzionalità compatibili, come descritto qui:

Caratteristiche	Microsoft Exchange 2019/2016/2013		Microsoft Exchange 2010/2007		
	Edge	Casella di posta	Edge	Hub	Casella di posta
Livello di Trasporto					
Filtro antimalware	x	x	x	x	
Filtro antispam	x	x	x	x	
Filtro contenuti	x	x	x	x	
Filtro allegati	x	x	x	x	
Store Exchange					
Scansione antimalware a richiesta		x			x

5.5.1. Preparazione all'installazione

Prima di installare Security for Exchange, assicurati che tutti i requisiti siano soddisfatti, altrimenti Bitdefender Endpoint Security Tools potrebbe essere installato senza il modulo Protezione Exchange.

Per far funzionare il modulo Protezione Exchange senza problemi e impedire eventuali conflitti e risultati indesiderati, rimuovere ogni agente antimalware e di filtro e-mail.

Bitdefender Endpoint Security Tools rileva e rimuove automaticamente la maggior parte dei prodotti antimalware e disattiva l'agente antimalware del Server Exchange fin dalla versione 2013. Per maggiori dettagli sulla lista dei software di sicurezza rilevati, fai riferimento a questo articolo della FAQ.

Puoi riattivare manualmente l'agente antimalware di Exchange in qualsiasi momento, anche se non si consiglia di farlo.

5.5.2. Installare la protezione sui server Exchange

Per proteggere i tuoi server Exchange, devi installare Bitdefender Endpoint Security Tools con il ruolo Protezione Exchange su ciascuno di loro.

Hai diverse opzioni per impiegare Bitdefender Endpoint Security Tools sui server Exchange:

- Installazione locale, scaricando ed eseguendo il pacchetto di installazione sul server.
- Installazione remota, eseguendo un'attività di **Installazione**.
- Remota, eseguendo l'attività **Riconfigura client**, se Bitdefender Endpoint Security Tools offre già la protezione del file system sul server.

Per i passaggi dettagliati dell'installazione, fai riferimento a «Installare gli agenti di sicurezza» (p. 39).

5.6. Installare la Protezione memorizzazione

Security for Storage è un servizio di Bitdefender sviluppato per proteggere i dispositivi Network-Attached Storage (NAS) e i sistemi di condivisione dei file conformi con l'Internet Content Adaptation Protocol (ICAP). Per i sistemi di condivisione dei file, fai riferimento a «Protezione archiviazione» (p. 33).

Per usare Security for Storage con la tua soluzione di GravityZone:

1. Installare e configurare almeno due Security Server nel tuo ambiente per funzionare come server ICAP. I Security Server di Bitdefender analizzano i file, inviano verdetti ai sistemi di memorizzazione e, se necessario, prendono le azioni appropriate. In caso di sovraccarico, il primo Security Server ridireziona l'eccesso di dati al secondo.

   Nota
   Come prassi ottimale, installa i Security Server dedicati per la protezione dell'archiviazione, separatamente dai Security Server usati per altri ruoli, come la scansione antimalware.

   Per maggiori dettagli sulla procedura di installazione del Security Server, fai riferimento alla sezione **Installare Security Server** di questa guida.

2. Configura il modulo **Protezione archiviazione** dalle impostazioni della policy di GravityZone.

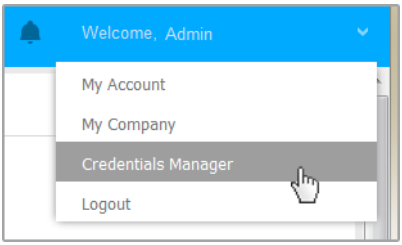
   Per maggiori dettagli, fai riferimento al capitolo **Policy di sicurezza > Policy computer e virtual machine > Protezione archiviazione** della Guida per gli amministratori di GravityZone.

Per maggiori dettagli sulla configurazione e la gestione dei server ICAP su un determinato dispositivo NAS o sistema di condivisione dei file, fai riferimento alla documentazione per quella determinata piattaforma.

5.7. 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**.

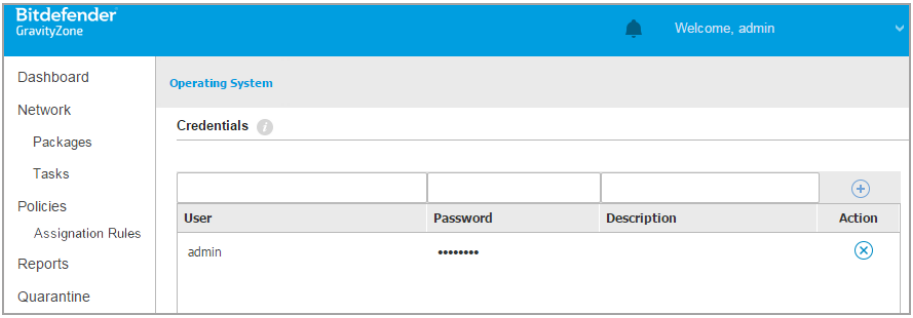


Il menu Credentials Manager

5.7.1. 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.

5.7.2. Eliminare le credenziali dal Credentials Manager

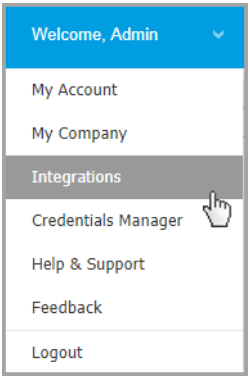
Per eliminare credenziali obsolete dal Credentials Manager:

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.

6. INTEGRAZIONI

GravityZone offre la possibilità di integrare la Control Center con soluzioni di terze parti.

Puoi configurare l'integrazione delle tue soluzioni di terze parti nella pagina **Integrazioni**, a cui puoi accedere tramite il tuo nome utente nell'angolo in alto a destra della console e selezionando **Integrazioni**.



Da questa pagina, puoi aggiungere, modificare o rimuovere le integrazioni in base alle tue esigenze.

6.1. Integrazione con Microsoft Windows Defender ATP

L'integrazione tra GravityZone e Windows Defender Advanced Threat Protection di Microsoft consente ai clienti Microsoft di gestire la sicurezza dei propri endpoint macOS e Linux nella console di gestione di Windows Defender Security Center.

Con questa integrazione, GravityZone invierà informazioni su malware ed eventi relativi allo stato del prodotto dai suoi endpoint macOS e Linux gestiti a Windows Defender Security Center.

Segui le linee guida descritte in questo articolo della KB per integrare GravityZone con Microsoft Windows Defender ATP.

7. DISINSTALLARE LA PROTEZIONE

Puoi disinstallare e reinstallare le componenti di GravityZone quando è necessario usare un codice di licenza per un'altra macchina, correggere eventuali errori o effettuare un upgrade.

Per disinstallare correttamente la protezione di Bitdefender dagli endpoint nella tua rete, segui le istruzioni descritte in questo capitolo.

- Disinstallare la protezione per endpoint
- Disinstallare la protezione di Exchange

7.1. Disinstallare la protezione per endpoint

Per rimuovere in modo sicuro la protezione di Bitdefender, devi prima disinstallare gli agenti di sicurezza e poi Security Server, se necessario. Se vuoi disinstallare solo il Security Server, assicurati prima di connettere i suoi agenti a un altro Security Server.

- Disinstallare gli agenti di sicurezza
- Disinstallare Security Server

7.1.1. Disinstallare gli agenti di sicurezza

Hai due opzioni per disinstallare gli agenti di sicurezza:

- In remoto nella Control Center
- Manualmente nella macchina bersaglio

Disinstallazione remota

Per disinstallare la protezione di Bitdefender da un endpoint gestito in remoto:

1. Vai alla pagina **Rete**.
2. Seleziona il contenitore desiderato dal pannello sulla sinistra. Tutti i computer del contenitore selezionato sono mostrati nella tabella a destra.
3. Seleziona gli endpoint da cui vuoi disinstallare l'agente di sicurezza di Bitdefender.
4. Clicca su **Attività** nel lato superiore della tabella e seleziona **Disinstalla client**. Apparirà una finestra di configurazione.

5. Nella finestra dell'attività **Disinstalla agente**, puoi selezionare se mantenere i file in quarantena nell'endpoint o eliminarli.
6. Clicca su **Salva** per creare l'attività. Apparirà un messaggio di conferma.

Puoi visualizzare e gestire l'attività in **Rete e attività**.

Disinstallazione locale

Per disinstallare manualmente l'agente di sicurezza di Bitdefender da una macchina Windows:

1. In base al tuo sistema operativo:
   - In Windows 7, vai in **Start - Pannello di Controllo - Disinstalla un programma** nella categoria **Programmi e funzionalità**.
   - In Windows 8, vai in **Impostazioni - Pannello di Controllo - Disinstalla un programma** nella categoria **Programmi e funzionalità**.
   - In Windows 8.1, fai clic con il pulsante destro del mouse sul pulsante **Start**, poi seleziona **Pannello di Controllo - Programmi e funzionalità**.
   - In Windows 10, vai in **Start - Impostazioni - App - App e funzionalità**.
2. Seleziona l'agente di Bitdefender dall'elenco dei programmi.
3. Clicca su **Disinstalla**.
4. Inserisci la password di Bitdefender, se attivata nella policy di sicurezza. Durante la disinstallazione, puoi visualizzare i progressi dell'attività.

Per disinstallare manualmente l'agente di sicurezza di Bitdefender da una macchina Linux:

1. Apri il terminale.
2. Ottieni l'accesso root usando i comandi `su` o `sudo su`.
3. Usa il comando `cd` per esplorare il seguente percorso: `/opt/BitDefender/bin`
4. Esegui lo script:

```
# ./remove-sve-client
```

5. Inserisci la password di Bitdefender per continuare, se attivata nella policy di sicurezza.

Per disinstallare manualmente l'agente di Bitdefender da un Mac:

1. Vai in **Finder - Applicazioni**.
2. Apri la cartella Bitdefender.
3. Fai doppio click su **Disinstalla Mac Uninstall**.
4. Nella finestra della configurazione, clicca sia sua **Controlla** e **Disinstalla** per continuare.

7.1.2. Disinstallare Security Server

Per rimuovere Security Server:

1. Disattiva ed elimina la macchina virtuale Security Server dal tuo ambiente di virtualizzazione.
2. Accedi a GravityZone Control Center.
3. Vai su **Rete** e cerca Security Server nell'inventario. Poco dopo aver eliminato la macchina virtuale, Security Server risulterà offline.
4. Seleziona la casella di controllo corrispondente a Security Server.
5. Clicca sul pulsante ⊖ **Elimina** sulla barra degli strumenti.

   Security Server verrà spostato nella cartella **Eliminato**. Da qui puoi rimuoverlo definitivamente cliccando nuovamente sul pulsante ⊖ **Elimina** nella barra degli strumenti.

7.2. Disinstallare la protezione di Exchange

Puoi rimuovere la Protezione Exchange da qualsiasi Microsoft Exchange Server che ha Bitdefender Endpoint Security Tools installato con questo ruolo. Puoi eseguire la disinstallazione nella Control Center.

1. Vai alla pagina **Rete**.
2. Seleziona il contenitore desiderato dal pannello sulla sinistra. Le entità saranno mostrate nel pannello a destra.
3. Seleziona l'endpoint da cui vuoi disinstallare la Protezione Exchange.
4. Clicca su **Riconfigura client** nel menu **Attività** nel pannello in alto della tabella. Apparirà una finestra di configurazione.
5. Nella sezione **Generale**, deseleziona la casella **Protezione Exchange**.

Avvertimento
Nella finestra di configurazione, assicurati di aver selezionato tutti gli altri ruoli che sono attivi sull'endpoint. Diversamente, saranno anch'essi disinstallati.

6. Clicca su **Salva** per creare l'attività.

Puoi visualizzare e gestire l'attività in **Rete e attività**.

Se vuoi reinstallare la Protezione Exchange, fai riferimento a «Installare la protezione di Exchange» (p. 63).

8. 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.

8.1. 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.

8.2. Necessiti di assistenza

Puoi chiederci assistenza attraverso il nostro Centro di supporto online. Compila il modulo di contatto e invialo.

8.3. 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.

8.3.1. 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.

8.3.2. 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

8.3.3. 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.

8.4. 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.

8.4.1. 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

8.4.2. 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.

8.4.3. 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. Oggetti Sandbox Analyzer

A.2.1. 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.2.2. 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.2.3. Eccezioni predefinite all'invio automatico

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

A.3. Kernel supportati dal sensore Incidenti

Il sensore Incidenti supporta i seguenti kernel: