Bitdefender

GravityZone

GUIDA PER L'ANALISTA DELLA SICUREZZA

Bitdefender GravityZone
Guida per l'analista della sicurezza

Data di pubblicazione 2021.01.12

Avvertenze legali

Bitdefender

Indice

1. INFORMAZIONI SU GRAVITYZONE

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

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)**

2.2. Advanced Threat Control

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

Advanced Threat Control monitora costantemente i processi in esecuzione e classifica i comportamenti sospetti come un tentativo di: mascherare il tipo di

processo, eseguire il codice nello spazio di un altro processo (disattivando la memoria del processo per l'escalation dei privilegi), replicare, rilasciare file, nascondere applicazioni dall'enumerazione dei processi, ecc. Ogni comportamento sospetto aumenta la valutazione del processo. Quando viene raggiunta una determinata soglia, viene attivato un allarme.

2.3. HyperDetect

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

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

2.4. Anti-exploit avanzato

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

2.5. Firewall

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

2.6. Controllo contenuti

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

2.7. Network Attack Defense

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

2.8. Patch Management

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

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

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

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

2.9. Controllo dispositivi

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

2.10. Full Disk Encryption

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

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

2.11. Security for Exchange

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

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

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

2.12. Sandbox Analyzer

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

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

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

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

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

2.13. Endpoint Detection and Response (EDR)

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

Tramite Bitdefender Endpoint Security Tools, puoi attivare un modulo di protezione chiamato Sensore EDR sui tuoi endpoint gestiti, per raccogliere i dati sull'hardware e i sistemi operativi. Seguendo un framework client-server, i metadati vengono ottenuti ed elaborati in entrambi i lati.

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

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

2.14. Endpoint Risk Analytics (ERA)

Endpoint Risk Analytics (ERA) identifica, valuta e corregge le vulnerabilità degli endpoint attraverso scansioni dei rischi (a richiesta o programmate), prendendo

in considerazione un gran numero di indicatori di rischio. Dopo aver scansionato la tua rete con determinati indicatori di rischio, avrai accesso a una panoramica dello stato di rischio della rete tramite la dashboard di **Gestione rischi**, disponibile dal menu principale. Potrai risolvere alcuni rischi di sicurezza automaticamente da GravityZone Control Center e visualizzare suggerimenti per la mitigazione dell'esposizione degli endpoint.

2.15. Email Security

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

2.16. Disponibilità dei livelli di protezione di GravityZone

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

3. ARCHITETTURA DI GRAVITYZONE

La soluzione di GravityZone include i seguenti componenti:

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

3.1. Security Server

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

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

3.2. 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

3.2.1. 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).

Livelli di protezione

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

- Antimalware
- Advanced Threat Control
- HyperDetect

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

Ruoli degli endpoint

- Utente esperto
- Relay
- Server caching patch

Utente esperto

Gli amministratori del Control Center possono garantire diritti di Utente esperto agli utenti degli endpoint tramite le impostazioni della policy. Il modulo Utente esperto consente di garantire diritti di amministrazione a livello di utente, permettendo all'utente dell'endpoint di accedere e modificare le impostazioni di sicurezza tramite una console in locale. Control Center riceve una notifica ogni volta che un endpoint passa in modalità Utente esperto e l'amministratore di Control Center può sempre sovrascrivere le impostazioni di sicurezza locali.

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

Relay

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

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

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

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

-
- 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.

3.2.2. 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

3.3. Architettura di Sandbox Analyzer

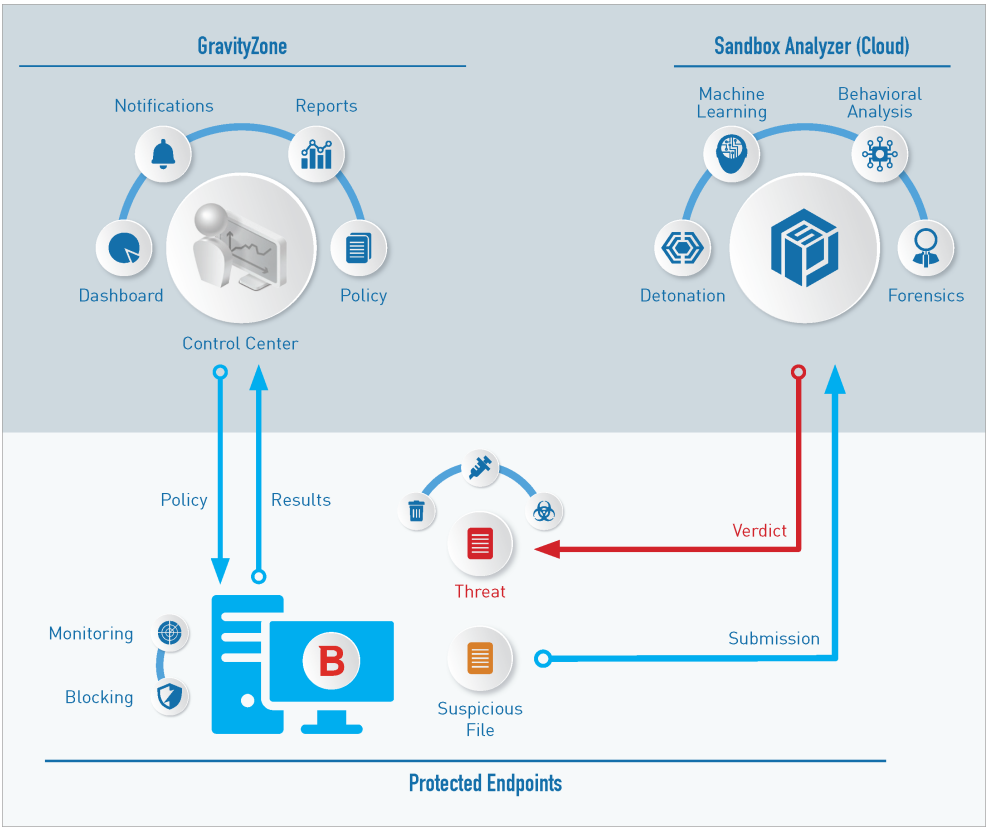
Bitdefender Sandbox Analyzer fornisce un potente livello di protezione dalle minacce avanzate, eseguendo un'analisi automatica e approfondita dei file sospetti non ancora firmati dai motori antimalware di Bitdefender.

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

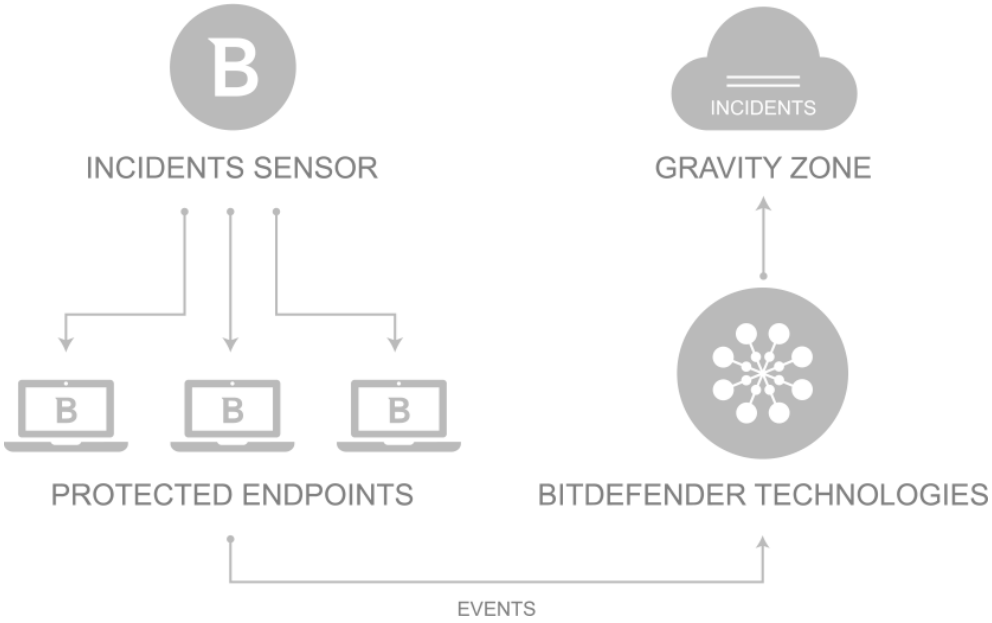
altro endpoint, si ottiene una risposta immediata, perché i risultati sono già disponibili nel database.

3.4. Architettura EDR

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

L'EDR include due componenti principali:

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



Flusso dell'EDR dall'endpoint al Control Center

4. COME INIZIARE

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

4.1. Connessione a Control Center

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

Prerequisiti:

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

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

Per connetterti a Control Center:

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

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

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

b. Autenticati con il fornitore di identità.

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

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

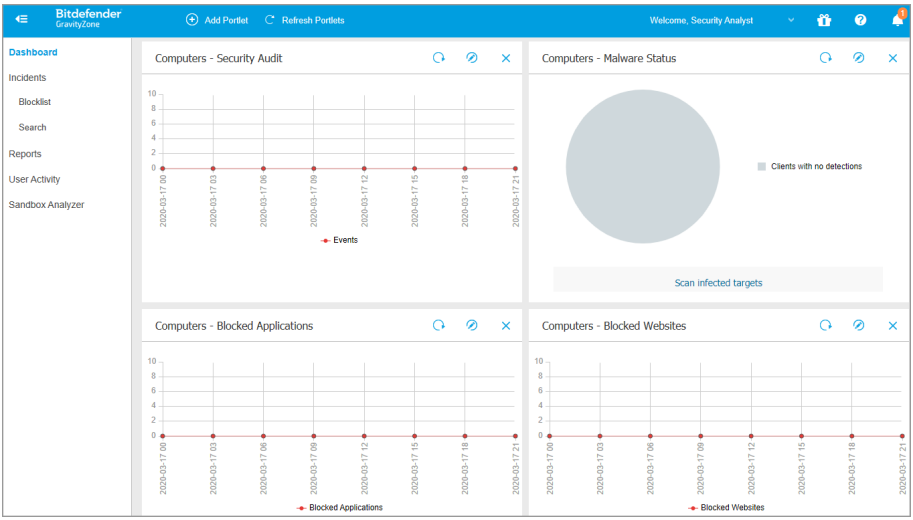
Al primo accesso, devi accettare le Condizioni d'uso di Bitdefender. Clicca su **Continua** per iniziare a usare GravityZone.

Nota

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

4.2. Control Center a prima vista

Control Center consente un accesso immediato a tutte le funzionalità. Usa la barra del menu nell'area superiore per muoverti nella console.



L'interfaccia

I segnalatori possono accedere alle seguenti sezioni nella barra del menu:

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

Rapporti
Ottieni rapporti di sicurezza relativi ai clienti gestiti.

Attività utente
Controlla il rapporto delle attività dell'utente.

Evidenziando il nome utente nell'angolo in alto a destra della console, sono disponibili le seguenti opzioni:

- **Il mio Account**. Clicca su questa opzione per gestire i dettagli e le preferenze del tuo account utente.
- **Aiuto e Supporto**. Clicca su questa opzione per trovare informazioni di aiuto e supporto.
- **Feedback**. Clicca su questa opzione per mostrare un modulo che ti consente di modificare e inviare eventuali messaggi di feedback relativi alla tua esperienza con GravityZone.

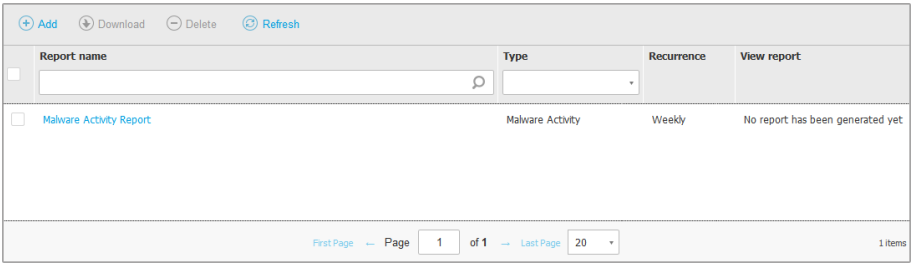
- **Uscita**. Clicca su questa opzione per uscire dal tuo account.

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

- L'icona della **modalità Aiuto**, che attiva una funzione di aiuto in grado di fornire alcune caselle di assistenza espandibili posizionate nei vari elementi di Control Center. Troverai facilmente molte informazioni utili relative alle caratteristiche di Control Center.
- L'icona **Notifiche**, che fornisce un accesso rapido ai messaggi di notifica e anche alla pagina **Notifiche**.

4.2.1. Tabella dati

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



La pagina dei rapporti

Muoversi tra le pagine

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

Cercare determinate voci

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

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

Ordinare i dati

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

Aggiornare i dati della tabella

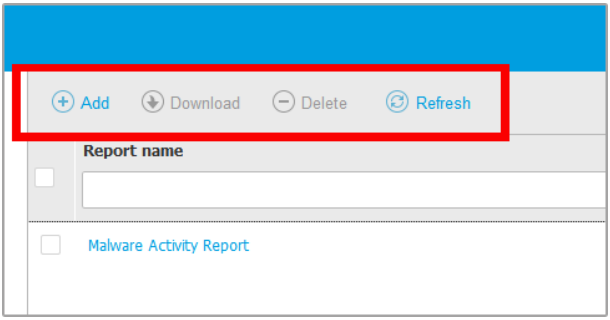
Per assicurarsi che la console mostri i dati più aggiornati, clicca sul pulsante **Aggiorna** nel lato superiore della tabella.

Potrebbe essere necessario se si trascorre molto tempo nella pagina.

4.2.2. Barre degli strumenti

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

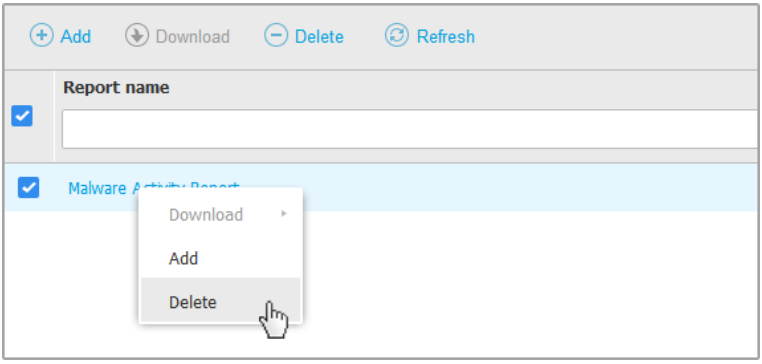
- Crea un nuovo rapporto.
- Scarica un rapporto programmato.
- Elimina un rapporto programmato.



La pagina Rapporti - Barra degli strumenti

4.2.3. Menu contestuale

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



La pagina dei Rapporti - Menu contestuale

4.3. Modificare la password di accesso

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

Si consigliare di eseguire le seguenti operazioni:

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

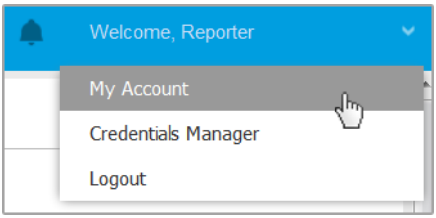
Per modificare la password di accesso:

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

4.4. Gestire il tuo account

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

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



Il menu Account utente

2. In **Dettagli account**, correggi o aggiorna i dettagli del tuo account.
   - **Nome completo.** Inserisci il tuo nome completo.
   - **E-mail.** Questo è il tuo indirizzo e-mail di accesso e contatto. A questo indirizzo vengono inviati i rapporti e le notifiche inerenti la sicurezza. Le e-mail di notifica vengono inviate automaticamente ogni volta che nella rete vengono rilevate importanti condizioni di rischio.
   - Un link **Modifica password** ti consente di modificare la tua password di accesso.
3. In **Impostazioni**, configura le impostazioni dell'account in base alle tue preferenze.
   - **Fuso orario.** Seleziona il fuso orario del tuo account dal menu. La console mostrerà le informazioni orarie in base al fuso orario selezionato.
   - **Lingua.** Seleziona la lingua utilizzata dalla console nel menu.
   - **Scadenza sessione.** Seleziona l'intervallo di tempo di inattività prima della scadenza della sessione dell'utente.
4. In **Sicurezza accesso**, configura l'autenticazione a due fattori e verifica lo stato delle policy disponibili per proteggere il tuo account di GravityZone. Le policy stabilite a livello aziendale sono di sola lettura.

   Per attivare l'autenticazione a due fattori:

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

      Quando accedi per la prima volta al tuo account di GravityZone ti sarà chiesto di scaricare e installare Google Authenticator, Microsoft Authenticator o un

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

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

Per attivare l'autenticazione a due fattori:

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

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

iii. Sul tuo dispositivo mobile, apri Google Authenticator.

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

Puoi anche inserire il codice segreto manualmente.

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

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

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

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

Nota
Tieni presente che, se la 2FA attualmente configurata viene disattivata per il tuo account, il codice segreto non sarà più valido.

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

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

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

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

Nota
Non puoi eliminare il tuo account personale.

5. INTERFACCIA DI MONITORAGGIO

Una corretta analisi della sicurezza della rete richiede l'accessibilità e la correlazione dei dati. Avere informazioni di sicurezza centralizzate consente di monitorare e garantire la conformità con le politiche di sicurezza dell'organizzazione, identificare rapidamente i problemi, e analizzare minacce e vulnerabilità.

5.1. Dashboard

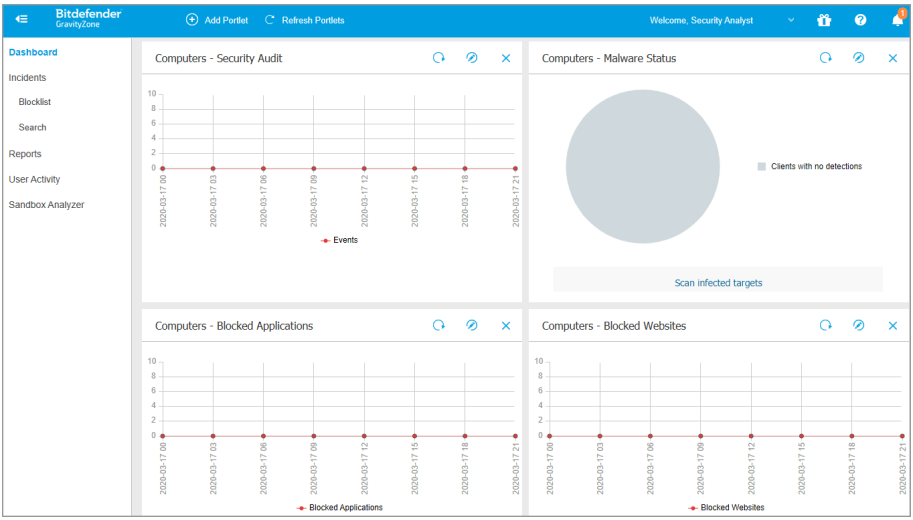
La dashboard di Control Center è una schermata personalizzabile che offre una rapida panoramica di tutti gli endpoint protetti e dello stato della rete.

Ci sono due sezioni:

- Barra della dashboard stato della rete
- Portlet dashboard

La barra di stato della rete nella dashboard ti aggiorna sul numero di incidenti aperti o in corso, le risorse minacciate (endpoint) e le minacce rilevate nella propria rete. Usa queste informazioni per scoprire eventuali elementi di rete non risolti. Clicca su **Vedi** per accedere alla pagina **Incidenti**. Per maggiori informazioni, fai riferimento a «Indagare sugli incidenti» (p. 28).

I portlet della dashboard mostrano diverse informazioni sulla sicurezza in tempo reale, utilizzando diagrammi facilmente consultabili per identificare rapidamente ogni problema che potrebbe richiedere la tua attenzione.



L'interfaccia

Ecco quello che devi sapere sui portlet della dashboard:

- Control Center ha diversi portlet predefiniti nella dashboard.
- Ogni portlet della dashboard include un rapporto dettagliato in background, accessibile con un semplice click sul diagramma.
- Ci sono diversi tipi di portlet che includono varie informazioni sulla protezione dell'endpoint, come stato di aggiornamento, stato dei malware e attività del firewall.

> **Nota**
> Di norma, i portlet recuperano i dati per il giorno attuale e, a differenza dei rapporti, non possono essere impostati per intervalli superiore a un mese.

- Le informazioni mostrate tramite portlet fanno riferimento a endpoint solo nel tuo account. Puoi personalizzare il bersaglio e le preferenze di ciascun portlet utilizzando il comando **Modifica portlet**.
- Clicca sulle voci della legenda del diagramma, se disponibili, per nascondere o mostrare la variabile corrispondente sul grafico.
- I portlet vengono mostrati in gruppi di quattro. Usa la barra di scorrimento verticale o i tasti freccia su e giù per sfogliare i diversi gruppi di portlet.

- Per gli utenti nelle aziende partner sono disponibili portlet specifici (**Stato licenza**, **Panoramica stato cliente** e **Top 10 aziende infettate**).
- Per diverse tipologie di rapporto, hai la possibilità di avviare istantaneamente determinate attività sugli endpoint di destinazione, senza dover andare alla pagina **Rete** per eseguire tale attività (per esempio, una scansione degli endpoint infetti o un aggiornamento per gli endpoint). Usa il pulsante nel lato inferiore del portlet per eseguire l'azione disponibile.

La dashboard è facile da configurare, basandosi sulle preferenze individuali. Puoi modificare le impostazioni del portlet, aggiungere altri portlet, rimuovere o riorganizzare i portlet esistenti.

5.1.1. Aggiornare i dati del portlet

Per assicurarti che il portlet mostri le informazioni più recenti, clicca sul pulsante **Aggiorna** sulla sua barra del titolo.

Per aggiornare le informazioni per tutti i portlet contemporaneamente, clicca sul pulsante **Aggiorna portlet** in cime alla dashboard.

5.1.2. Modificare le impostazioni del portlet

Alcuni portlet offrono informazioni sullo stato, mentre altri segnalano gli eventi di sicurezza avvenuti nell'ultimo periodo. Puoi controllare e configurare il periodo di segnalazione di un portlet, cliccando sull'icona **Modifica portlet** nella sua barra del titolo.

5.1.3. Aggiungere un nuovo portlet

Puoi aggiungere altri portlet per ottenere le informazioni di cui necessiti.

Per aggiungere un nuovo portlet:

1. Vai alla pagina **Dashboard**.
2. Clicca sul pulsante **Aggiungi portlet** nel lato superiore della console. Viene mostrata la finestra di configurazione.
3. Nella scheda **Dettagli**, configura i dettagli del portlet:
   - Tipo di rapporto in background
   - Nome indicativo del portlet
   - L'intervallo di tempo per gli eventi da segnalare

   Per maggiori informazioni sui tipi di rapporto disponibili, fai riferimento a «Tipo di rapporto» (p. 101).

4. Nella scheda **Bersagli**, seleziona gli elementi e i gruppi della rete da includere.
5. Clicca su **Salva**.

5.1.4. Rimuovere un portlet

Puoi rimuovere facilmente ogni portlet cliccando sull'icona ⊗ **Rimuovi** nella sua barra del titolo. Una volta rimosso un portlet, non puoi più ripristinarlo. Tuttavia, puoi creare un altro portlet con le stesse impostazioni.

5.1.5. Riorganizzare i portlet

Puoi riorganizzare i portlet della dashboard per adattarsi meglio alle tue esigenze. Per riorganizzare i portlet:

1. Vai alla pagina **Dashboard**.
2. Trascina e rilascia ciascun portlet nella posizione desiderata. Tutti gli altri portlet tra le nuove e vecchie posizioni vengono spostati per preservarne l'ordine.

> **Nota**
> Puoi spostare i portlet solo in posizioni già prese.

6. INDAGARE SUGLI INCIDENTI

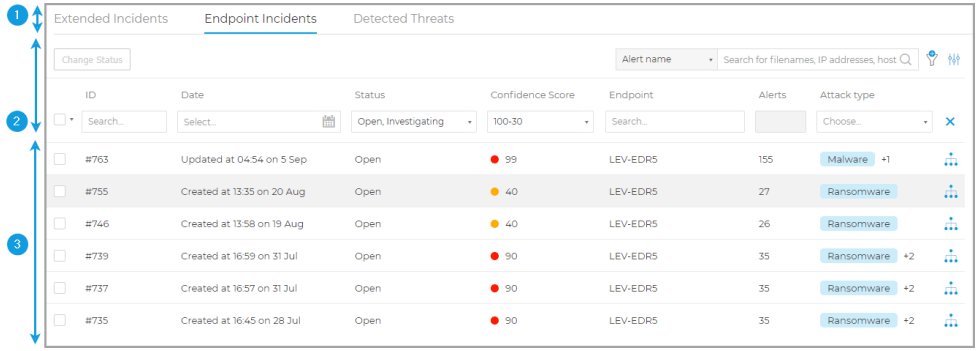
La sezione **Incidenti** aiuta a filtrare, analizzare e intraprendere azioni su tutti gli eventi di sicurezza rilevati dal Sensore incidenti in un determinato intervallo di tempo.

La sezione **Incidenti** include le seguenti pagine:

- **Incidenti**: consente di visualizzare e studiare gli eventi di sicurezza.
- **Lista bloccati**: gestisce i file bloccati coinvolti negli eventi di sicurezza.
- **Ricerca**: fornisce opzioni per analizzare il database degli eventi di sicurezza.

6.1. La pagina Incidenti

Usa la pagina **Incidenti** per filtrare e gestire gli eventi di sicurezza.



Panoramica pagina degli incidenti

Nota
La disponibilità di queste schede potrebbe differire in base alla licenza inclusa nel tuo piano attuale.

Questa pagina include le seguenti aree:

1. Una barra della finestra con schede che includono diversi tipi di incidente:
   - **Incidenti endpoint**: mostra tutti gli incidenti rilevati a livello di endpoint, che richiedono un'indagine e su cui non è ancora stata intrapresa un'azione.

- **Minacce rilevate**: mostra tutti gli eventi di sicurezza identificati come minacce dai moduli di prevenzione di GravityZone. Questi incidenti sono rilevati a livello di endpoint e vengono eseguiti con azioni predefinite nelle policy di sicurezza applicate al tuo ambiente.

2. Opzioni di filtro per personalizzare la tua griglia:
   - Clicca sul pulsante **Mostra/Nascondi colonne** per aggiungere o rimuovere colonne al filtro.

     La pagina si aggiornerà automaticamente, caricando le schede degli eventi di sicurezza con informazioni che corrispondono alle colonne aggiunte.
   - Clicca sul pulsante **Mostra/Nascondi filtri** per mostrare o nascondere la barra dei filtri.
   - Clicca sul pulsante **Cancella filtri** per reimpostare tutti i filtri.
3. La griglia Incidenti, che mostra un elenco degli eventi di sicurezza che corrispondono ai filtri applicati.

Nota
Questa funzionalità non supporta più Internet Explorer.

La barra Panoramica

La barra **Panoramica** elenca gli incidenti aperti, le principali allerte, i dispositivi interessati, oltre a molti altri dati importanti, per darti una rapida visione sulla situazione generale sulle minacce che il tuo ambiente sta affrontando.

La barra Panoramica

Nota
Disponibilità e contenuti della barra **Panoramica** potrebbero differire in base alla licenza inclusa nel tuo piano attuale.

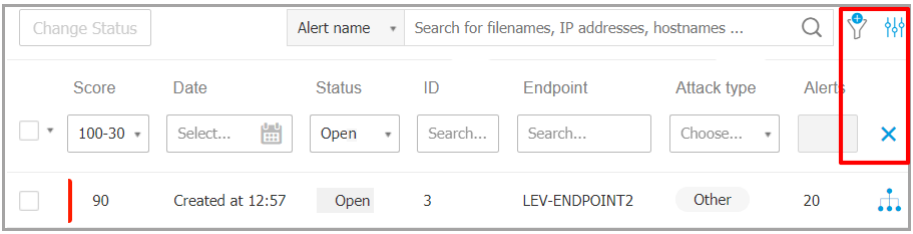
Filtrare gli incidenti dalla barra Panoramica

Puoi filtrare l'elenco degli incidenti selezionando i valori nella barra Panoramica:

- Cliccando su un valore nella sezione **INCIDENTI APERTI**, sarà possibile mostrare solo gli incidenti con il livello di severità selezionato.
- Cliccando su un valore nella sezione **ALLERTE PRINCIPALI**, si inserirà nel campo di ricerca il nome dell'allerta e saranno mostrati solo gli incidenti in cui l'allerta è stata rilevata.
- Cliccando su un valore nella sezione **TECNICHE PRINCIPALI**, si inserirà nel campo di ricerca il nome della tecnica e saranno mostrati solo gli incidenti in cui la tecnica è stata rilevata.
- Cliccando su un valore nella sezione **PRINCIPALI DISPOSITIVI INTERESSATI**, saranno mostrati solo gli incidenti che interessano il dispositivo selezionato.

6.1.1. La griglia dei filtri

La pagina **Incidenti** ti consente di scegliere quali incidenti mostrare personalizzando la griglia dei filtri.



La griglia dei filtri

- Clicca sul pulsante **Mostra/Nascondi colonne** per aggiungere o rimuovere colonne al filtro.

  La pagina si aggiornerà automaticamente, caricando le schede degli eventi di sicurezza con informazioni che corrispondono alle colonne aggiunte.
- Clicca sul pulsante **Mostra/Nascondi filtri** per mostrare o nascondere la barra dei filtri.
- Clicca sul pulsante **Cancella filtri** per reimpostare tutti i filtri.

Puoi trovare maggiori dettagli sulle opzioni di filtraggio disponibili nella seguente tabella:

Opzioni di filtro	Dettagli
Punteggio	Il punteggio di sicurezza è un numero tra 100 e 10, che indica il potenziale livello di pericolosità di un evento di sicurezza. Maggiore è il punteggio, più l'evento è pericoloso con maggiore certezza. Indica il contesto in base agli indicatori di attacco e alle tecniche di attacco, se applicabili. Per filtrare in base al punteggio di sicurezza, trascina la barra di scorrimento fino ai valori desiderati. In alternativa, puoi usare il campo numerico sotto la barra. Clicca su **OK** per confermare la selezione del punteggio.
Data	Per filtrare in base alla data: 1. Clicca sull'icona del calendario o il campo **Data** per aprire la pagina di configurazione della data. 2. Seleziona l'intervallo di tempo quando si è verificato l'incidente: • Clicca sulle schede **Da** e **A** per selezionare le date che definiscono l'intervallo di tempo. **Nota** Puoi indicare il momento esatto per le date di inizio e fine, usando i campi ore e minuti sotto il calendario. • Puoi anche selezionare un intervallo di tempo predeterminato, relativo al momento attuale (gli ultimi 7 giorni. Per ulteriore spazio di archiviazione per gli eventi devi contattare il tuo rappresentante vendite per fare l'upgrade della soluzione con un add-on **Conservazione dati** di 30, 90 o 180 giorni. 3. Clicca su **OK** per applicare il filtro.
Stato	Filtra gli incidenti in base al proprio stato attuale selezionando una o più opzioni di stato, disponibili nel menu a discesa **Stato**: • **Apri**: per gli eventi di sicurezza non analizzati • **In corso di indagine**: per gli eventi di sicurezza sotto indagine.

Opzioni di filtro	Dettagli
	• **Falso positivo**: per gli eventi di sicurezza etichettati come falso allarme • **Chiusi**: per gli eventi di sicurezza con un'indagine chiusa.
ID	Riduci l'elenco degli incidenti cercando un numero ID specifico dell'evento di sicurezza.
Endpoint	Riduci l'elenco degli incidenti cercando un determinato nome dell'endpoint dalla tua rete gestita.
Tipo di attacco	Il tipo di attacco è un elenco dinamico dei tipi più comuni di attacco, che cambia in base agli indicatori di attacco presenti negli eventi di sicurezza elencati.
Avvisi	La colonna **Allerte** mostra il numero di allerte attivate per incidente.
SO endpoint	Questa opzione filtra gli eventi di sicurezza in base al sistema operativo degli endpoint coinvolti.

Nota
Le opzioni di filtro potrebbero variare in base al tipo di codice di licenza incluso nel tuo piano attuale.

Per cercare altri elementi non visibili nella griglia del filtro, selezionare una delle opzioni di ricerca dal menu a discesa **Cerca**:

- **Nome dell'allerta** - da 3 a 1.000 caratteri al massimo.
- **Tecnica ATT&CK** - 100 caratteri al massimo.
- **IP endpoint** - 45 caratteri al massimo.
- **MD5** - 32 caratteri al massimo.
- **SHA256** - 64 caratteri al massimo.
- **Nome del nodo** - 360 caratteri al massimo.
- **Nome utente** - 1.000 caratteri al massimo.

La pagina si aggiornerà automaticamente, caricando solo le schede degli eventi di sicurezza che corrispondono all'elemento cercato. Per una ricerca più granulare, puoi creare delle query di ricerca nella Pagina di ricerca.

6.1.2. Visualizzare la lista degli eventi di sicurezza

La pagina **Incidenti** mostra un elenco di eventi di sicurezza che corrispondono ai filtri selezionati.

Di norma, ci sono 20 eventi per pagina, raccolti per data. La pagina si aggiorna automaticamente a intervalli regolari, mentre l'EDR attiva nuovi eventi.

Importante
Tutti gli eventi di sicurezza più vecchi di 90 giorni vengono automaticamente eliminati dalla sezione **Incidenti endpoint** e dalla sezione **Minacce rilevate**, oltre che dall'archivio degli eventi di sicurezza.

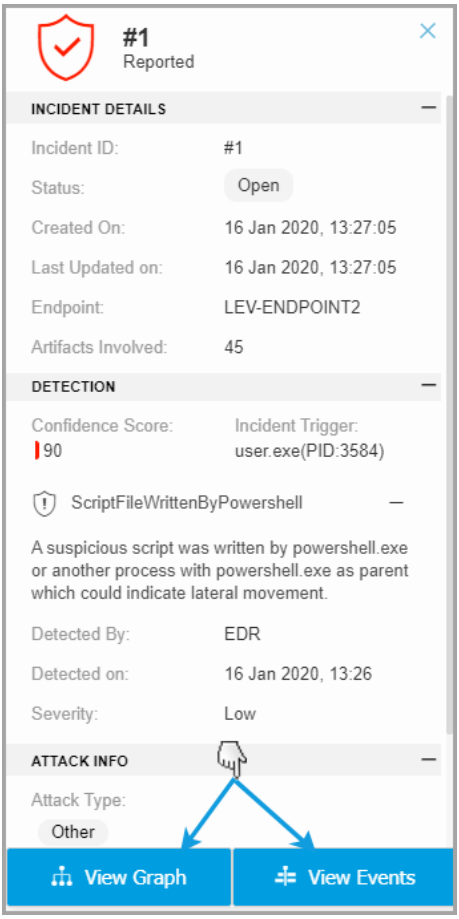
Per navigare nella pagina, usa i tasti di direzione o la rotellina del mouse oppure clicca la barra di scorrimento. Cambia il numero di eventi mostrati in fondo alla pagina. Puoi avere fino a 100 eventi per pagina.

Ogni voce dell'evento di sicurezza è elencata in un formato rich card e fornisce una panoramica di ciascun incidente, con informazioni basate sui filtri selezionati.

Nota
Controlla il colore del bordo sinistro per valutare rapidamente il livello di confidenza (basso, medio o alto).

Scheda evento di sicurezza

- Cliccando sul pulsante **Vedi grafico** corrispondente della scheda di un evento di sicurezza, potrai aprirlo in una nuova pagina, dove potrai analizzare l'incidente in dettaglio e intraprendere le azioni appropriate.
- Cliccando sulla scheda di un evento di sicurezza, si aprirà un pannello di visualizzazione rapida laterale con informazioni sull'incidente selezionato.



Visuale rapida dei dettagli dell'incidente

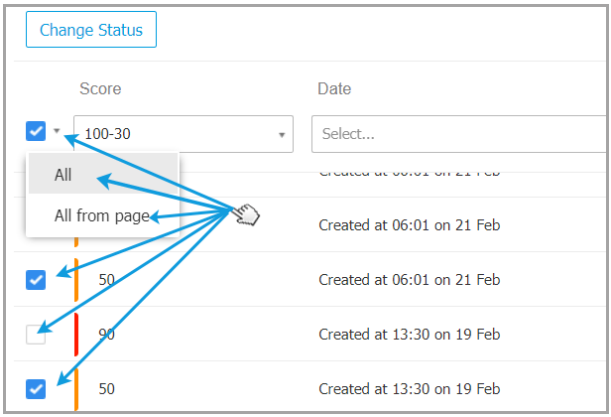
  - Clicca sul pulsante **Vedi grafico** per accedere alla visualizzazione grafica dell'incidente.
  - Clicca sul pulsante **Vedi eventi** per accedere alla cronologia dell'incidente.
- Selezionando la casella della scheda di un qualsiasi evento di sicurezza, si attiverà il pulsante **Cambia stato**, che ti consentirà di modificare lo stato attuale dell'incidente.

Modificare lo stato degli eventi di sicurezza

Lo stato dell'indagine ti aiuta a tenere traccia degli incidenti che sono già stati analizzati e marcati come chiusi o falsi positivi, degli incidenti che sono attualmente sotto indagine, e dei nuovi incidenti o quelli aperti che devono ancora essere analizzati.

Puoi scegliere di modificare lo stato di uno o più eventi di sicurezza alla volta:

1. Seleziona le caselle delle schede dell'evento di sicurezza che subiranno un cambiamento di stato.

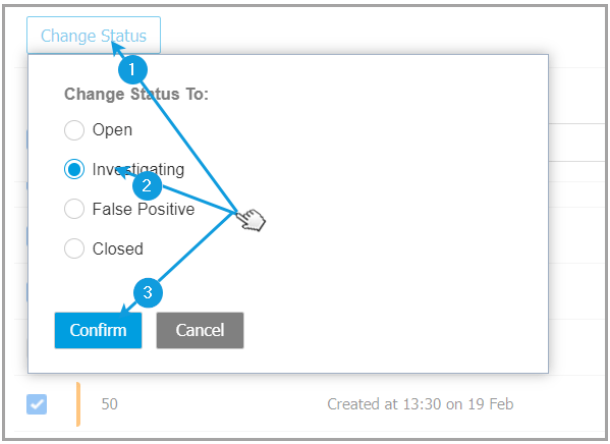


Selezionare le schede degli eventi di sicurezza

Puoi selezionarle individualmente usando le opzioni di selezione in blocco nel menu a discesa.

Nota
Puoi anche scorrere tra le pagine di diversi eventi di sicurezza mantenendo la tua selezione.

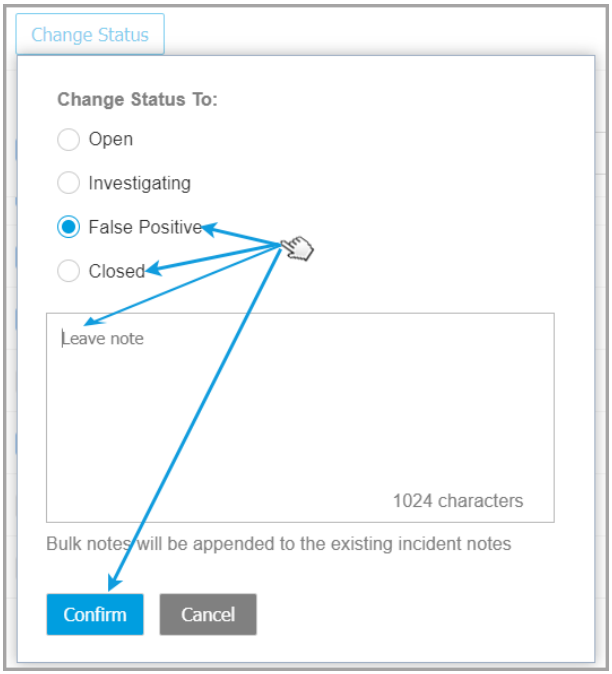
2. Clicca sul pulsante **Cambia stato** e seleziona le opzioni desiderate:



Modificare lo stato dell'evento di sicurezza

- **Aperto** - Quando l'evento di sicurezza non è ancora sotto indagine.
- **Indagine in corso**- quando hai iniziato a indagare sull'evento.
- **Falso positivo** - quando hai analizzato l'evento, identificandolo come un falso positivo.
- **Chiusa**- quando hai completato l'indagine.

Nota
Quando si modifica lo stato degli eventi in **Falso positivo** o **Chiuso** si aprirà una finestra, dove potrai lasciare una nota sulle motivazioni del cambio di stato dell'evento, per eventuali consultazioni successive.



Lasciare una nota per gli eventi indicati come chiusi o falsi positivi

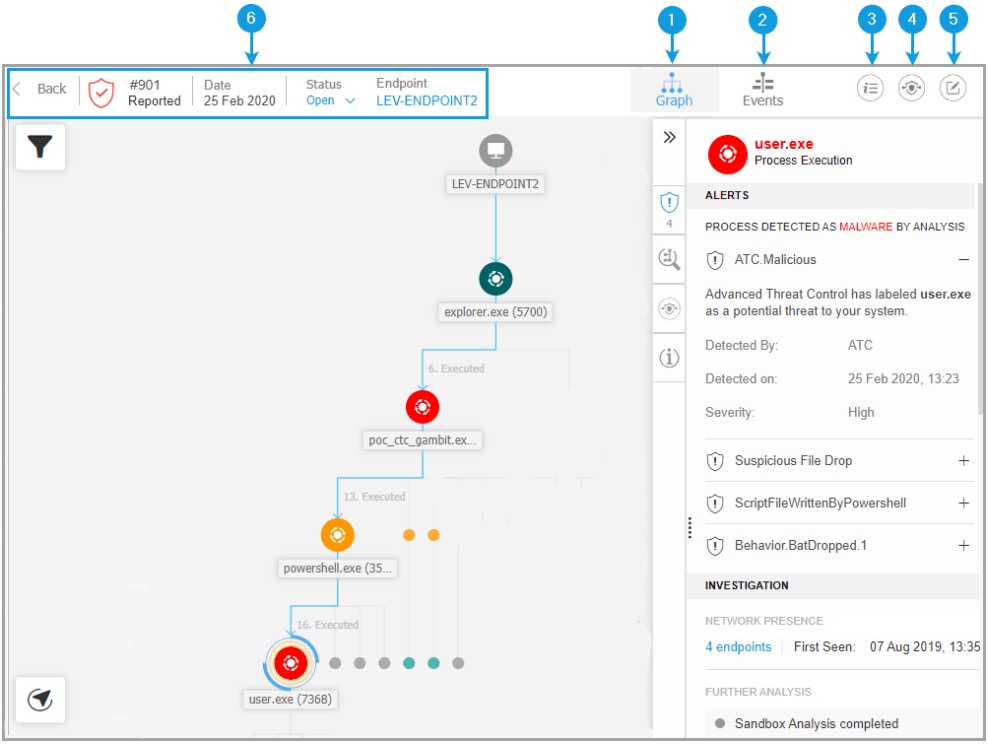
Nota
La nota sarà aggiunta a quelle già esistenti all'interno degli incidenti filtrati.

3. Clicca su **Conferma** per applicare l'opzione di stato selezionata.

6.1.3. Indagare un incidente degli endpoint

Nella pagina **Incidenti**, identifica l'evento di sicurezza che vuoi analizzare e clicca sul pulsante **Vedi grafico** per mostrarlo in una nuova pagina.

Ogni incidente di sicurezza ha una pagina dedicata contenente informazioni dettagliate sulla sequenza degli eventi (visualizzata nel grafico come nodi di eventi di sicurezza collegati) che hanno portato all'attivazione dell'incidente e offre opzioni per eseguire azioni correttive.


6
1
2
3
4
5
Back
#901
Reported
Date
25 Feb 2020
Status
Open
Endpoint
LEV-ENDPOINT2
Graph
Events
LEV-ENDPOINT2
explorer.exe (5700)
6. Executed
poc_ctc_gambit.ex...
13. Executed
powershell.exe (35...
16. Executed
user.exe (7368)
user.exe
Process Execution
ALERTS
PROCESS DETECTED AS MALWARE BY ANALYSIS
ATC.Malicious
Advanced Threat Control has labeled user.exe as a potential threat to your system.
Detected By: ATC
Detected on: 25 Feb 2020, 13:23
Severity: High
Suspicious File Drop
ScriptFileWrittenByPowershell
Behavior.BatDropped.1
INVESTIGATION
NETWORK PRESENCE
4 endpoints
First Seen: 07 Aug 2019, 13:35
FURTHER ANALYSIS
Sandbox Analysis completed

1. Scheda Grafico

   Il grafico mostra l'incidente di sicurezza e i suoi elementi costitutivi, evidenziando il percorso critico dell'incidente e mostrando i dettagli del nodo che ha attivato l'incidente nel pannello **Dettagli nodo**.

2. Scheda Eventi

   La scheda Eventi visualizza eventi e avvisi di sistema rilevati filtrabili, e le relative descrizioni degli eventi.

3. Pannello Informazioni incidente

   Questo pannello include sezioni comprimibili con dettagli come ID incidente, stato attuale, data e ora di creazione e aggiornamento per l'ultima volta, numero di elementi coinvolti, nome del trigger e informazioni sull'attacco.

4. Pannello Riparazione

   Questo pannello include sezioni flessibili con le azioni intraprese automaticamente da GravityZone e i passaggi suggeriti da seguire per contenere l'incidente.

5. Note negli appunti

   Cliccando sul pulsante **Note** si apre un blocco degli appunti in cui è possibile aggiungere note sull'incidente attuale, che sarà possibile leggere quando si rivedrà l'incidente in un secondo momento.

6. Barra stato incidente

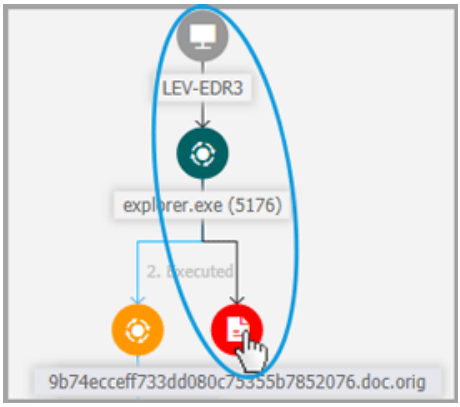
   La barra dello stato offre dettagli sull'ID dell'incidente, la data e l'ora in cui è stato generato, lo stato, il trigger dell'incidente e l'endpoint coinvolto. Cliccando sul pulsante **Indietro** tornerai alla pagina principale **Incidenti**.

Nodi eventi di sicurezza

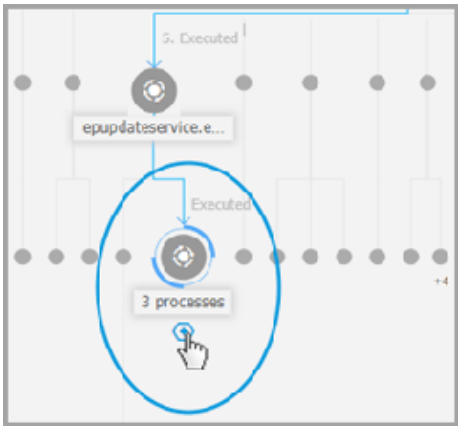
Questo è ciò che devi sapere sui nodi degli eventi di sicurezza:

- Ogni nodo rappresenta un determinato elemento coinvolto nell'incidente analizzato.
- Tutti i nodi che compongono il percorso critico vengono mostrati con più dettagli per impostazione predefinita quando si apre l'incidente, mentre gli altri elementi vengono sbiaditi, per evitare di ingombrare la vista.

– Passando il mouse su un nodo che non fa parte del percorso critico lo evidenzierai, mostrando il percorso per il punto di origine, senza interrompere il Percorso critico.



- Tre o più nodi dello stesso tipo di evento generati da un nodo parentale vengono raggruppati in un nodo cluster espandibile.



– Solo i nodi senza elementi figlio saranno nascosti nel grafico dell'incidente quando il nodo cluster viene eliminato.

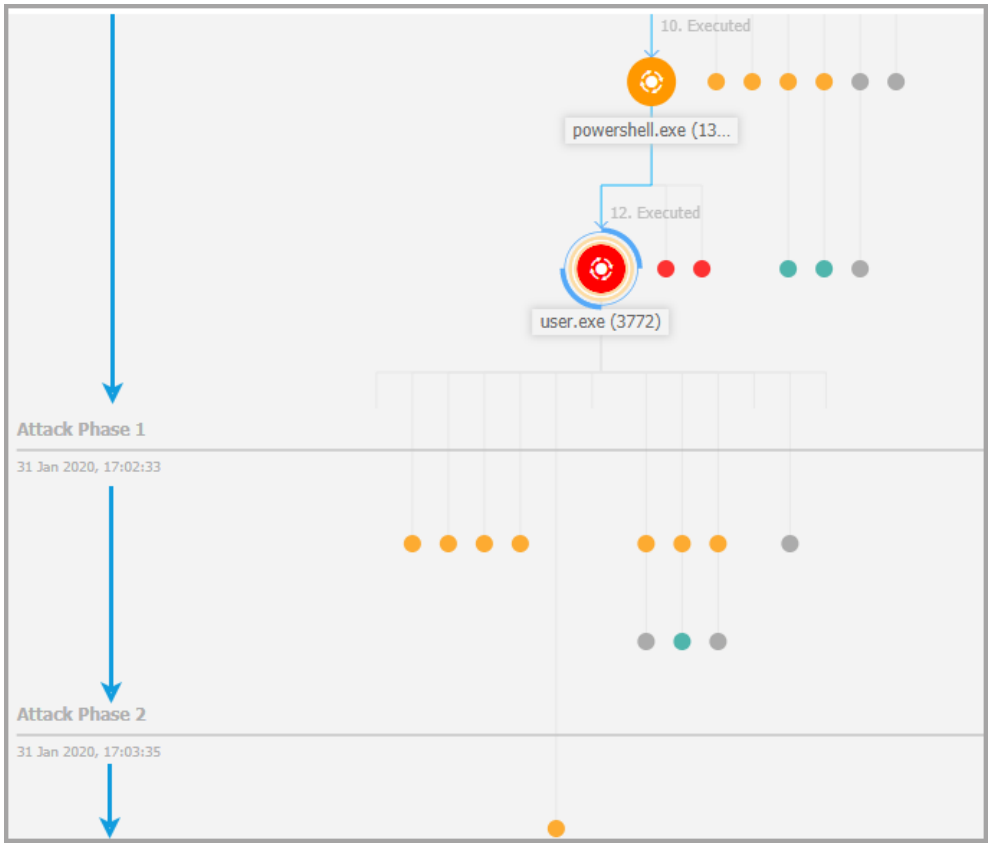
  - I nodi in cui è stata rilevata un'attività sospetta non saranno aggiunti al nodo del cluster.
- Cliccando su un nodo, saranno mostrati i seguenti dettagli:
  - Evidenzierà in blu il percorso per il nodo dell'endpoint insieme a tutti gli altri elementi coinvolti.
  - Un pannello laterale con sezioni espandibili che forniscono informazioni dettagliate sul nodo selezionato, avvisi nel caso in cui vengano evidenziati rilevamenti, le azioni disponibili ed eventuali suggerimenti. Fai riferimento a «Dettagli nodo» (p. 52) per maggiori informazioni.
- I nodi sono collegati da linee di freccia che indicano il corso delle azioni che si sono verificate sull'endpoint durante l'incidente. Ogni linea è indicata con il nome dell'azione e il suo numero cronologico.

I seguenti elementi di un incidente possono essere rappresentati come nodi:

Tipo di nodo	Descrizione
Endpoint	Mostra i dettagli dell'endpoint e lo stato della gestione delle patch.
Dominio	Mostra informazioni sull'host del dominio e i relativi endpoint.
Processo	Mostra i dettagli sul ruolo del processo nell'incidente attuale, informazioni sui file, dettagli sulle esecuzioni dei processi, la presenza di rete e ulteriori opzioni dell'indagine.
File	Mostra dettagli sul ruolo del file nell'incidente attuale, le informazioni dei file, la presenza di rete e ulteriori opzioni dell'indagine.
Registro	Mostra informazioni del registro e dettagli sul processo parentale.

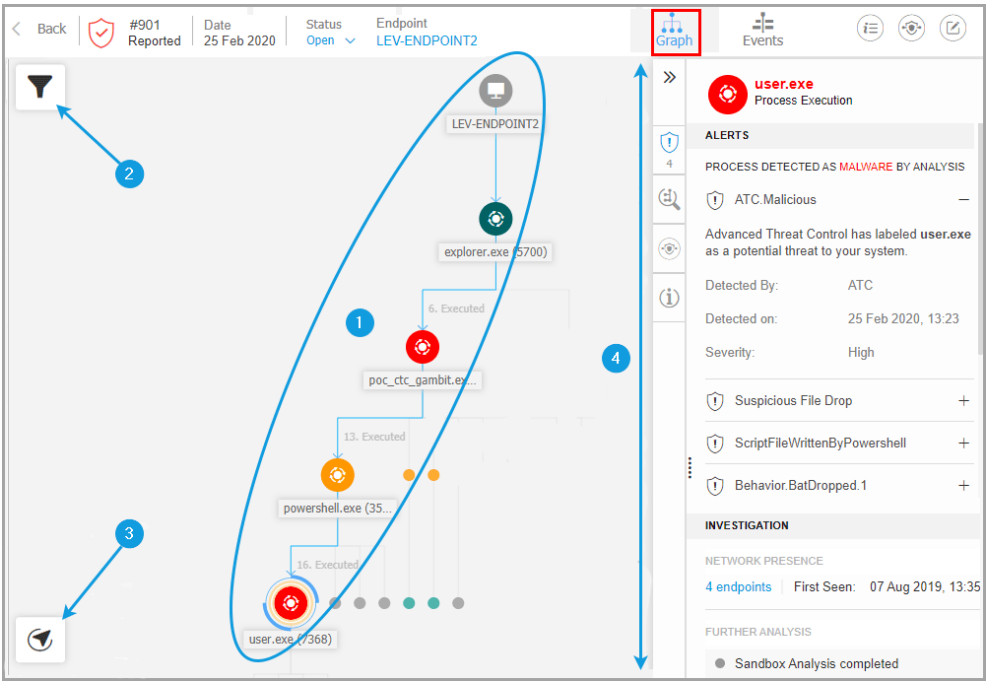
Grafico

Il **Grafico** fornisce una rappresentazione grafica interattiva dell'incidente indagato e il suo contesto, evidenziando la sequenza di elementi direttamente coinvolti nell'attivazione, nota come **Percorso critico** dell'incidente, oltre a tutti gli altri elementi coinvolti, che sono sbiaditi per impostazione predefinita. In caso di incidenti complessi che si evolvono nel tempo, il grafico mostra ogni singola fase dell'attacco.



Attacco organizzato

Il grafico include opzioni di filtraggio che consentono una personalizzazione grafica dell'incidente per migliorarne la visualizzazione, oltre a funzionalità per esplorare la mappa dell'incidente e pannelli di dettagli con maggiori informazioni su ciascun elemento.



La scheda Grafico

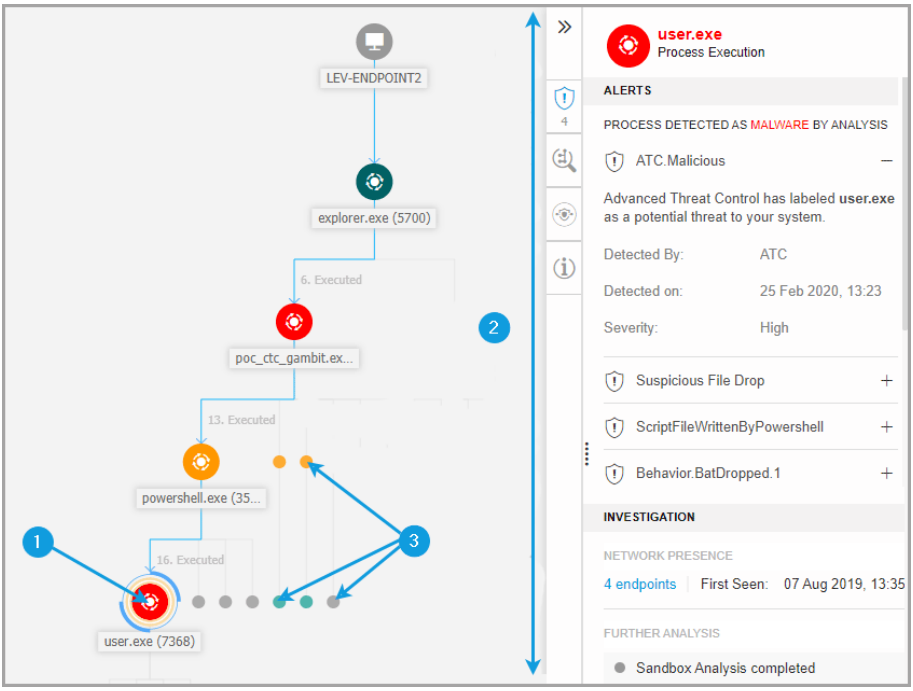
1. Percorso critico
2. Menu Filtri
3. Menu navigatore
4. Pannello dettagli nodo

Percorso critico

Il **Percorso critico** è la sequenza degli eventi di sicurezza collegati che hanno portato alla creazione di un'allerta, a partire dal punto di ingresso nella rete fino al nodo dell'evento che ha causato l'incidente. Il percorso critico dell'incidente è evidenziato per impostazione predefinita nel grafico, con tutti i nodi degli eventi consistenti su di esso, mentre gli altri elementi saranno minimizzati.

Il nodo del trigger si distingue facilmente dal resto degli elementi nel grafico, essendo circondato da funzionalità di evidenziazione aggiuntive (due cerchi

arancioni). Inoltre, viene visualizzato un pannello informativo correlato per impostazione predefinita accanto al grafico dell'incidente, che fornisce informazioni dettagliate sul nodo del trigger.



Percorso critico

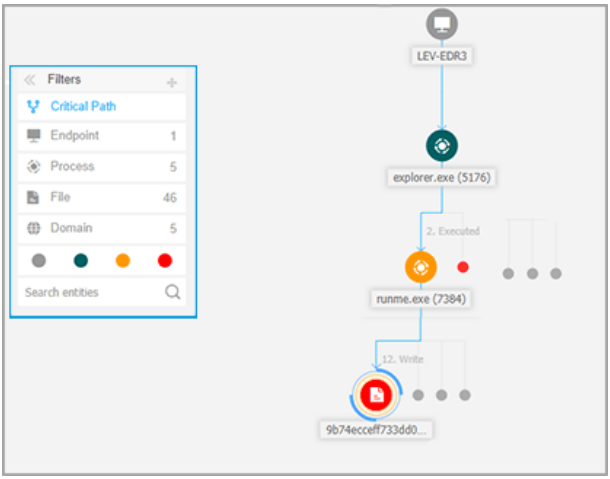
1. Nodo del trigger
2. Il pannello Dettagli nodo con informazioni raggruppate in categorie e sezioni a scomparsa
3. I nodi sbiaditi indirettamente coinvolti nell'incidente

Nota
Cliccando su un altro elemento rispetto al nodo del trigger si interromperà il percorso critico, evidenziando il percorso per l'origine, dal nodo selezionato a monte al nodo dell'endpoint.

Filtri

Il menu **Filtri** offre funzionalità di filtro avanzate, che consentono la completa manipolazione del grafico dell'incidente, evidenziando gli elementi in base al loro tipo o rilevanza, o nascondendoli per rendere l'incidente più compatto e facile da analizzare.

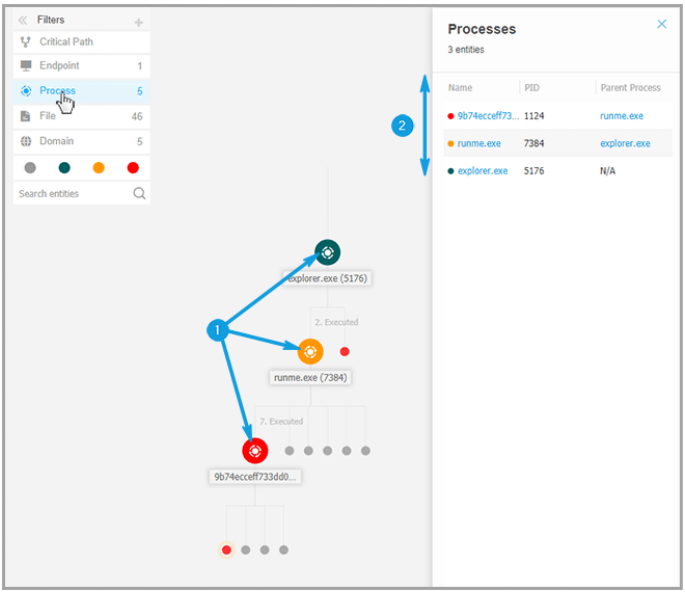
Clicca e tieni premuto sull'icona **Trascina** per posizionare il pannello Filtri in qualsiasi punto del grafico dell'incidente.



Filtri grafico incidente

Quando si seleziona un filtro di tipo elemento:

1. Il grafico dell'incidente si rimpicciolisce ed evidenzia tutti gli elementi del tipo selezionato, mentre gli elementi di un altro tipo vengono sbiaditi.
2. Apre istantaneamente un pannello con l'elenco di tutti gli elementi evidenziati.



Nota
Selezionando un elemento dall'elenco visualizzato lo evidenzierai nel grafico dell'incidente, aprendo anche un pannello con informazioni relativi a quell'elemento. Può essere applicato solo un filtro alla volta.

Le opzioni di filtro includono:

- **Percorso critico**: evidenzia il percorso critico dell'incidente di compromissione.
- **Endpoint**: evidenzia gli endpoint coinvolti dall'incidente.
- **Processo**: evidenzia tutti i nodi di tipo processo coinvolti nell'incidenti.
- **File**: evidenzia i nodi di tipo file coinvolti nell'incidente.
- **Dominio**: evidenzia tutti i nodi di tipo dominio coinvolti nell'incidente.
- **Registro**: evidenzia tutti i nodi di tipo registro coinvolti nell'incidente.

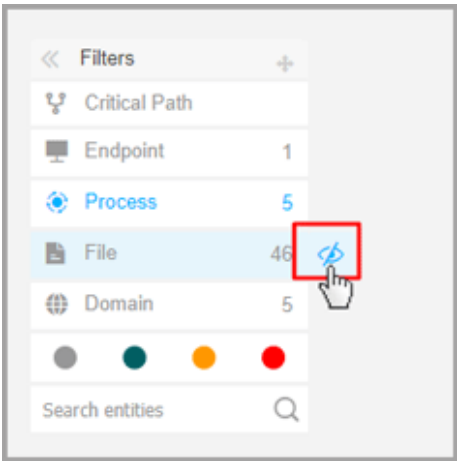
- **Rilevanza degli elementi**: è possibile anche filtrare gli elementi per la loro importanza nell'incidente.
  - **Nodo neutrale**: elementi senza alcun impatto diretto nell'incidente di sicurezza.
  - **Nodo importante**: elementi con un ruolo importante nell'incidente di sicurezza.
  - **Nodo di origine**: il punto di ingresso dell'attacco all'interno della rete.
  - **Nodo sospetto**: elementi con un comportamento sospetto, direttamente coinvolti nell'incidente di sicurezza.
  - **Nodo dannoso**: elementi che hanno causato danni nella tua rete.

    Nota
    Passando il mouse su uno dei filtri colorati viene visualizzato il numero di elementi con la stessa rilevanza coinvolti nell'incidente.

- **Ricerca entità**: è possibile cercare nomi o estensioni di file dei componenti degli incidenti nel campo di ricerca e i risultati saranno visualizzati nel pannello laterale.

Se non viene selezionato alcun filtro, il grafico dell'incidente viene ripristinato al suo stato predefinito, con endpoint, origine ed elementi trigger evidenziati, mentre gli altri elementi vengono sbiaditi.

Puoi anche nascondere determinati elementi dal grafico dell'incidente cliccando sul pulsante **Mostra/Nascondi** posizionando il mouse sul filtro del tipo: File, Dominio e Registro.



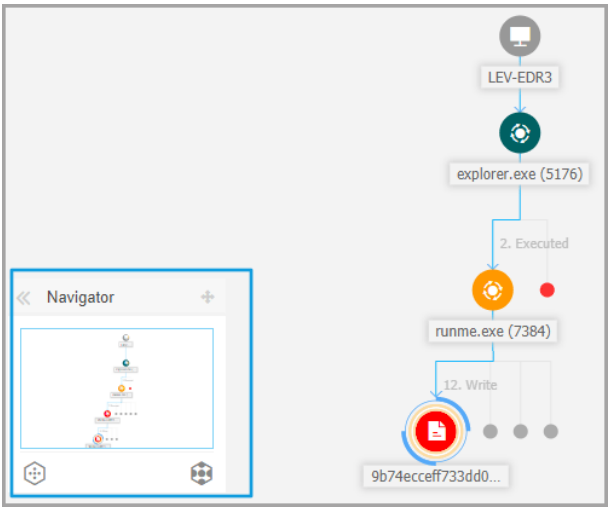
Nascondere un tipo di elemento ridisegna il grafico dell'incidente rimuovendo tutti gli elementi corrispondenti, anche se vengono ingranditi, ad eccezione del nodo trigger e dei nodi con elementi figli.

Navigatore

Il **Navigatore** ti consente di spostarti rapidamente attraverso il grafico dell'incidente ed esplorare tutti gli elementi visualizzati usando la mini-mappa e i diversi livelli di visualizzazione.

Clicca e tieni premuto sull'icona ✣ **Trascina** per posizionare il pannello Navigatore mobile ovunque all'interno del grafico dell'incidente.

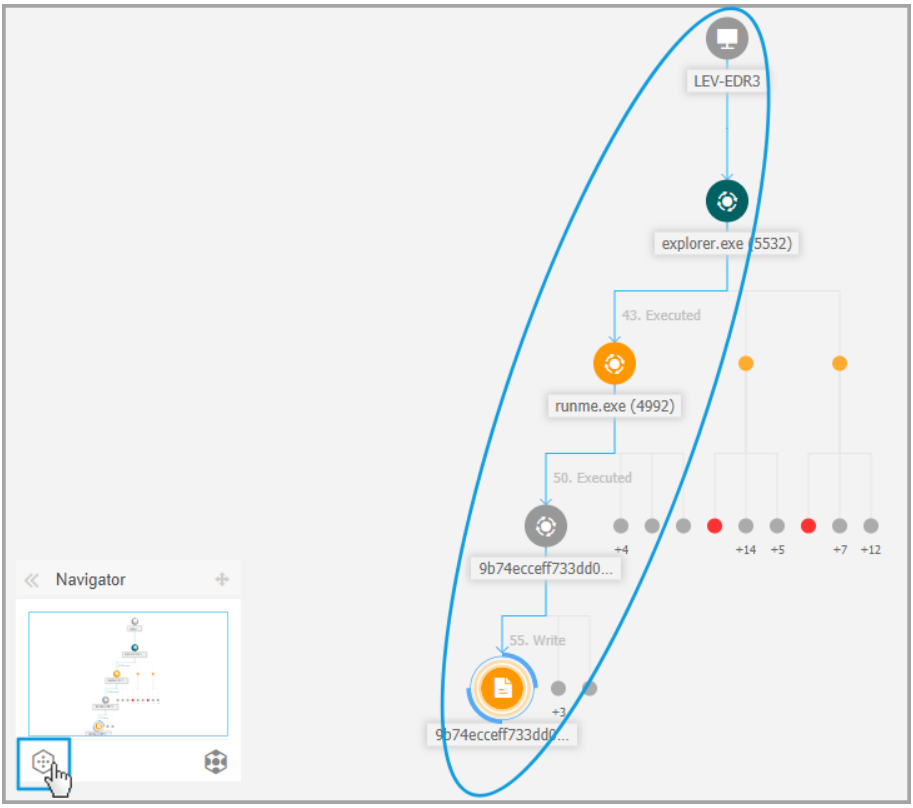
Il **Navigatore** non è selezionato in maniera predefinita. Espandendolo, il menu mostrerà la versione miniaturizzata dell'intera mappa dell'incidente, e i pulsanti azione per regolare il livello di visualizzazione.



Navigatore

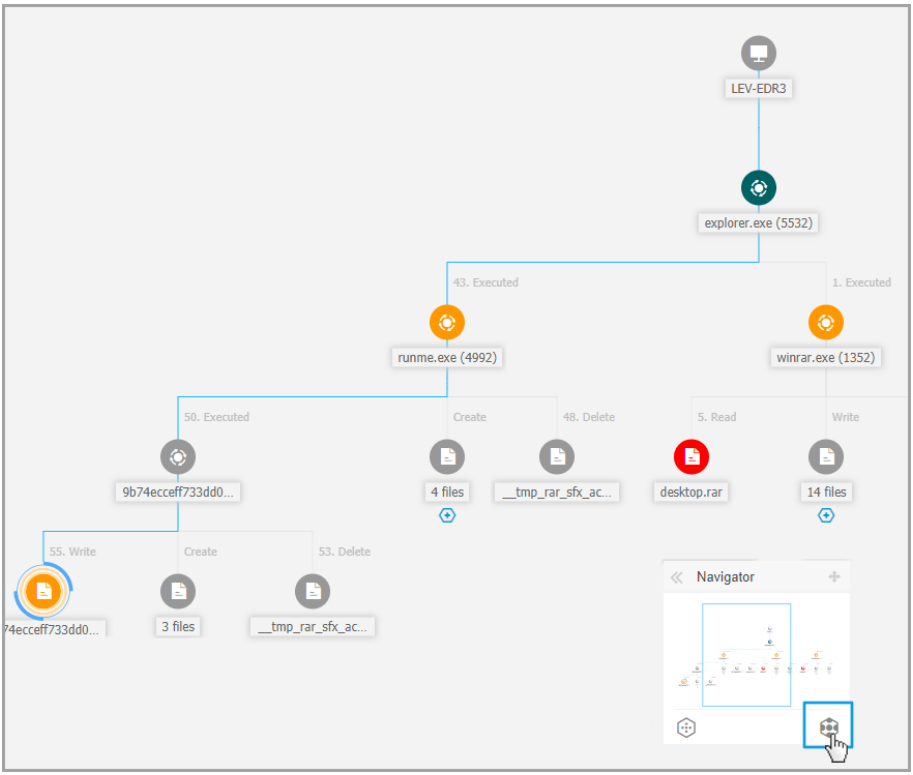
Il menu **Navigatore** fornisce due pulsanti azione per regolare il modo di visualizzare il grafico dell'incidente: il pulsante **Meno dettagli** e il pulsante **Più dettagli**

Cliccando sul pulsante **Meno dettagli**, il grafico viene impostato nel suo stato predefinito, evidenziando solo il percorso critico dell'incidente.



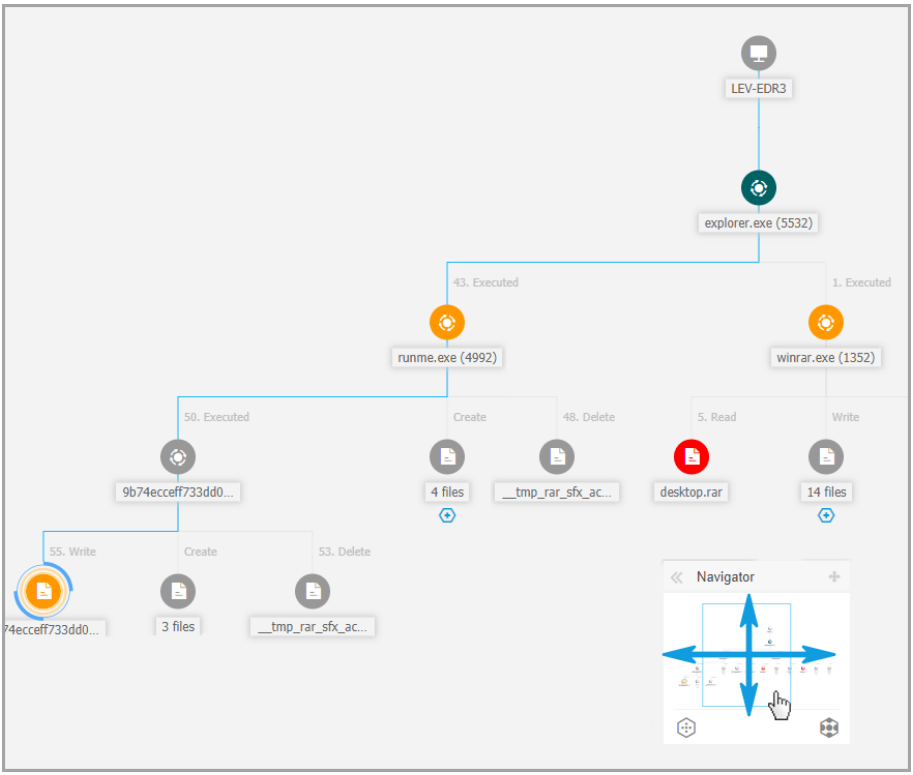
Visualizzazione panoramica

Cliccando sul pulsante **Più dettagli**, tutti gli elementi del grafico dell'incidente vengono espansi, evidenziando ogni nodo e cluster dei nodi.



Visualizzazione ingrandita

Quando l'incidente viene ingrandito e tutti gli elementi vengono evidenziati, il grafico potrebbe spesso espandersi oltre i limiti dello schermo. In questo caso, tieni premuto e trascina il selettore della mappa nella mini-mappa del Navigatore per scorrere facilmente all'area della mappa dell'incidente desiderata, o trascina semplicemente l'area del grafico nella direzione desiderata.

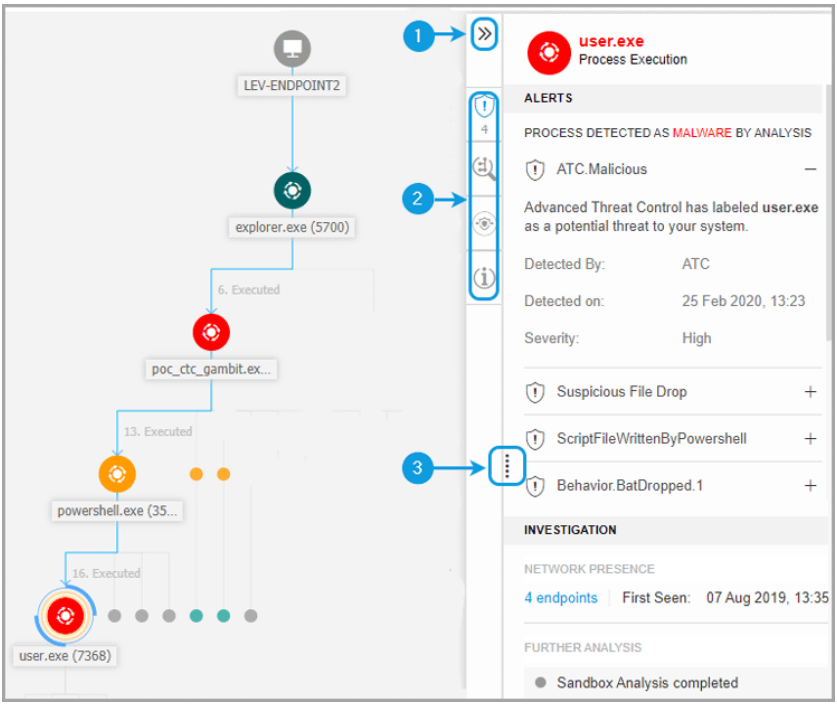


Selettore mini-mappa

Dettagli nodo

Il pannello **Dettagli nodo** include sezioni con informazioni dettagliate sul nodo selezionato, tra cui azioni preventive o di risanamento da poter intraprendere per contenere l'incidente, dettagli sul tipo di rilevamento e le allerte rilevate sul nodo, presenza della rete, dettagli sull'esecuzione dei processi, ulteriori suggerimenti per gestire l'evento di sicurezza, o azioni per esaminare ulteriormente l'elemento.

Per visualizzare queste informazioni e intraprendere azioni all'interno del pannello, seleziona un nodo nella mappa dell'evento di sicurezza.



Pannello dettagli nodo

1. Puoi ridurre o espandere il pannello **Dettagli nodo** cliccando sul pulsante **Comprimi**.
2. Puoi facilmente esplorare le informazioni mostrate nel pannello **Dettagli nodo**, cliccando sulle icone di ciascuna delle quattro categorie principali:
   - **ALLERTE**

     Questa sezione mostra uno o più rilevamenti attivati sul nodo selezionato, incluso dettagli sulla tecnologia di Bitdefender che ha incluso l'elemento nell'incidente, il motivo che ha attivato il rilevamento, il nome del rilevamento, il tipo e la famiglia di malware, e la data del rilevamento.
   - **INDAGINE**

     Questa sezione mostra gli indicatori della data per il rilevamento iniziale e tutti gli endpoint in cui è stato individuato questo elemento.

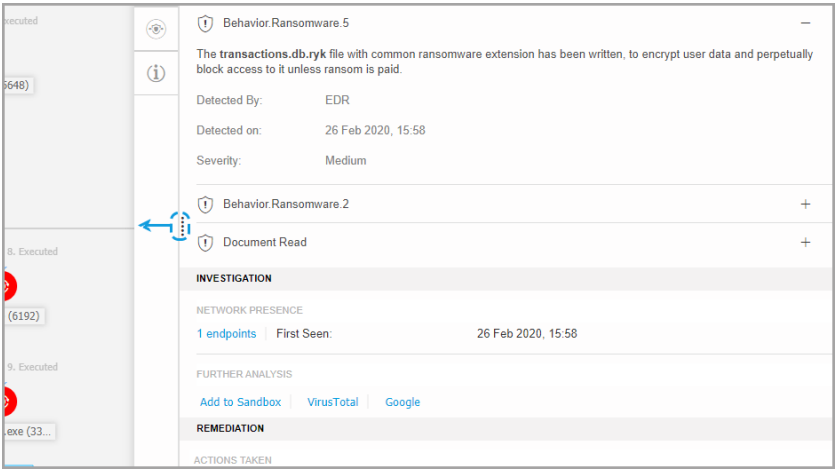
- **RIMEDIO**

  Questa sezione mostra le azioni intraprese automaticamente da GravityZone, azioni che puoi effettuare subito per ridurre l'impatto della minaccia, oltre a suggerimenti dettagliati per ciascuna allerta rilevata nel nodo selezionato per assisterti nella mitigazione dell'incidente e aumentare il livello di sicurezza del tuo ambiente.

- **INFO**

  Questa sezione mostra informazioni generali su ciascun file e informazioni più specifiche in base al tipo di nodo selezionato.

3. Puoi trascinare il pannello **Dettagli nodo** verso il centro della schermata per visualizzarne facilmente i contenuti.



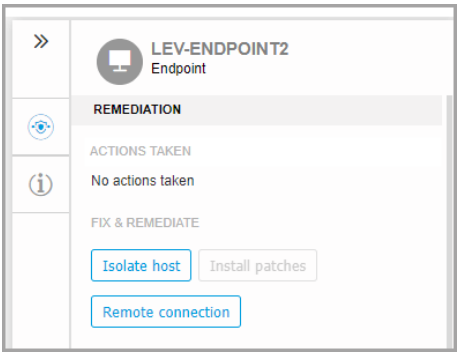
Pannello esteso

Pannello dei dettagli per i nodi dell'endpoint

Il pannello **Dettagli nodo** per gli endpoint include due categorie:

- **RIMEDIO**

  Mostra informazioni sulle azioni intraprese automaticamente da GravityZone per mitigare le minacce, e le azioni che puoi intraprendere:

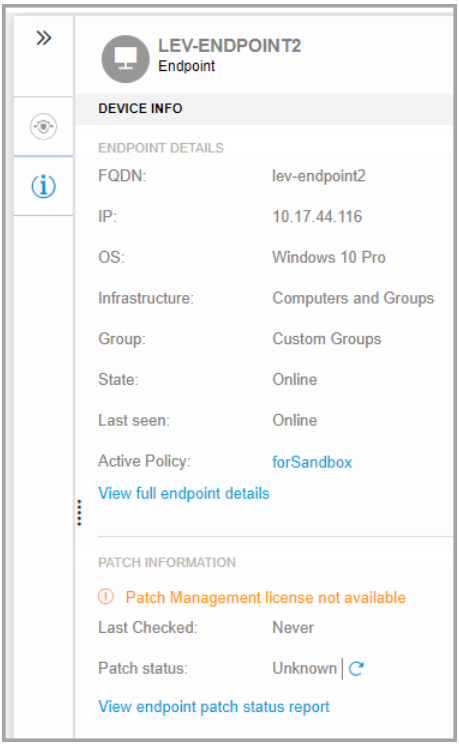


- **Isola host** - Usa questa soluzione di riparazione per isolare l'endpoint dalla rete.
- **Installa patch** - Usa questa azione per installare una patch di sicurezza mancante nell'endpoint bersaglio. Questa opzione risulta disponibile solo con il modulo Gestione patch, un add-on disponibile con un codice di licenza separato. Fai riferimento a Installazione patch per maggiori informazioni.
- **Connessione remota** - Usa questa scheda per stabilire una connessione remota all'endpoint coinvolto nell'incidente attuale ed esegui un numero di comandi shell personali sul suo sistema operativo, per rimediare alla minaccia subito oppure ottenere dati per un'ulteriore indagine.

  Cliccando su questo pulsante mostrerai la finestra Connessione remota.

- **INFORMAZIONI DISPOSITIVO**

  Mostra informazioni generali sull'endpoint interessato, come nome dell'endpoint, indirizzo IP, sistema operativo, gruppo pertinente, stato, policy attive e un link che apre una nuova finestra dove poter visualizzare tutti i dettagli dell'endpoint.



Fornisce anche informazioni come il numero di patch installate, le patch la cui installazione non è riuscita o qualsiasi patch mancante, sia di sicurezza che di diverso tipo. Puoi anche generare un rapporto sullo stato delle patch per negli endpoint. Questa sezione viene fornita su richiesta per l'endpoint bersaglio.

All'interno del pannello puoi eseguire le seguenti azioni:

– Visualizzare informazioni sulle patch per l'endpoint di destinazione Per visualizzare i dettagli della patch, clicca su **Aggiorna** all'interno di questa sezione.

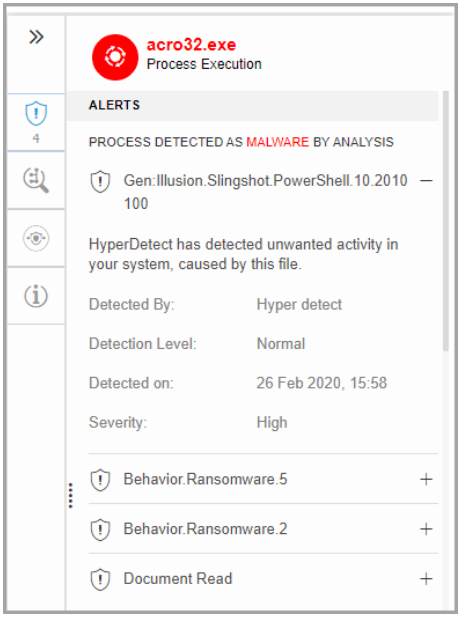
– Visualizzare il rapporto sullo stato delle patch per l'endpoint di destinazione Per generare un rapporto, clicca su **Vedi rapporto stato patch endpoint**.

Pannello dei dettagli per i nodi dei processi

Il pannello **Dettagli nodo** per i nodi dei processi include quattro categorie:

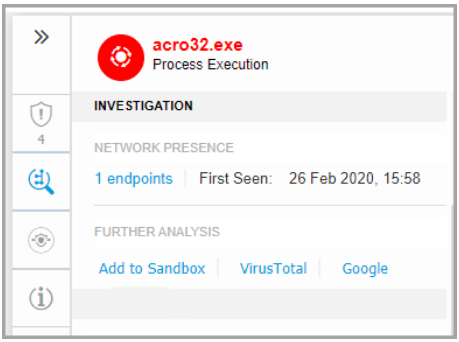
- **ALLERTE**

  Mostra uno o più rilevamenti attivati sul nodo selezionato, incluso dettagli sulla tecnologia di Bitdefender che ha incluso l'elemento nell'incidente, il motivo che ha attivato il rilevamento, il nome del rilevamento, il tipo e la famiglia di malware, e la data del rilevamento. La descrizione per ogni avviso segue gli standard MITRE più recenti.

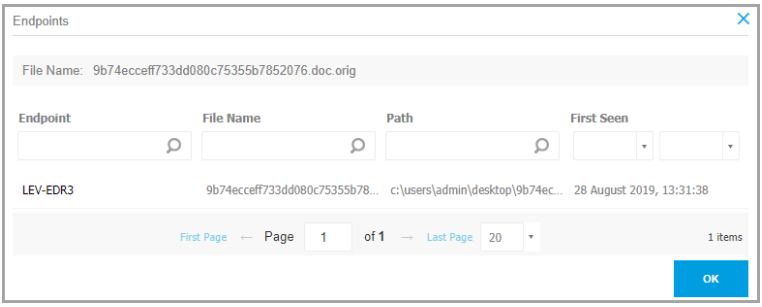


- **INDAGINE**

  Mostra gli indicatori della data per il rilevamento iniziale e tutti gli endpoint in cui è stato individuato questo elemento.



Per visualizzare questo elenco, clicca sul numero mostrato nel campo **endpoint** e comparirà una nuova finestra.

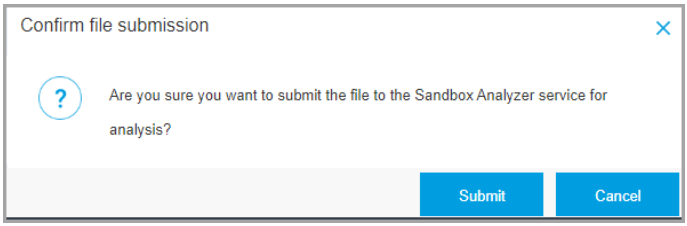


Questa sezione fornisce anche un'analisi esterna, tramite componenti interni e soluzioni di terze parti.

Sono disponibili le seguenti opzioni:

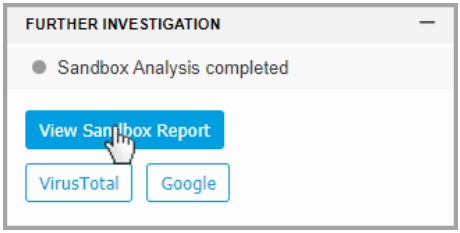
– **Aggiungi a Sandbox** - Usa questa azione per generare un rapporto di Sandbox Analyzer.

  Scegliendo **Aggiungi a Sandbox** ti sarà chiesto di confermare l'invio del file con un'apposita schermata.



Dopo aver confermato, verrai reindirizzato automaticamente alla schermata di invio.

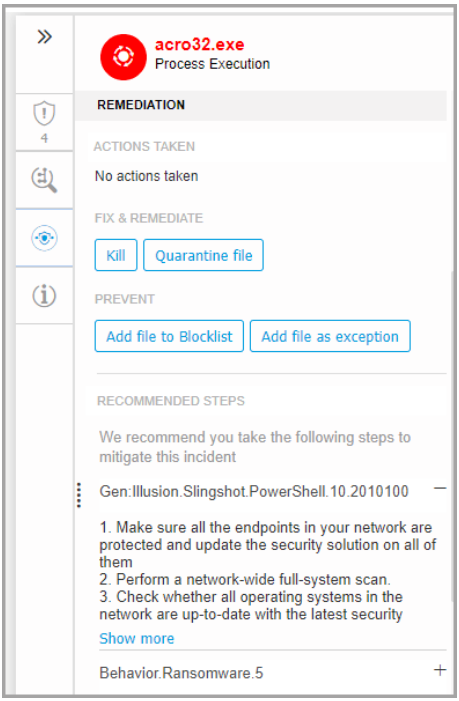
Una volta completata l'analisi, clicca sul pulsante **Vedi rapporto sandbox** per aprire il rapporto completo.



- **VirusTotal** - Usa questa azione per inviare un file esternamente per l'analisi.
- **Google** - Usa questa azione per cercare il valore di hash di un file.

- **RIMEDIO**

  Mostra informazioni sulle azioni intraprese automaticamente da GravityZone per mitigare le minacce, e le azioni che puoi intraprendere:



- **Blocca** - Usa questa azione per bloccare l'esecuzione di un processo. Questa azione crea un'attività di terminazione del processo, visibile nella barra di esecuzione. `Da questa azione sono esclusi i processi system32` e Bitdefender.
- **File di quarantena** - Usa questa azione per archiviare l'elemento in questione e impedirgli di eseguire il suo payload. Questa azione richiede che il modulo Firewall sia stato installato sull'endpoint bersaglio.
- **Aggiungi file a lista elementi bloccati** - Gestisci gli elementi bloccati nella sezione Elementi bloccati.
- **Aggiungi file come eccezione** - Usa questa opzione per escludere attività legittime su una specifica policy. Quando scegli questa azione, si apre una finestra di configurazione in cui ti viene richiesto di selezionare la policy, se

desideri aggiungere un'eccezione. Puoi gestire le eccezioni in **Policy > Antimalware > Impostazioni**.

– **Aggiungi come eccezione EDR** - Usa questa opzione per creare una regola personale che non considererà più il processo come un rilevamento EDR sospetto o dannoso.

1. Cliccando sul pulsante **Aggiungi come eccezione EDR**, comparirà una nuova finestra che ti chiederà di confermare l'azione o annullarla.
2. Dopo aver confermato l'azione, GravityZone ti avviso che la nuova regola è disponibile nella griglia Regole delle eccezioni. Nota che il nome di tutte le regole create all'interno del grafico dell'incidente iniziano con il numero dell'incidente.

Nota
Quando accedi ai dettagli della regola per modificarla, noterai che tutti i criteri per tale regola sono stati inseriti automaticamente, ed è stato aggiunto un criterio di sola lettura con il nome dell'avviso.

Importante
La funzionalità **Aggiungi come eccezione EDR** è disponibile solo per:

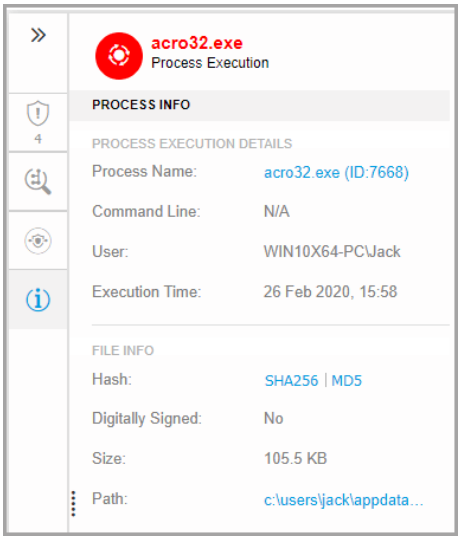
- allerte attivate dalla tecnologia EDR
- nodi generati da un altro processo
- nodi sospetti e dannosi

Se il processo escluso fa parte del percorso critico dell'incidente, allora gli incidenti futuri che corrispondono a questo criterio di eccezione non verranno più generati nella griglia Incidenti. Tali eventi saranno ancora disponibili per la visualizzazione e l'analisi nella pagina Ricerca.
Se il processo escluso non fa parte del percorso critico dell'incidente, allora gli incidenti futuri che corrispondono a questo criterio di eccezione non verranno più generati nella griglia Incidenti, ma non considereranno più tale processo come sospetto o dannoso.

Questa sezione fornisce anche suggerimenti dettagliati per ciascuna allerta rilevata nel nodo selezionato per assisterti nella mitigazione dell'incidente e aumentare il livello di sicurezza del tuo ambiente.

- **INFORMAZIONI SUL PROCESSO**

Mostra dettagli sul nodo del processo selezionato, tra cui il nome del processo, la linea di comando eseguita, l'utente, il momento dell'esecuzione, l'origine e il percorso del file, il valore dell'hash o la firma digitale.



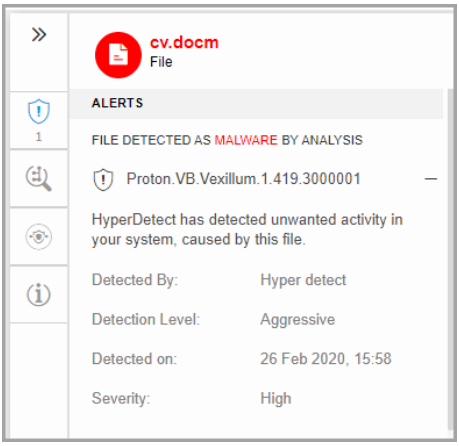
Puoi copiare il valore dell'hash negli appunti cliccando sugli algoritmi di hash disponibili nel campo **Hash** e poi seleziona **Copia negli appunti** per usarlo per aggiungere un valore dell'hash dei file alla **Lista bloccati**. Per maggiori informazioni, fai riferimento a **Inserire file nella lista bloccati**.

Pannello dei dettagli per i nodi dei file

Il pannello **Dettagli del nodo** per i nodi dei file include quattro categorie:

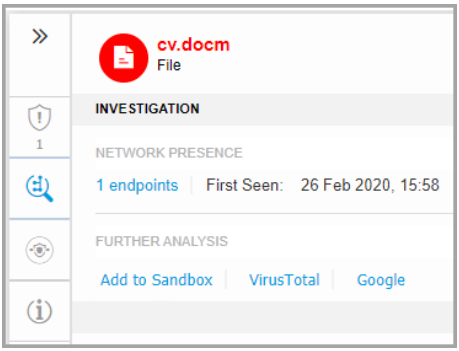
- **ALLERTE**

  Mostra uno o più rilevamenti attivati sul nodo selezionato, incluso dettagli sulla tecnologia di Bitdefender che ha incluso l'elemento nell'incidente, il motivo che ha attivato il rilevamento, il nome del rilevamento, il tipo e la famiglia di malware, e la data del rilevamento. La descrizione per ogni avviso segue gli standard MITRE più recenti.

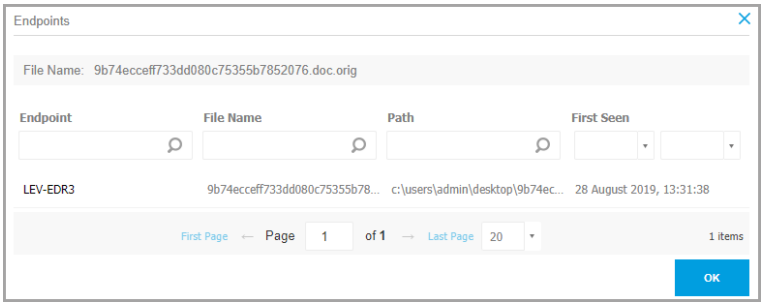


- **INDAGINE**

  Mostra gli indicatori della data per il rilevamento iniziale e tutti gli endpoint in cui è stato individuato questo elemento.



  Per visualizzare questo elenco, clicca sul numero mostrato nel campo **endpoint** e comparirà una nuova finestra.

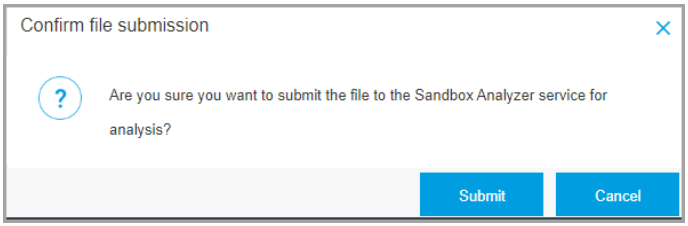


Questa sezione fornisce anche un'analisi esterna, tramite componenti interni e soluzioni di terze parti.

Sono disponibili le seguenti opzioni:

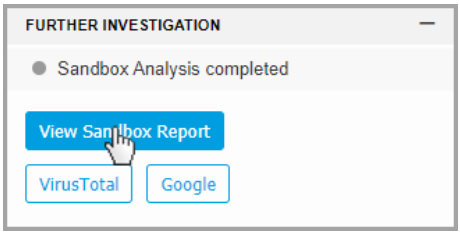
– **Aggiungi a Sandbox** - Usa questa azione per generare un rapporto di Sandbox Analyzer.

  Scegliendo **Aggiungi a Sandbox** ti sarà chiesto di confermare l'invio del file con un'apposita schermata.



  Dopo aver confermato, verrai reindirizzato automaticamente alla schermata di invio.

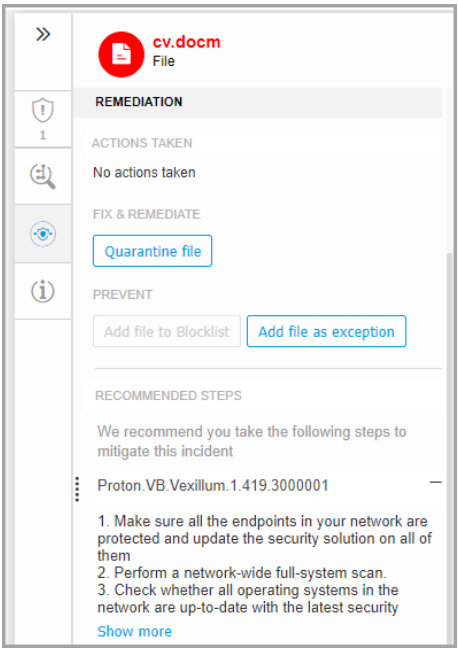
  Una volta completata l'analisi, clicca sul pulsante **Vedi rapporto sandbox** per aprire il rapporto completo.



  - **VirusTotal** - Usa questa azione per inviare un file esternamente per l'analisi.
  - **Google** - Usa questa azione per cercare il valore di hash di un file.

- **RIMEDIO**

  Mostra informazioni sulle azioni intraprese automaticamente da GravityZone per mitigare le minacce, e le azioni che puoi intraprendere:



- **File di quarantena** - Usa questa azione per archiviare l'elemento in questione e impedirgli di eseguire il suo payload. Questa azione richiede che il modulo Firewall sia stato installato sull'endpoint bersaglio.
- **Aggiungi file a lista elementi bloccati** - Gestisci gli elementi bloccati nella sezione Elementi bloccati.
- **Aggiungi file come eccezione** - Usa questa opzione per escludere attività legittime su una specifica policy. Quando scegli questa azione, si apre una finestra di configurazione in cui ti viene richiesto di selezionare la policy, se desideri aggiungere un'eccezione. Puoi gestire le eccezioni in **Policy > Antimalware > Impostazioni**.
- **Aggiungi come eccezione EDR** - Usa questa opzione per creare una regola personale che non considererà più il file come un rilevamento EDR sospetto o dannoso.

  1. Cliccando sul pulsante **Aggiungi come eccezione EDR**, comparirà una nuova finestra che ti chiederà di confermare l'azione o annullarla.

2. Dopo aver confermato l'azione, GravityZone ti avviso che la nuova regola è disponibile nella griglia Regole delle eccezioni. Nota che il nome di tutte le regole create all'interno del grafico dell'incidente iniziano con il numero dell'incidente.

Nota
Quando accedi ai dettagli della regola per modificarla, noterai che tutti i criteri per tale regola sono stati inseriti automaticamente, ed è stato aggiunto un criterio di sola lettura con il nome dell'avviso.

Importante
La funzionalità **Aggiungi come eccezione EDR** è disponibile solo per:

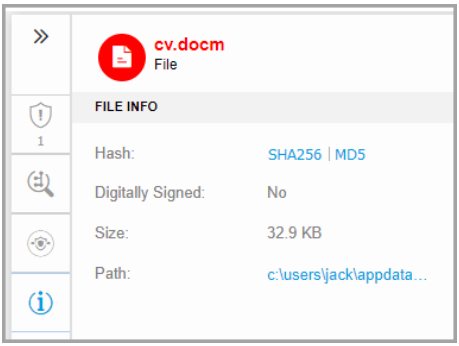
- allerte attivate dalla tecnologia EDR
- nodi generati da un altro processo
- nodi sospetti e dannosi

Se il file escluso fa parte del percorso critico dell'incidente, allora gli incidenti futuri che corrispondono a questo criterio di eccezione non verranno più generati nella griglia Incidenti. Tali eventi saranno ancora disponibili per la visualizzazione e l'analisi nella pagina Ricerca.
Se il file escluso non fa parte del percorso critico dell'incidente, allora gli incidenti futuri che corrispondono a questo criterio di eccezione non verranno più generati nella griglia Incidenti, ma non considereranno più tale processo come sospetto o dannoso.

Questa sezione fornisce anche suggerimenti dettagliati per ciascuna allerta rilevata nel nodo selezionato per assisterti nella mitigazione dell'incidente e aumentare il livello di sicurezza del tuo ambiente.

- **INFO FILE**

  Mostra dettagli sul nodo dei file selezionato, incluso l'origine e il percorso del file, il valore dell'hash o la firma digitale.



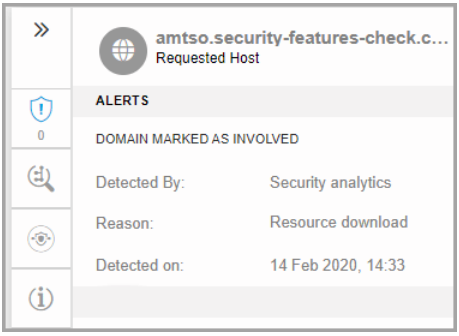
Puoi copiare il valore dell'hash negli appunti cliccando sugli algoritmi di hash disponibili nel campo **Hash** e poi seleziona **Copia negli appunti** per usarlo per aggiungere un valore dell'hash dei file alla **Lista bloccati**. Per maggiori informazioni, fai riferimento a **Inserire file nella lista bloccati**.

Pannello dei dettagli per i nodi dei domini

Il pannello **Dettagli del nodo** per i nodi dei domini include quattro categorie:

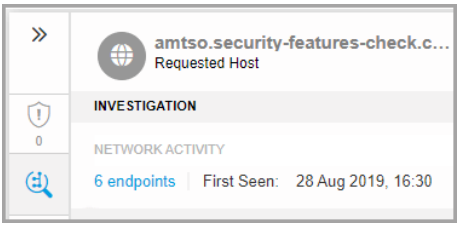
- **ALLERTE**

  Mostra la severità del dominio come indicata dalla tecnologia di Bitdefender che ha incluso tale entità nell'incidente, il motivo che ha attivato il rilevamento e la data in cui è stato rilevato.

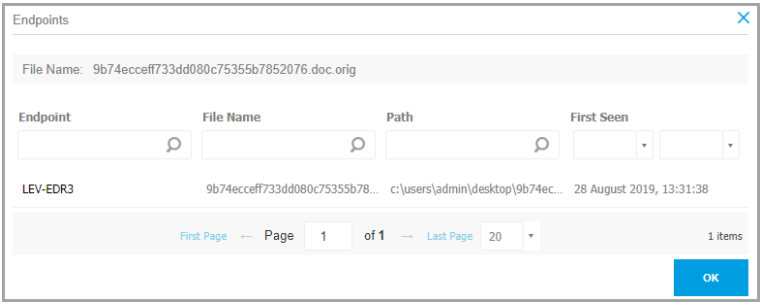


- **INDAGINE**

Mostra gli indicatori della data per il rilevamento iniziale e tutti gli endpoint in cui è stato individuato questo elemento.

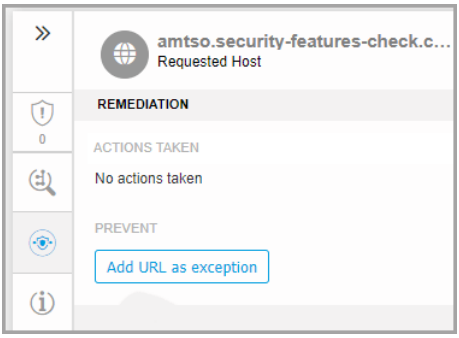


Per visualizzare questo elenco, clicca sul numero mostrato nel campo **endpoint** e comparirà una nuova finestra.



- **RIMEDIO**

  Mostra informazioni sulle azioni intraprese automaticamente da GravityZone per mitigare le minacce, e le azioni che puoi intraprendere:



- **Aggiungi URL come eccezione** - Usa questa opzione per escludere attività legittime su una specifica policy. Quando scegli questa azione, si apre una finestra di configurazione in cui ti viene richiesto di selezionare la policy, se desideri aggiungere un'eccezione. Puoi gestire le eccezioni in **Policy > Antimalware > Impostazioni**.
- **Aggiungi come eccezione EDR** - Usa questa opzione per creare una regola personale che non considererà più il dominio come un rilevamento EDR sospetto o dannoso.

  1. Cliccando sul pulsante **Aggiungi come eccezione EDR**, comparirà una nuova finestra che ti chiederà di confermare l'azione o annullarla.
  2. Dopo aver confermato l'azione, GravityZone ti avviso che la nuova regola è disponibile nella griglia Regole delle eccezioni. Nota che il nome di tutte le regole create all'interno del grafico dell'incidente iniziano con il numero dell'incidente.

  Nota
  Quando accedi ai dettagli della regola per modificarla, noterai che tutti i criteri per tale regola sono stati inseriti automaticamente, ed è stato aggiunto un criterio di sola lettura con il nome dell'avviso.

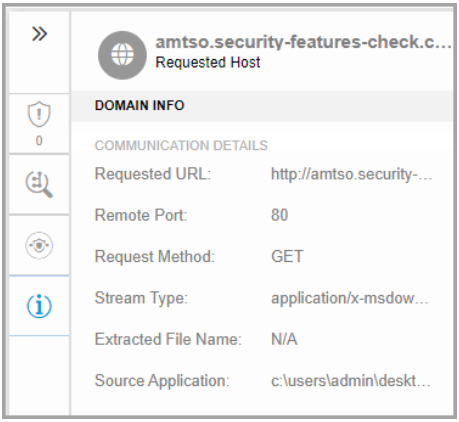
  Importante
  La funzionalità **Aggiungi come eccezione EDR** è disponibile solo per:

  - allerte attivate dalla tecnologia EDR
  - nodi generati da un altro processo
  - nodi sospetti e dannosi

Se il dominio escluso fa parte del percorso critico dell'incidente, allora gli incidenti futuri che corrispondono a questo criterio di eccezione non verranno più generati nella griglia Incidenti. Tali eventi saranno ancora disponibili per la visualizzazione e l'analisi nella pagina Ricerca.
Se il dominio escluso non fa parte del percorso critico dell'incidente, allora gli incidenti futuri che corrispondono a questo criterio di eccezione non verranno più generati nella griglia Incidenti, ma non considereranno più tale processo come sospetto o dannoso.

- **INFORMAZIONI DEL DOMINIO**

  Mostra dettagli sul nodo dei domini selezionato, incluso l'URL richiesto, la porta usata, il metodo della richiesta, il tipo di stream, il nome del file estratto e l'applicazione di origine.

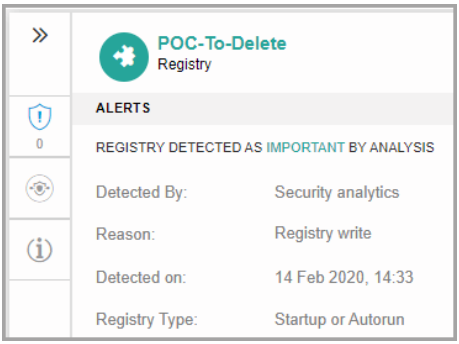


Pannello dei dettagli per i nodi del registro

Il pannello **Dettagli del nodo** per i nodi del registro include tre categorie:

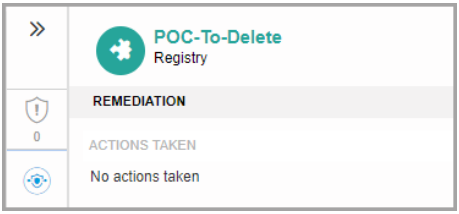
- **ALLERTE**

  Mostra la severità della manipolazione del registro come indicata dalla tecnologia di Bitdefender che ha incluso tale entità nell'incidente, il motivo che ha attivato il rilevamento, la data in cui è stato rilevato e il tipo di registro.



- **RIMEDIO**

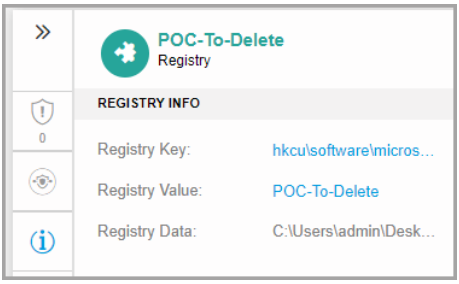
  Mostra informazioni sulle azioni intraprese automaticamente da GravityZone.



  La sezione **RIMEDIO** per i nodi del registro non fornisce alcuna opzione di azione diretta.

- **INFORMAZIONI DEL REGISTRO**

  Mostra dettagli sul nodo del registro selezionato, tra cui la chiave del registro, il valore e i dati.

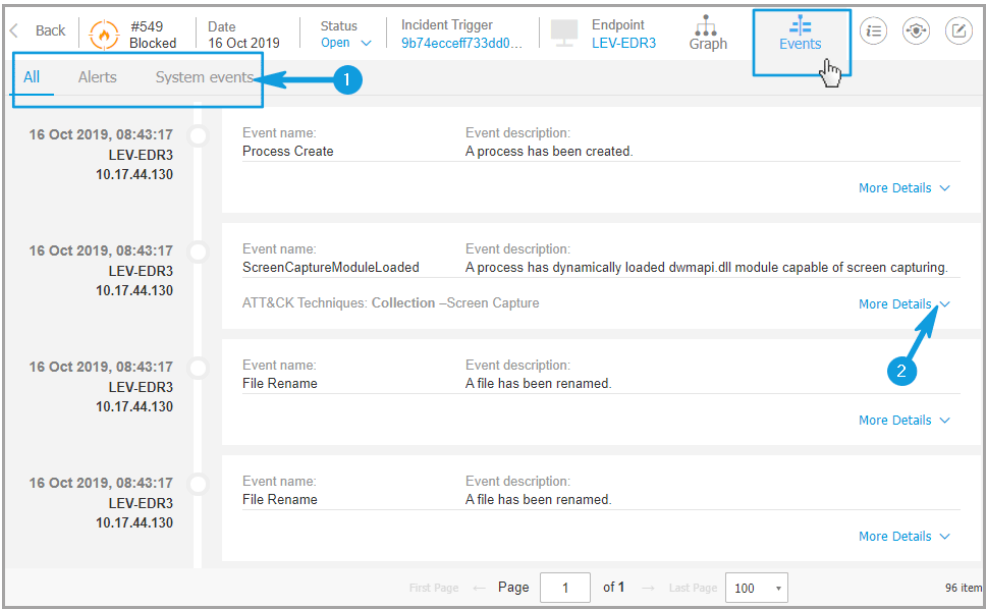


Puoi cliccare sulla chiave del registro e sul valore per copiarla per ulteriori analisi.

Eventi

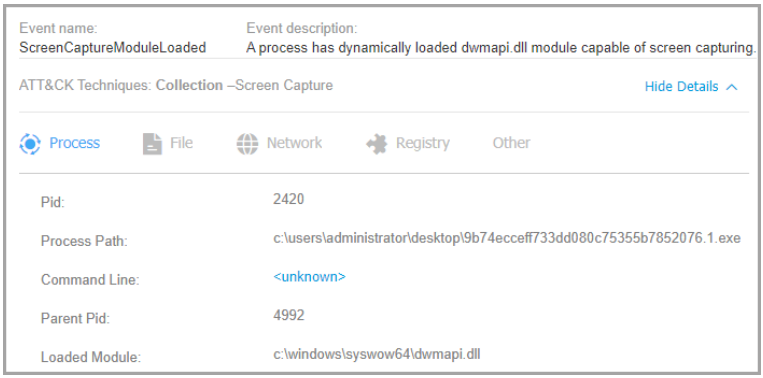
Usa la scheda **Eventi** per visualizzare come si è svolta la sequenza di eventi per innescare l'incidente attualmente indagato. Questa finestra mostra gli avvisi e gli eventi del sistema correlati e rilevati dalle tecnologie di GravityZone, come EDR, Network Attack Defense, Anomaly Detection, Advanced Anti-Exploit e Windows Antimalware Scan Interface (AMSI).

Ogni evento complesso ha una descrizione dettagliata che spiega come è stato rilevato e cosa potrebbe accadere se l'elemento venisse usato per scopi dannosi, in base alle più recenti tecniche e tattiche MITRE.



Scheda Eventi

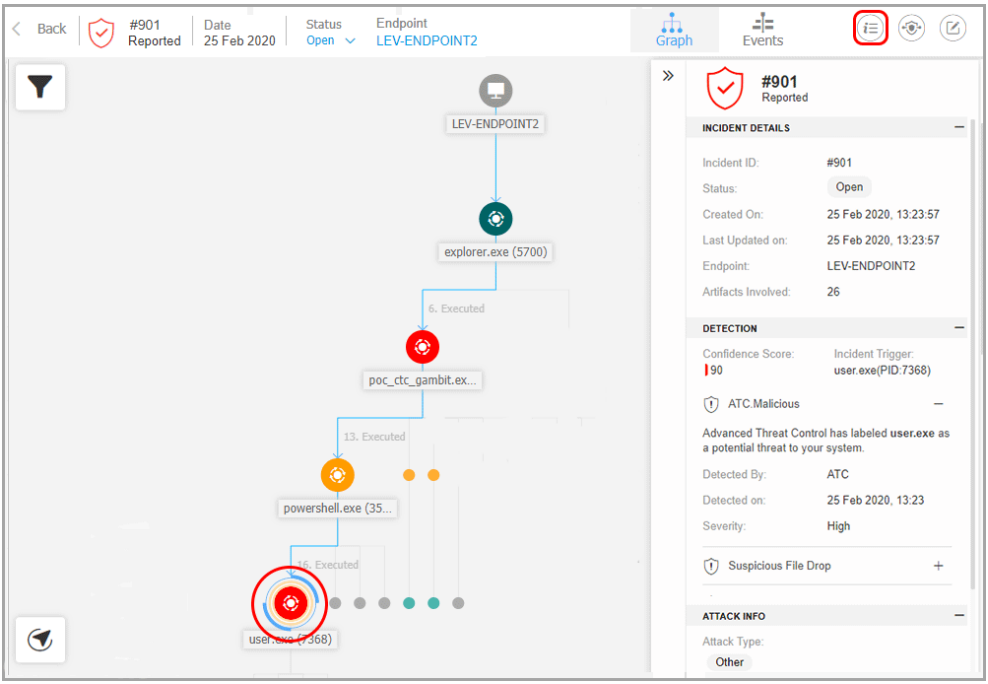
1. Usa le opzioni di filtro per mostrare tutti gli eventi o solo gli eventi del sistema o quelli complessi (avvisi).
2. Clicca sul pulsante **Altri dettagli** per espandere ciascun evento e accedere a informazioni aggiuntive.



Informazioni incidente

Questo pannello include sezioni comprimibili con dettagli come ID incidente, stato attuale, data e ora di creazione e ultimo aggiornamento, numero di elementi coinvolti, nome e descrizione del trigger, e informazioni sull'attacco.

Da questa sezione è possibile accedere all'incidente esteso che include questo incidente dell'endpoint, se il caso.

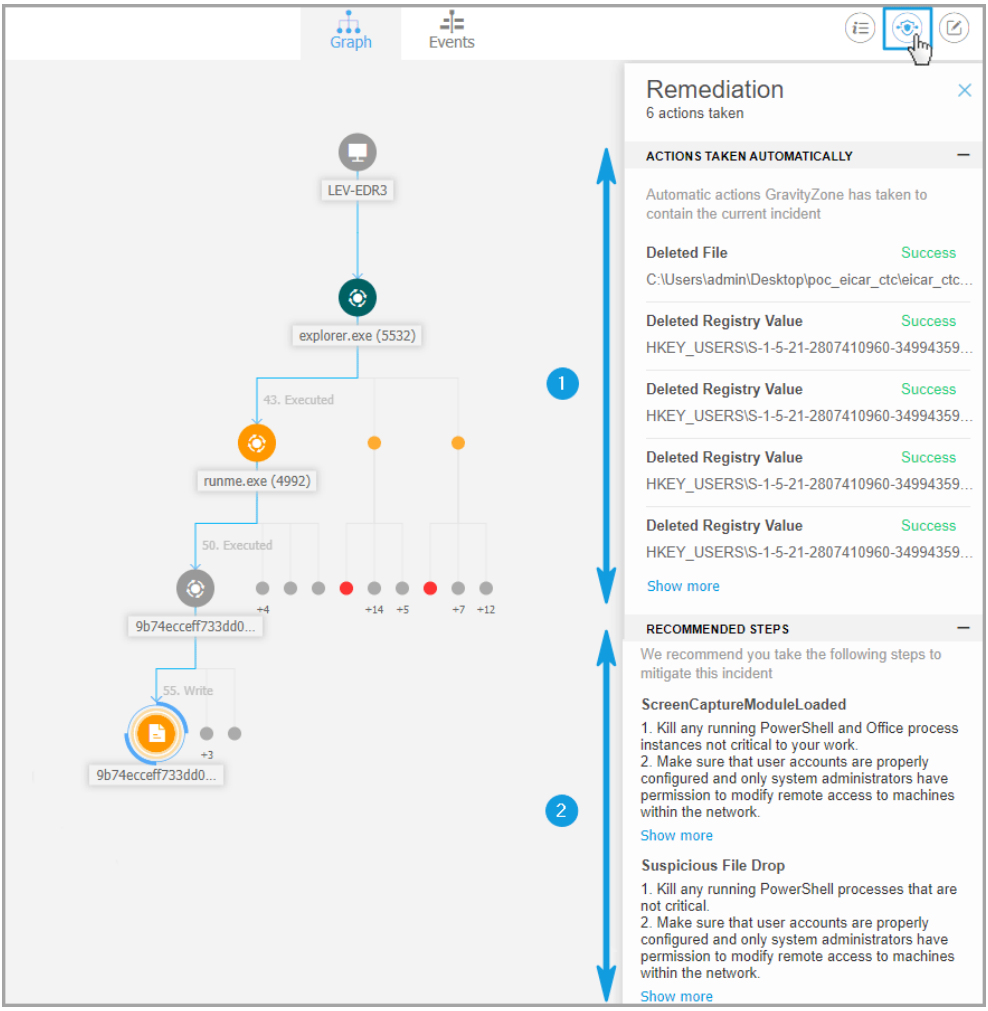


Pannello Informazioni incidente

Il pannello include anche gli avvisi rilevati sull'elemento che hanno innescato l'incidente.

Rimedio

Il pannello **Risanamento** fornisce informazioni complete sulle azioni correttive che sono state intraprese automaticamente da GravityZone in caso di attacchi bloccati da tecnologie come Advanced Threat Control (ATC), HyperDetect e Antimalware, oltre ai passaggi suggeriti da intraprendere per contenere l'incidente e aumentare il livello di sicurezza del proprio sistema.



Pannello riparazione

1. Azioni intraprese automaticamente da GravityZone.
2. Suggerimenti per contenere ulteriormente l'incidente e incrementare la sicurezza.

Nota
I passaggi suggeriti corrispondono agli avvisi rilevati sul nodo che ha innescato l'incidente indagato.

Note

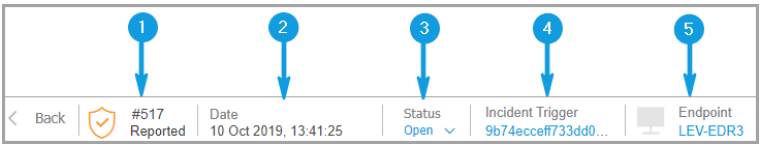
La sezione **Note** ti consente di aggiungere una nota per tenere traccia dei recenti cambiamenti e facilitare la modifica della proprietà dell'incidente.

Note negli appunti

1. Per lasciare una nota per l'evento attuale, clicca sul pulsante **Note** per mostrare una nuova finestra.
2. Inserisci il tuo messaggio in questa finestra (massimo 2.048 caratteri).

Barra stato incidente

La barra di stato dell'incidente fornisce tag dell'evento di sicurezza che possono aiutarti a rilevare informazioni chiave sugli endpoint di rete coinvolti.



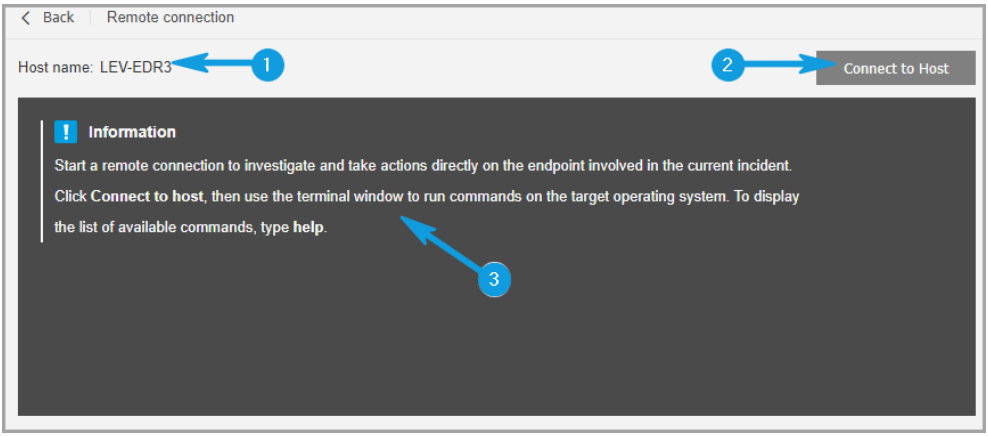
Barra stato incidente

1. ID incidente - il numero di identificazione dell'incidente sotto indagine e se l'incidente è stato bloccato o solo segnalato.
2. Intervallo temporale rilevamento - la data e l'ora in cui l'incidente è stato innescato.
3. Stato dell'incidente - lo stato attuale dell'incidente.
4. Trigger incidente - il nome dell'elemento che ha generato l'incidente.
5. Endpoint - il nome dell'endpoint bersaglio.

Cliccando sul pulsante **Indietro** tornerai alla pagina principale **Incidenti**.

Connessione remota

Usa questa scheda per stabilire una connessione remota all'endpoint coinvolto nell'incidente attuale ed esegui un numero di comandi shell personali sul suo sistema operativo, per annullare la minaccia subito oppure ottenere dati per un'ulteriore indagine.



Scheda Connessione remota

La scheda **Connessione remota** include i seguenti elementi:

1. Il nome dell'endpoint coinvolto nell'evento di sicurezza attuale
2. Il pulsante che controlla la connessione remota (connetti / disconnetti)
3. La finestra del terminale

Prerequisiti della sessione del terminale

- La versione dell'agente di Bitdefender installata sull'endpoint supporta la funzionalità Connessione remota.
- L'endpoint deve essere alimentato ed essere online.
- L'endpoint deve avere un sistema operativo Windows.
- GravityZone è in grado di comunicare con l'endpoint.
- Il tuo account di GravityZone deve avere i permessi di gestione per l'endpoint bersaglio.

Creare una Connessione remota

Ecco come funziona la connessione remota:

1. Avvia la sessione live cliccando sul pulsante **Connetti a host**.

   Lo stato della connessione sarà mostrato accanto al nome dell'endpoint.

   Se la connessione fallisse, nella finestra del terminale sarà mostrato un messaggio di errore.

   > **Nota**
   > Puoi aprire un massimo di cinque sessioni del terminale contemporaneamente con lo stesso endpoint.

2. Una volta connesso, il terminale mostra l'elenco dei comandi disponibili e la loro descrizione. Digita il comando desiderato nella finestra del terminale seguito da `Invio`.

   Per più informazioni su un comando, digita `help` seguito dal nome del comando (per esempio, `help ps`).

3. Il terminale mostra l'output del comando, quando il comando ha successo.

   Se l'endpoint non riesce a completare l'esecuzione del comando, il comando sarà scartato.

   La cronologia dei comandi viene registrata nella finestra del terminale. Tuttavia, puoi visualizzare i comandi digitati in precedenza premendo i tasti freccia.

4. Per terminare la connessione, clicca sul pulsante **Termina sessione**.

   La sessione del terminale scade automaticamente dopo cinque minuti di inattività.

   Anche navigando oltre la scheda **Connessione remota** mentre si è connessi a un endpoint terminerà la sessione del terminale.

Comandi sessione terminale

I comandi della sessione del terminale EDR sono comandi shell personalizzati, indipendenti dalla piattaforma e che usano una sintassi generica. Qui di seguito puoi trovare l'elenco dei comandi disponibili che puoi usare sugli endpoint tramite la sessione del terminale:

- `ps`

- **Descrizione**: mostra informazioni sui processi attualmente in esecuzione sull'endpoint bersaglio, come ID del processo (PID), nome, percorso o utilizzo della memoria.
- **Sintassi**: `ps`
- **Alias**: `tasklist`
- **Parametri**: -

- `kill`
  - **Descrizione**: Termina un processo o un'applicazione in esecuzione sull'endpoint bersaglio tramite il proprio PID. Usa il comando `ps/tasklist`per ottenere il PID.
  - **Sintassi**: `kill [PID]`
  - **Alias**: -
  - **Parametri**: `[PID]` - l'ID del processo dall'endpoint bersaglio.
- `ls (dir)`
  - **Descrizione**: Mostra informazioni su tutti i file e le cartelle della cartella specificata, come nome, tipo, dimensione e data di modifica. Consente i caratteri jolly per indicare il percorso. Per esempio:

    `C:\Users\admin\Desktop\s*` tutti i contenuti della cartella Desktop che iniziano con "s"

    `C:\Users\publ??` elenca tutti i contenuti del percorso specificato con una qualsiasi delle ultime due lettere.
  - **Sintassi**: `ls [path]`
  - **Alias**: `dir`
  - **Parametri**: `[Path]` - il percorso a un file o una cartella sull'endpoint bersaglio.
- `rm (del, delete)`
  - **Descrizione**: Elimina file o cartelle dal percorso specificato sull'endpoint bersaglio.
  - **Sintassi**: `rm [path]`
  - **Alias**: `del/delete`

- **Parametri**: `[Path]` - il percorso a un file o una cartella sull'endpoint bersaglio.

- `reg query`
  - **Descrizione**: Offre tutte le informazioni (nome, tipo e valore) per il percorso della chiave del registro specificato.
  - **Sintassi**: `reg query [keypath] [/k] [keyname] [/v] [valuename]`
  - **Alias**: -
  - **Parametri**:
    - `keypath`- riporta tutte le informazioni sulle chiave del registro del percorso specificato.
    - `/k [keyname]` - filtra i risultati delle chiavi del registro tramite il nome di una determinata chiave. Puoi anche usare caratteri jolly (*, ?) per filtrare una gamma più ampia di nomi.
    - `/v [valuename]` - filtra i valori del registro tramite un determinato nome del valore. Puoi anche usare caratteri jolly (*, ?) nel nome del valore per filtrare una gamma più ampia di nomi.
- `reg add`
  - **Descrizione**: Aggiunge un nuovo valore o chiave del registro. Sovrascrive un valore del registro, nel caso esistesse già. Nel sovrascrivere informazioni del registro, devi indicare tutti i parametri definiti.
  - **Sintassi**: `reg add [keyname] [/v] [valuename] [/t] [datatype] [/d] [data]`
  - **Alias**: -
  - **Parametri**:
    - `[keyname]` - il nome della chiave di registro.
    - `/v [valuename]` - il nome del valore del registro. Richiede almeno di aggiungere il parametro /d [data].
    - `/t [datatype]` - il tipo di dati del valore del registro. Puoi aggiungere uno dei seguenti tipi di dati:

`REG_SZ`, `REG_MULTI_SZ`, `REG_DWORD`, `REG_BINARY`, `REG_DWORD_LITTLE_ENDIAN`, `REG_LINK`, `REG_FULL_RESOURCE_DESCRIPTOR`, `REG_EXPAND_SZ`

Se non specificato, il tipo `REG_SZ` viene assegnato in modo predefinito.

Una volta impostato il tipo in `REG_BYNARY`, i dati del registro vengono interpretati come valori esadecimali.

- `reg delete`
  - **Descrizione**: elimina una chiave del registro o i suoi valori.
  - **Sintassi**:

    ```
    reg delete [keyname] [/v] [valuename]
    ```

    ```
    reg delete [keyname] [/va]
    ```
  - **Alias**: -
  - **Parametri**:

    `[keyname]` - elimina la chiave del registro e di tutti i suoi valori.

    `/v [valuename]` - elimina il valore del registro specificato.

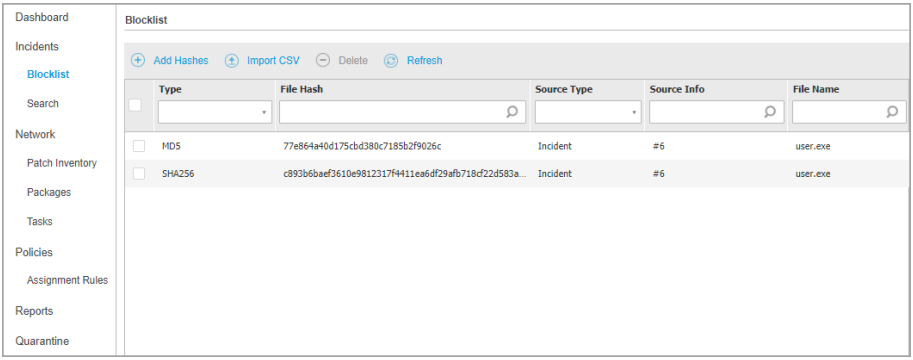
    `/va` - elimina tutti i valori della chiave del registro specificato.
- `cd`
  - **Descrizione**: Modifica la cartella di lavoro nel percorso specificato. Questo comando richiede, come parametro, il percorso di un'unità o una cartella dell'endpoint bersaglio.
  - **Sintassi**: `cd [path]`
  - **Alias**: -
  - **Parametri**: `[Path]` - il percorso a un file o una cartella sull'endpoint bersaglio.
- `aiuto`
  - **Descrizione**: Senza specificare un parametro, aiuta a elencare tutti i comandi disponibili con una breve descrizione. Quando si inserisce help seguito da un parametro, viene visualizzata la sintassi completa di tale comando, una breve descrizione e un esempio di utilizzo.

- **Sintassi**: `help [command]`
- **Alias**: -
- **Parametri**: command name (per esempio: `cd, kill, ls, ps`)

- `clear (cls)`
  - **Descrizione**: Libera la finestra del terminale e mostra il prompt con la cartella di lavoro attuale.
  - **Sintassi**: `clear`
  - **Alias**: `cls`
  - **Parametri**: -

6.2. Inserire file nella lista bloccati

Nella pagina **Lista bloccati**, puoi visualizzare e gestire gli elementi tramite i valori dei propri hash. Vedi le registrazioni delle attività nel Rapporto attività utente.



Pagina Lista bloccati

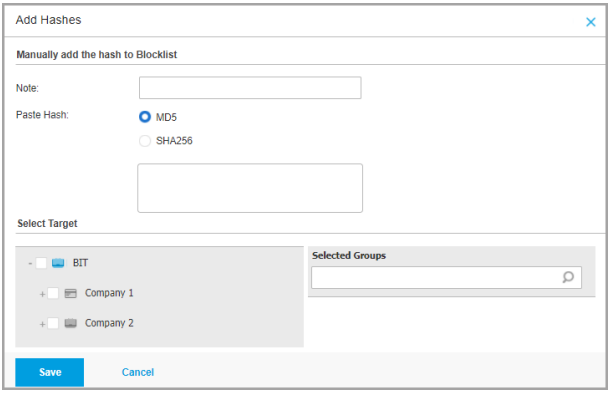
In una tabella di dati, puoi visualizzare i seguenti dettagli per ciascun elemento:

- Tipo di file:
  - MD5
  - SHA256
- Valore hash file

- Tipo di risorsa:
  - Incidente
  - Importa
  - Manuale
- Info sorgente
- Nome File
- Azienda

Aggiungi i valori hash alla Lista bloccati esistente:

1. Copia il valore dell'hash da **Informazioni file**.
2. Scegli da **MD5** o **SHA256** e copia il valore nello spazio sottostante.
   Se necessario, aggiungi una nota.
3. Clicca su **Salva**.



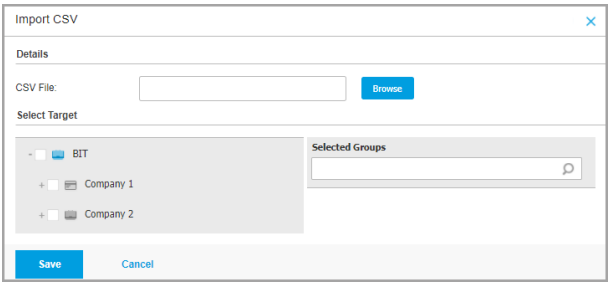
Aggiungere una finestra del valore hash

Importante
Il **Sensore incidenti** bloccherà ogni file binario il cui valore di hash è stato aggiunto alla **Lista bloccati** dall'avvio di un processo.

Importa i valori di hash nella Lista bloccati esistente. Per importare un file CSV:

1. Clicca su **Importa CSV**.

2. Cerca il tuo file CSV e clicca su **Salva**.



Finestra Importa CSV

Puoi anche importare file CSV locali dal tuo dispositivo nella pagina **Lista bloccati**, ma prima assicurati che il tuo file CSV sia valido.

Per creare un file CSV valido per l'importazione, devi prima inserire nelle tre colonne i seguenti dati:

1. La prima colonna del file CSV deve contenere il tipo di hash: `md5` o `sha256`.
2. La seconda colonna deve contenere i valori esadecimali dell'hash corrispondenti.
3. La terza colonna può contenere informazioni opzionali relative alla colonna **Informazioni sorgente** nella pagina **Lista bloccati**.

Nota
Le informazioni corrispondenti alle altre colonne nella pagina **Lista bloccati** saranno compilate automaticamente dopo l'importazione del file CSV.

6.3. Cercare gli eventi di sicurezza

Dalla pagina **Cerca** puoi passare in rassegna gli eventi passati in base a criteri complessi.

Panoramica pagina di ricerca

Per visualizzare gli eventi che ti interessano, devi creare delle query usando il linguaggio query disponibile in GravityZone.

Nella pagina **Cerca** sono disponibili le seguenti opzioni:

- Una barra di ricerca per l'inserimento di query, che puoi cliccare per visualizzare l'elenco dei termini delle query suddivisi per categoria, con una funzionalità di completamento automatico.
- Il salvataggio delle ricerche preferite, da usare in futuro.
-
- Una sezione **Inizia**, con un link alla guida per la sintassi del linguaggio delle query.
- Query predefinite, progettate per casi utili di ricerca di eventi di sicurezza.

6.3.1. Il linguaggio query

Il linguaggio query fornisce il vocabolario (campi e operatori) e la sintassi necessari per creare delle query. Li trovi descritti nel presente documento.

Clicca sul link di **Aiuto sintassi** e seleziona la scheda **Linguaggio query** per visualizzare i relativi contenuti.

Campi

Il campo delle query corrisponde a quello del database di GravityZone. I campi rappresentano elementi come percorsi e hash di file, nomi dell'host o nomi di dominio.

Ciascun campo può avere uno o più valori, che rappresentano il suo stato in un dato momento. Questi valori indicano tipi di dati differenti, a seconda del campo.

Operatori

Gli operatori ti permettono di creare relazioni tra i campi o criteri di ricerca. Puoi usare i seguenti operatori:

Operatore	Esempio	Descrizione
`:`	`fieldCategory.option: value1`	Confronta il valore del campo della query con i valori del campo corrispondente del database.
`" "`	`fieldCategory.option: "value1 value2"`	Le stringhe contenute all'interno delle virgolette vengono prese in considerazione insieme, come frase.

Operatore	Esempio	Descrizione
( )	`fieldCategory1.option: value1 E (fieldCategory2.option: value2 O fieldCategory3.option: value3)`	Raggruppa i termini della query.
AND	`fieldCategory1.option: value1 E fieldCategory2.option: value2`	Restituisce i risultati che corrispondono a tutte le condizioni della tua query.
O	`fieldCategory1.option: value1 O fieldCategory2.option: value2`	Restituisce i risultati una qualsiasi delle condizioni della tua query.
E NON	`fieldCategory1.option: value1 E NON fieldCategory2.option: value2`	Questo operatore è utile nelle query complesse e fornisce risultati che non corrispondono al termine specificato, a parte tutte le altre condizioni.
exists	`_exists_: fieldCategory.option`	Restituisce risultati che contengono il campo indicato.
-	`fieldCategory.option: -value`	Usa il segno meno (-) quando il valore deve essere escluso dai risultati.
?	`fieldCategory.option: ???_file.path`	Usa un punto di domanda (?) per abbinare un qualsiasi carattere nel valore del campo.
*	`fieldCategory.option: file.*`	Usa un asterisco (*) per indicare qualsiasi valore.

Sintassi query

Una query è una condizione o una serie di condizioni logiche legate da operatori che restituiscono come risultato eventi provenienti dal database EDR.

Tutte le condizioni devono essere correlate ai campi. Alcune condizioni richiedono l'immissione di un valore, altre no. Ad esempio, non hai bisogno di inserire un valore se vuoi soltanto sapere se il campo è presente tra i dettagli dell'evento.

Le query possono essere semplici o complesse. Le query complesse hanno query annidate (query in un'altra query).

Una valida sintassi del campo consiste nella categoria del campo seguita da una delle opzioni nella sezione **Lingua query**, e il suo valore corrispondente: `fieldCategory.option: value`.

Per esempio, `file.path: "%system32%\com\svchost.exe"` è una query abbastanza semplice che cerca tutti gli eventi che includono `%system32%\com\svchost.exe`, e consiste in:

- Una categoria di campo obbligatoria e relativa opzione (separate da un punto): `file.path`
- Un operatore: i due punti (:), per confrontare il valore del campo
- Il valore ricercato: `%system32%\com\svchost.exe`
- Virgolette (" "), perché il valore contiene caratteri speciali, come <\> e <.>

6.3.2. Eseguire query

Per eseguire una query:

1. Digita la stringa della query nel campo.

   Clicca il campo **Cerca** per vedere l'elenco dei termini di ricerca suddivisi per categoria. Seleziona il termine che desideri per iniziare a creare la tua query.

   Control Center ti aiuta durante la digitazione, con suggerimenti per il completamento automatico. Usa i tasti di direzione per selezionare una delle opzioni suggerite, quindi premi **Invio** per aggiungerla alla query.

   Se ti serve ulteriore aiuto, clicca il link **Aiuto sintassi**.

   Nota
   Puoi usare le query annidate per effettuare ricerche complesse.

2. Per filtrare gli eventi in base a un intervallo temporale, clicca il campo dell'ora.

   Importante
   L'intervallo di conservazione dei dati predefinito per gli eventi è 7 giorni. Se vuoi aumentare la tua capacità, devi contattare il tuo rappresentante vendite per fare l'upgrade della soluzione con un add-on **Conservazione dati** di 30, 90 o 180 giorni.

   Ha diverse opzioni a disposizione per definire l'intervallo di tempo della ricerca:

   - Solo una data specifica.

     Seleziona una data nella scheda **Da** del calendario.
   - Un intervallo di tempo esatto.
     a. Seleziona la data iniziale nella scheda **Da** del calendario.
     b. Seleziona la data di termine nella scheda **A**.
   - Un intervallo di tempo recente dalle opzioni disponibili.
   - Clicca su **OK**.

3. Clicca su **Cerca** o premi **Invio**.

   Puoi vedere gli eventi corrispondenti, insieme ai relativi dettagli, sotto la query.

   Importante
   Quando cerchi la query `detections.detection_type` nel campo *Cerca*, Control Center richiede di completarla con un valore intero compreso tra 1 a 15 (ad esempio `detections.detection_type:1`).

   Ogni valore inserito corrisponde a un determinato tipo di rilevazione, come segue:

   a. `detections.detection_type:1` - Rilevamento di Advanced Threat Control
   b. `detections.detection_type:2` - Rilevamento motori statici antimalware
   c. `detections.detection_type:3` - Rilevamento HyperDetect
   d. `detections.detection_type:4` - Notifica evento sospetto Advanced Threat Control
   e. `detections.detection_type:5` - Rilevamento di HyperDetect per tipo di attacco segnalato

f. `detections.detection_type:6` - Rilevamento Antimalware CMDLine Scanner

g. `detections.detection_type:7` - Rilevamento Cross Technologies Correlation

h. `detections.detection_name:8` - Rilevamento Network Attack Defense

i. `detections.detection_type:9` - Rilevamento di HyperDetect da tipo di attacco non segnalato

j. `detections.detection_type:10` - Sandbox Analyzer ha effettuato un rilevamento in un ambiente limitato dopo un'analisi dinamica

k. `detections.detection_type:11` - Rilevamento Buffer Register Scan

l. `detections.detection_type:12` - Rilevamento URL

m. `detections.detection_type:13` - Rilevamento avanzato Anti-Exploit

n. `detections.detection_type:14` - Rilevamento analisi comportamento utenti

o. `detections.detection_type:15` - Rilevamento interfaccia scansione antimalware

p. `detections.detection_type:16` - Rilevamento della correlazione tra tecnologie basate sul machine learning

Control Center può mostrare fino a 10.000 eventi. Se i risultati della query contengono più di 10.000 eventi, comparirà un messaggio sullo schermo. In questo caso, dovrai restringere la tua ricerca.

6.3.3. Ricerche preferite

La maggior parte delle query è piuttosto lunga e quindi difficile da creare o ricordare. Invece di salvarle in un file per poi copiarle e incollarle in GravityZone, puoi salvarle direttamente in GravityZone in modo da averle sempre a portata di mano.

Per salvare la tua query:

1. Inserisci la stringa nel campo **Cerca**.
2. Clicca sull'icona ☆ a destra del campo **Cerca**.
3. Quando ti viene richiesto di assegnarle un nome, digita il nome che vuoi dare alla query.

4. Clicca su **Add** (Aggiungi).

Clicca sul link **Ricerche preferite** sotto il campo **Query** per visualizzare le query che hai salvato.

A questo punto puoi scegliere tra tre opzioni:

- Eseguire la query.
- Modificare il nome della query.
- Eliminare la query.

Per eseguire una query salvata:

1. Clicca sul link **Ricerche preferite**.
2. Seleziona la query che preferisci.

   La stringa salvata verrà aggiunta al campo **Cerca**.

   Nota
   Se necessario, modifica la stringa della query. Inoltre, puoi anche salvare la nuova query di ricerca nelle tue ricerche preferite.

3. Usa i filtri per azienda e calendario per restringere la ricerca.
4. Clicca su **Cerca**.

Se devi modificare l'elenco delle tue query, posiziona il cursore del mouse sulla query salvata per vedere le opzioni incorporate.

- Clicca sull'icona **Modifica** per rinominare la query.
- Se non hai più bisogno della query, clicca sull'icona **Elimina**.

6.3.4. Query predefinite

La pagina **Cerca** contiene alcuni esempi di ricerche tramite query complesse, specifiche per indagini relative a eventi di sicurezza.

Le query predefinite sono raggruppate per categoria di indagine di sicurezza.

Per eseguire una query predefinita:

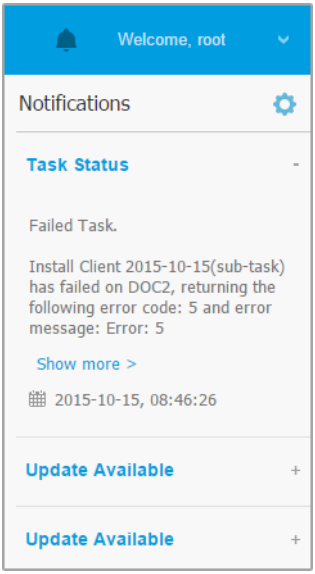
- Clicca l'icona accanto alla descrizione della query predefinita.
- La frase della query comparirà automaticamente nella barra **Cerca**. Inserisci i dettagli specifici dei termini della query.

- Clicca il pulsante **Cerca** per eseguire la query.

Nota
Dalla pagina **Cerca** puoi ritornare in qualsiasi momento alle opzioni **Inizia**, cliccando sul link **Inizia** nell'angolo in alto a destra della pagina.

7. NOTIFICHE

In base agli eventi che potrebbero verificarsi nella tua rete, Control Center mostrerà diverse notifiche per informarti dello stato di sicurezza del tuo ambiente. Le notifiche saranno mostrate nell'**Area notifiche**, localizzata nel lato destro di Control Center.



Area notifiche

Quando nella rete vengono rilevati nuovi eventi, l'icona 11 nell'angolo in alto a destra di Control Center mostrerà il numero di nuovi eventi rilevati. Cliccare sull'icona consente di mostrare l'Area notifiche contenente l'elenco degli eventi rilevati.

7.1. Tipi di notifiche

Questo è l'elenco dei tipi di notifica disponibili:

Epidemia malware

Questa notifica viene inviata agli utenti che hanno almeno il 5% di tutti i loro elementi di rete gestiti infettati dallo stesso malware.

Perciò, per le aziende partner, la notifica viene generata quando lo stesso malware viene rilevato in maniera cumulativa su endpoint della loro stessa rete e delle reti delle aziende figlie.

Puoi configurare la soglia di diffusione dei malware in base alle tue necessità nella finestra **Impostazioni notifiche**. Per maggiori informazioni, fai riferimento a «Configurare le impostazioni di scansione» (p. 98).

Le minacce rilevate da HyperDetect sono escluse da questa notifica.

Anti-exploit avanzato

Questa notifica ti avvisa quando l'Anti-exploit avanzato ha rilevato tentativi di exploit nella tua rete.

Accesso da nuovo dispositivo

Questa notifica ti informa che il tuo account GravityZone è stato usato per accedere a Control Center da un dispositivo che finora non hai mai utilizzato a tale scopo. La notifica viene configurata automaticamente per essere visibile sia in Control Center che via e-mail, e solo tu potrai visualizzarla.

Evento incidenti di rete

Questa notifica viene inviata ogni volta che il modulo Network Attack Defense rileva un tentativo di attacco nella tua rete. Questa notifica ti informa anche se il tentativo di attacco è stato condotto dall'esterno della rete o da un endpoint compromesso nella rete. Altri dettagli includono dati sull'endpoint, la tecnica di attacco, l'IP dell'aggressore e l'azione intrapresa da Network Attack Defense.

Attività HyperDetect

Questa notifica segnala quando HyperDetect trova qualsiasi antimalware o eventi non bloccati all'interno della rete. Viene inviata per ciascun evento di HyperDetect e contiene i seguenti dettagli:

- Informazioni sull'endpoint interessato (nome, IP, agente installato)
- Tipo e nome del malware
- Percorso del file infetto. Per gli attacchi privi di file, viene indicato il nome dell'eseguibile usato nell'attacco.
- Stato dell'infezione
- L'hash SHA256 dell'eseguibile malware
- Il tipo di attacco previsto (attacco mirato, grayware, exploit, ransomware, file sospetti e traffico di rete)

- Grado di rilevazione (Permissivo, Normale, Aggressivo)
- Ora e data della rilevazione

Puoi visualizzare maggiori dettagli sull'infezione e investigare ulteriormente sui problemi generando un rapporto **Attività HyperDetect** direttamente dalla pagina **Notifiche**. Per farlo:

1. In Control Center, clicca sul pulsante **Notifiche** per visualizzare l'area delle notifiche.
2. Clicca sul link **Mostra altro** al termine della notifica per aprire la pagina **Notifiche**.
3. Clicca sul pulsante **Vedi rapporto** nei dettagli della notifica. In questo modo si aprirà la finestra di configurazione.
4. Se necessario, configura il rapporto. Per maggiori informazioni, fai riferimento a «Creare i rapporti» (p. 117).
5. Clicca su **Genera**.

Nota
Per evitare di creare spam, riceverai un massimo di una notifica ogni ora.

Problema patch mancante

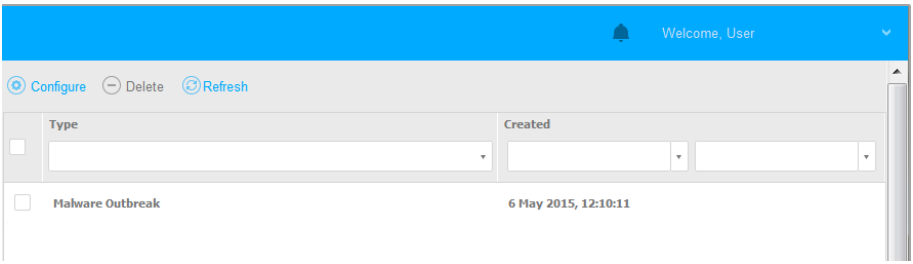
Questa notifica si verifica quando gli endpoint nella tua rete non hanno una o più patch disponibili.

Puoi visualizzare quali endpoint sono in questa situazione cliccando sul pulsante **Vedi rapporto** nei dettagli della notifica.

Di norma, la notifica fa riferimento a patch di sicurezza, ma potresti configurarla per informarti anche sulle patch di non sicurezza.

7.2. Visualizzare le notifiche

Per visualizzare le notifiche, clicca sul pulsante **Notifiche** e clicca su **Vedi tutte le notifiche**. Viene mostrata una tabella contenente tutte le notifiche.



La pagina Notifiche

In base al numero di notifiche, la tabella può essere formata da diverse pagine (di norma, per ogni pagina sono presenti solo 20 voci).

Per muoversi tra le pagine, usa i pulsanti di navigazione nella parte inferiore della tabella.

Per cambiare il numero di valori mostrati in una pagina, seleziona un'opzione nel menu accanto ai pulsanti di navigazione.

Nel caso ci fossero troppi valori, puoi usare le caselle di ricerca sotto le intestazioni delle colonne o il menu filtro nel lato superiore della tabella per filtrare i dati mostrati.

- Per filtrare le notifiche, seleziona il tipo di notifica che vuoi visualizzare nel menu **Tipo**. In alternativa, puoi selezionare l'intervallo di tempo durante il quale è stata generata la notifica, per ridurre il numero di valori nella tabella, specialmente se è stato generato un numero elevato di notifiche.
- Per visualizzare i dettagli della notifica, clicca sul nome della notifica nella tabella. Sotto la tabella viene mostrata una sezione **Dettagli**, in cui puoi visualizzare l'evento che ha generato la notifica.

7.3. Eliminare le notifiche

Per eliminare le notifiche:

1. Clicca sul pulsante **Notifiche** sul lato destro della barra dei menu e clicca su **Vedi tutte le notifiche**. Viene mostrata una tabella contenente tutte le notifiche.
2. Seleziona le notifiche che vuoi eliminare.
3. Clicca sul pulsante **Elimina** nel lato superiore della tabella.

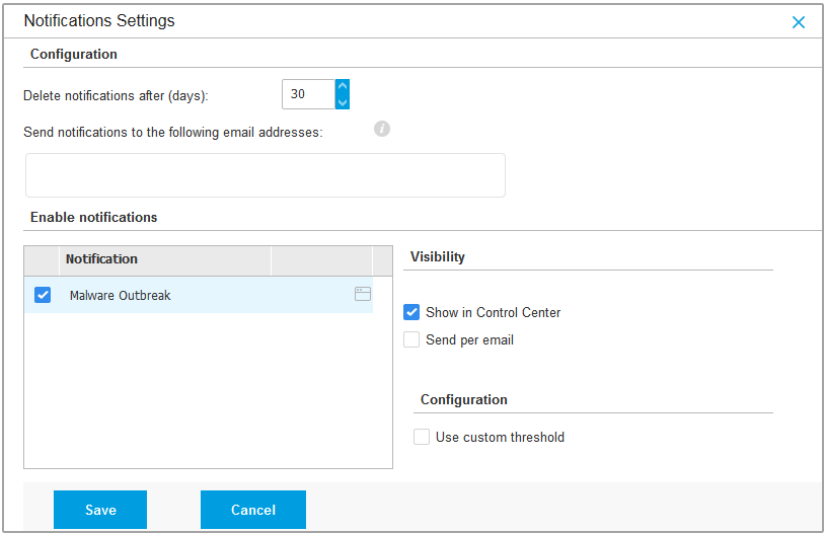
Puoi anche configurare le notifiche per essere eliminate automaticamente dopo un determinato numero di giri. Per maggiori informazioni, fai riferimento a «Configurare le impostazioni di scansione» (p. 98).

7.4. Configurare le impostazioni di scansione

Il tipo di notifiche da inviare e gli indirizzi email a cui vengono inviate possono essere configurati per ciascun utente.

Per configurare le impostazioni delle notifiche:

1. Clicca sul pulsante **Notifiche** sul lato destro della barra dei menu e clicca su **Vedi tutte le notifiche**. Viene mostrata una tabella contenente tutte le notifiche.
2. Clicca sul pulsante **Configura** nel lato superiore della tabella. Viene mostrata la finestra **Impostazioni delle notifiche**.



Impostazioni notifiche

Nota
Puoi anche accedere direttamente alla finestra **Impostazioni delle notifiche** usando l'icona **Configura** nell'angolo in alto a destra della finestra **Area notifiche**.

3. Nella sezione **Configurazione**, puoi definire le seguenti impostazioni:
   -
   - Inoltre, puoi inviare le notifiche via email a determinati destinatari. Inserisci gli indirizzi email nel campo dedicato, premendo il tasto `Invio` dopo ogni indirizzo.
4. Nella sezione **Attiva notifiche** puoi selezionare il tipo di notifiche che vuoi ricevere da GravityZone. Puoi anche configurare individualmente visibilità e opzioni di invio per ciascun tipo di notifica.

   Seleziona il tipo di notifica che desideri dall'elenco. Per maggiori informazioni, fai riferimento a «Tipi di notifiche» (p. 94). Una volta selezionato un tipo di notifica, puoi configurare le sue opzioni specifiche (se disponibili) nell'area a destra:

Visibilità

- **Mostra in Control Center** indica che questo tipo di evento viene mostrato in Control Center, con l'aiuto del pulsante **Notifiche**.
- **Invia per e-mail** indica che questo tipo di evento viene inviato anche a determinati indirizzi e-mail. In questo caso, è necessario inserire gli indirizzi e-mail nel campo dedicato, premendo `Invio` dopo ogni indirizzo.

Configurazione

- **Usa soglia personalizzata** - Ti consente di definire una soglia per gli eventi che si verificano, da cui viene inviata la notifica selezionata.

  Per esempio, la notifica Epidemia malware viene inviata di norma agli utenti che hanno almeno il 5% dei loro elementi di rete gestiti infettati dallo stesso malware. Per modifica il valore della soglia di un'epidemia malware, attiva l'opzione **Usa soglia personalizzata** e inserisci il valore che desideri nel campo **Soglia epidemia malware**.
- Per **Stato attività**, puoi selezionare il tipo di stato che attiverà questo tipo di notifica:
  - **Ogni stato** - Notifica ogni volta che un'attività inviata da Control Center viene eseguita con uno stato qualsiasi.

- **Solo fallite** - Notifica ogni volta che un'attività inviata da Control Center è fallita.

5. Clicca su **Salva**.

8. UTILIZZARE I RAPPORTI

Control Center ti consente di creare e visualizzare rapporti centralizzati sullo stato di sicurezza degli elementi di rete gestiti. I rapporti possono essere usati per diversi scopi, come:

- Monitorare e assicurare la conformità alle policy di sicurezza dell'organizzazione.
- Controllare e valutare lo stato di sicurezza della rete.
- Identificare problemi, minacce e vulnerabilità di sicurezza della rete.
- Monitorare gli incidenti di sicurezza.
- Fornire una gestione superiore con dati di facile interpretazione sulla sicurezza della rete.

Sono disponibili diversi tipi di rapporto, così da poter ottenere facilmente tutte le informazioni di cui necessiti. Le informazioni vengono presentate con tabelle e diagrammi di facile interpretazione, consentendoti di controllare rapidamente lo stato di sicurezza della rete e individuare eventuali problemi.

I rapporti possono raccogliere i dati dall'intera rete di elementi gestiti o solo da alcuni gruppi specifici. In questo modo, da un singolo rapporto, puoi scoprire:

- Dati statistici relativi a tutti gli elementi di rete gestiti o a gruppi di essi.
- Informazioni dettagliate per ogni elemento di rete gestito.
- L'elenco di computer che soddisfano determinati criteri (per esempio, quelli con la protezione antimalware disattivata).

Alcuni rapporti ti consentono anche di risolvere rapidamente eventuali problemi rilevati nella tua rete. Per esempio, puoi aggiornare facilmente tutti gli elementi di rete bersaglio direttamente dal rapporto, senza dover uscire ed eseguire un'attività di aggiornamento dalla pagina **Rete**.

Tutti i rapporti programmati sono disponibili in Control Center ma puoi salvarli sul computer o inviarli via e-mail.

I formati disponibili includono Portable Document Format (PDF) e comma-separated values (CSV).

8.1. Tipo di rapporto

Per ogni tipo di endpoint sono disponibili diverse tipologie di rapporto:

- Rapporti per computer e virtual machine
- Rapporti Exchange

8.1.1. Rapporti per computer e virtual machine

Questi sono i tipi di rapporto disponibili per macchine virtuali e fisiche:

Attività antiphishing

Ti informa sulle attività del modulo Antiphishing di Bitdefender Endpoint Security Tools. Puoi visualizzare il numero di siti web phishing bloccati sugli endpoint selezionati e l'utente che era collegato al momento dell'ultima rilevazione. Cliccando sui link della colonna **Siti web bloccati**, puoi anche visualizzare gli URL dei siti web, quante volte sono stati bloccati e quando si è verificato l'ultimo evento di blocco.

Applicazioni bloccate

Ti informa sulle attività dei seguenti moduli: Antimalware, Firewall, Controllo contenuti, Anti-exploit avanzato e ATC/IDS. Puoi visualizzare il numero di applicazioni bloccate sugli endpoint selezionati e l'utente che era collegato al momento dell'ultima rilevazione.

Clicca sul numero associato a un bersaglio per visualizzare informazioni aggiuntive sulle applicazioni bloccate, il numero di eventi verificatesi e la data e l'ora dell'ultimo evento di blocco.

Siti web bloccati

Ti informa sulle attività del modulo Controllo web di Bitdefender Endpoint Security Tools. Per ogni bersaglio, puoi visualizzare il numero di siti web bloccati. Cliccando su questo numero, puoi visualizzare informazioni aggiuntive, come:

- URL del sito web e categoria
- Numero di tentativi di accesso per sito web
- Data e ora dell'ultimo tentativo, oltre all'utente che era collegato al momento della rilevazione.
- Il motivo del blocco, che include accesso programmato, rilevazione malware, filtro categorie e blacklist.

Panoramica stato cliente

Ti aiuta a rilevare problemi di protezione nelle aziende clienti. Un'azienda ha problemi se viene rilevato un malware, l'antimalware è datato o la licenza è scaduta. Il nome dell'azienda è un link a una nuova finestra, in cui potrai trovare i dettagli aziendali.

Protezione dati

Ti informa sulle attività del modulo Protezione dati di Bitdefender Endpoint Security Tools. Puoi visualizzare il numero di e-mail e siti web bloccati sugli endpoint selezionati, oltre all'utente che era collegato al momento dell'ultima rilevazione.

Attività controllo dispositivi

Ti informa sugli eventi verificatisi durante l'accesso agli endpoint tramite i dispositivi monitorati. Per ogni endpoint bersaglio, puoi visualizzare il numero di accessi consentiti / bloccati e gli eventi di sola lettura. Se tali eventi si verificano, sono disponibili ulteriori informazioni cliccando sui numeri corrispondenti. I dettagli fanno riferimento a:

- Utente collegato alla macchina
- ID e tipo di dispositivo
- ID prodotto e fornitore dispositivo
- Data e ora dell'evento.

Stato moduli endpoint

Fornisce una panoramica della copertura dei moduli di protezione sui bersagli selezionati. Nei dettagli del rapporto, per ogni endpoint bersaglio puoi visualizzare quali moduli sono attivi, disattivati o non installati, e anche il motore di scansione in uso. Cliccando sul nome dell'endpoint comparirà la finestra **Informazioni** con dettagli sull'endpoint e i livelli di protezione installati.

Cliccando sul pulsante **Riconfigura client**, puoi avviare un'attività per modificare le impostazioni iniziali di uno o più endpoint selezionati. Per maggiori dettagli, fai riferimento a Riconfigura client.

Stato protezione endpoint

Ti fornisce diverse informazioni sullo stato relative agli endpoint selezionati della tua rete.

- Stato protezione antimalware
- Stato aggiornamento Bitdefender Endpoint Security Tools
- Stato attività di rete (online/offline)
- Stato gestione

Puoi applicare filtri per aspetto e stato della sicurezza così da trovare le informazioni che stai cercando.

Attività Firewall

Ti informa sulle attività del modulo Firewall di Bitdefender Endpoint Security Tools. Puoi visualizzare il numero di tentativi di traffico bloccato e i port scan bloccati sugli endpoint selezionati, oltre all'utente che aveva eseguito l'accesso al momento dell'ultimo rilevamento.

Attività HyperDetect

Ti informa sulle attività del modulo HyperDetect di Bitdefender Endpoint Security Tools.

Il grafico nella parte superiore della pagina del rapporto ti mostra le dinamiche dei tentativi di attacco nel periodo di tempo indicato e la loro distribuzione per tipo di attacco. Spostando il mouse sui valori della legenda evidenzierai il relativo tipo di attacco nel grafico. Cliccando sul valore mostrerai o nasconderai la rispettiva linea nel grafico. Cliccando su un punto qualsiasi su una linea filtrerai i dati della tabella in base al tipo selezionato. Per esempio, cliccando su un punto nella linea arancione, la tabella mostrerà solo gli exploit.

I dettagli nella parte inferiore del rapporto consentono di identificare le violazioni nella rete e se sono state risolte. Si riferiscono a:

- Il percorso del file dannoso o l'URL rilevato in caso di file infetti. Per gli attacchi privi di file viene riportato il nome dell'eseguibile usato nell'attacco, con un link a una finestra di dettagli contenente i motivi per cui è stato rilevato e la stringa della riga di comando dannosa.
- L'endpoint su cui è stato fatto il rilevamento
- Il modulo di protezione che ha rilevato la minaccia. Poiché HyperDetect è un livello aggiuntivo dei moduli Antimalware e Controllo contenuti, il rapporto fornirà informazioni su uno di questi moduli, in base al tipo di rilevamento.
- Il tipo di attacco previsto (attacco mirato, grayware, exploit, ransomware, file sospetti e traffico di rete)
- Lo stato della minaccia
- Il livello di protezione del modulo a cui è stata rilevata la minaccia (Permissivo, normale, aggressivo)
- Numero di volte che la minaccia è stata rilevata
- Rilevamento più recente
- Identificazione come attacco privo di file (sì o no), per filtrare rapidamente gli attacchi di questo tipo rilevati

Nota
Un file può essere utilizzato in più tipi di attacchi. Inoltre, GravityZone lo segnala per ogni tipo di attacco in cui è stato coinvolto.

Da questo rapporto, puoi risolvere rapidamente falsi positivi, aggiungendo eccezioni nelle policy di sicurezza assegnate. Per farlo:

1. Seleziona quanti valori nella tabella ti servono.

   Nota
   I rilevamenti di attacchi privi di file non possono essere aggiunti all'elenco delle eccezioni, poiché l'eseguibile rilevato non è di per sé un malware, ma può essere una minaccia utilizzando una linea di comando codificata dannosa.

2. Clicca sul pulsante **Aggiungi eccezione** nel lato superiore della tabella.
3. Nella finestra di configurazione, seleziona le policy a cui deve essere aggiunta l'eccezione, quindi clicca su **Aggiungi**.

   Di norma, le informazioni relative a ogni eccezione aggiunta vengono inviate ai Bitdefender Labs per aiutare a migliorare le capacità di rilevazione dei prodotti Bitdefender. Puoi controllare questa azione utilizzando la casella **Invia questo feedback a Bitdefender per ulteriori analisi**.

Se la minaccia viene rilevata dal modulo Antimalware, l'eccezione sarà applicata sia alla modalità Scansione all'accesso che alla Scansione a richiesta.

Nota
Puoi trovare queste eccezioni nelle seguenti sezioni delle policy selezionate: **Antimalware > Impostazioni** per i file, e **Controllo contenuti > Traffico** per gli URL.

Stato della licenza

Ti informa sulla copertura della protezione di Bitdefender nella tua rete. Vengono forniti dettagli relativi al tipo, l'utilizzo e la durata delle licenze per le aziende selezionate.

Cliccando nel numero nella colonna **Uso**, che corrisponde a un'azienda con licenza mensile, puoi anche visualizzare i dettagli di utilizzo, come il numero totale di posti della licenza e il numero di posti restanti disponibili per l'installazione.

Stato malware

Ti aiuta a scoprire quanti e quali endpoint selezionati sono stati influenzati dai malware in un determinato periodo di tempo e come sono state gestite le minacce. Puoi anche visualizzare l'utente che aveva eseguito l'accesso al momento dell'ultimo rilevamento.

Gli endpoint sono raggruppati in base a questi criteri:

- Endpoint senza rilevazioni (nel periodo indicato non è stata rilevata alcuna minaccia malware)
- Endpoint con malware risolti (tutti i file rilevati sono stati disinfettati o spostati in quarantena con successo)
- Endpoint con malware non risolti (non è stato possibile accedere ad alcuni dei file rilevati)

Per ogni endpoint, cliccando sui link disponibili nelle colonne del risultato della disinfezione, puoi visualizzare l'elenco delle minacce e i percorsi dei file influenzati.

In questo rapporto, puoi eseguire rapidamente un'attività di Scansione completa sui bersagli non risolti, cliccando sul pulsante **Esamina bersagli infetti** dalla barra degli strumenti sopra la tabella dei dati.

Incidenti di rete

Ti informa sulle attività del modulo Network Attack Defense. Un grafico mostra il numero di tentativi di attacco rilevato in un determinato intervallo. I dettagli del rapporto includono:

- Nome endpoint, IP e FQDN
- Utente
- Nome rilevato
- Tecnica di attacco
- Numero di tentativi
- IP dell'aggressore
- IP colpito e porta
- Quando l'attacco è stato bloccato più di recente

Cliccando sul pulsante **Aggiungi eccezioni** per un determinato rilevamento, si crea automaticamente un valore in **Eccezioni globali** nella sezione **Protezione rete**.

Stato patch rete

Controlla lo stato dell'aggiornamento del software che è stato installato nella tua rete. Il rapporto svela i seguenti dettagli:

- Macchina obiettivo (nome endpoint, IP e sistema operativo).
- Patch di sicurezza (patch installate, patch fallite, patch di sicurezza e non mancanti).
- Stato e ultima modifica per gli endpoint controllati.

Stato protezione rete

Ti fornisce informazioni dettagliate sullo stato della sicurezza generale degli endpoint bersaglio. Ad esempio, puoi vedere informazioni su:

- Nome, IP e FQDN
- Stato:
  - **Ha problemi** - L'endpoint ha delle vulnerabilità nella protezione (agente di sicurezza non aggiornato, minacce alla sicurezza rilevate, ecc.)
  - **Nessun problema** - L'endpoint è protetto e non ci sono motivi di preoccupazione.
  - **Sconosciuto** - L'endpoint era offline quando il rapporto è stato generato.
  - **Non gestito** - L'agente di sicurezza non è ancora stato installato sull'endpoint.
- Livelli di protezione disponibili
- Endpoint gestiti e non gestiti (l'agente di sicurezza è installato oppure no)
- Tipo e stato della licenza (per impostazione predefinita, le colonne aggiuntive relative alla licenza sono nascoste)
- Stato dell'infezione (l'endpoint è "pulito" oppure no)
- Stato di aggiornamento del prodotto e del contenuto di sicurezza
- Stato delle patch di sicurezza dei software (patch mancanti, di sicurezza o differenti)

Per gli endpoint non gestiti, vedrai lo stato **Non gestito** sotto altre colonne.

Scansione a richiesta

Fornisce informazioni relative alle scansioni a richiesta eseguite sui bersagli selezionati. Un diagramma mostra le statistiche delle scansioni fallite e

avvenute con successo. La tabella sotto il diagramma fornisce maggiori dettagli sul tipo di scansione, la frequenza e l'ultima scansione avvenuta con successo per ciascun endpoint.

Conformità policy

Fornisce informazioni relative alle policy di sicurezza applicate ai bersagli selezionati. Un diagramma che mostra lo stato della policy. Nella tabella sotto il diagramma, puoi visualizzare la policy assegnata su ciascun endpoint e il tipo di policy, oltre alla data e all'utente che l'ha assegnata.

Invii non riusciti di Sandbox Analyzer

Mostra tutti gli invii di elementi falliti inviati dagli endpoint a Sandbox Analyzer in un determinato periodo di tempo. Un invio viene considerato fallito dopo diversi tentativi.

Il grafico mostra la variazione degli invii falliti durante il periodo selezionato, mentre nella tabella dei dettagli del rapporto è possibile visualizzare quali file possono essere inviati a Sandbox Analyzer, la macchina da cui l'elemento è stato inviato, la data e l'ora di ogni tentativo, il codice di errore ricevuto, la descrizione di ogni tentativo fallito e il nome dell'azienda.

Risultati di Sandbox Analyzer (deprecati)

Ti fornisce informazioni dettagliate relative ai file sugli endpoint bersaglio, che sono stati analizzati nel sandbox nel corso di un determinato periodo di tempo. Un grafico a linea mostra il numero di file puliti o pericolosi analizzati, mentre la tabella ti offre alcuni dettagli su ciascun caso.

Puoi generare un rapporto dei risultati di Sandbox Analyzer per tutti i file analizzati o solo per quelli rilevati come dannosi.

Puoi visualizzare:

- Il verdetto dell'analisi, che indica se il file è pulito, pericoloso o sconosciuto (**Minaccia rilevata** / **Nessuna minaccia rilevata** / **Non supportata**). Questa colonna compare solo quando selezioni il rapporto per visualizzare tutti gli elementi analizzati.

  Per visualizzare l'elenco completo delle estensioni e dei tipi di file supportati da Sandbox Analyzer, fai riferimento a «Estensioni e tipi di file supportati per l'invio manuale» (p. 129).
- Tipo di minaccia, come adware, rootkit, downloader, exploit, host-modifier, strumenti dannosi, ladri di password, ransomware, spam o Trojan.
- Data e ora del rilevamento, che puoi filtrare in base al periodo del rapporto.
- Il nome dell'host o l'IP dell'endpoint in cui il file è stato rilevato.

- Il nome dei file, se sono stati inviati individualmente o il numero di file analizzati in caso di un pacchetto. Clicca sul nome del file o il link del bundle per visualizzare i dettagli e le azioni intraprese.
- Lo stato dell'azione di risanamento per i file inviati (**Parziale**, **Fallito**, **Solo segnalato**, **Avvenuto con successo**).
- Nome azienda.
- Maggiori informazioni sulle proprietà del file analizzato sono disponibili cliccando sul pulsante **Leggi altro** nella colonna **Risultato analisi**. Qui puoi visualizzare approfondimenti sulla sicurezza e rapporti dettagliati sul comportamento del campione.

Sandbox Analyzer cattura i seguenti eventi comportamentali:

- Scrittura / eliminazione / spostamento / duplicazione / sostituzione dei file sul sistema e su unità rimovibili.
- Esecuzione di file appena creati.
- Modifiche al file di sistema.
- Modifiche alle applicazioni in esecuzione nella virtual machine.
- Modifiche alla barra delle applicazioni di Windows e al menu Start.
- Creazione / conclusione / inserimento processi.
- Scrittura / eliminazione chiavi del registro.
- Creazione di oggetti mutex.
- Creazione / esecuzione / blocco / modifica / interrogazione / eliminazione di servizi.
- Modificare le impostazioni di sicurezza del browser.
- Modificare le impostazioni di visualizzazione di Windows Explorer.
- Aggiungere file all'elenco delle eccezioni del firewall.
- Modificare le impostazioni della rete.
- Attivare l'esecuzione all'avvio del sistema.
- Connessione a un host remoto.
- Accesso a determinati domini.
- Trasferimento dati a e da determinati domini.
- Accesso a URL, IP e porte tramite diversi protocolli di comunicazione.
- Verifica degli indicatori dell'ambiente virtuale.
- Verifica degli indicatori degli strumenti di monitoraggio.
- Creazione di istantanee
- Hook SSDT, IDT, IRP.
- Dump di memoria per processi sospetti.
- Chiamate di funzioni API di Windows.

- Disattivazione per un determinato periodo di tempo per ritardare l'esecuzione.
- Creazione di file con azioni da eseguire in determinati intervalli di tempo.

Nella finestra **Risultato analisi**, clicca sul pulsante **Scarica** per salvare i contenuti del Riepilogo comportamento nei seguenti formati: XML, HTML, JSON, PDF.

Verifica sicurezza

Fornisce informazioni sugli eventi di sicurezza che si sono verificati su un bersaglio selezionato. Le informazioni fanno riferimento ai seguenti eventi:

- Rilevamento malware
- Applicazione bloccata
- Porta di scansione bloccata
- Traffico bloccato
- Sito web bloccato
- Blocca dispositivo
- E-mail bloccata
- Processo bloccato
- Eventi dell'Anti-exploit avanzato
- Eventi di Network Attack Defense

Stato Security Server

Ti aiuta a valutare lo stato del bersaglio del Security Server. Puoi identificare i problemi che ogni Security Server potrebbe avere, con l'aiuto di diversi indicatori di stato, come:

- **Stato**: mostra lo stato generale del Security Server.
- **Stato della macchina**: indica quali appliance del Security Server sono state bloccate.
- **Stato AV**: segnala se il modulo Antimalware è stato attivato o disattivato.
- **Stato aggiornamento**: mostra se le appliance del Security Server sono aggiornato o se gli aggiornamenti sono stati disattivati.
- **Stato del carico**: indica il livello di carico della scansione di un Security Server, come descritto di seguito:
  - **Sottocarico**, quando viene usata meno del 5% della sua capacità di scansione.
  - **Normale**, quando il carico della scansione è bilanciato.

- **Sovraccarico**, quando il carico della scansione supera il 90% della sua capacità. In tal caso, controlla le policy di sicurezza. Se tutti i Security Server assegnati in una policy sono sovraccaricati, dovrai aggiungere un altro Security Server all'elenco. Diversamente, controlla la connessione di rete tra i client e i Security Server senza problemi di carico.

Puoi anche visualizzare quanti agenti sono connessi al Security Server. Inoltre, cliccando sul numero di client connessi sarà mostrato l'elenco degli endpoint. Questi endpoint potrebbero essere vulnerabili se il Security Server ha problemi.

Top 10 malware rilevati

Ti mostra le 10 principali minacce malware rilevate in un determinato periodo di tempo sugli endpoint selezionati.

Nota
La tabella dei dettagli mostra tutti gli endpoint che sono stati infettati dai 10 principali malware rilevati.

Top 10 aziende infettate

Ti mostra le 10 aziende più infettate, in base alla tua selezione, tramite il numero di rilevamenti totali in un determinato periodo di tempo.

Top 10 endpoint infettati

Ti mostra i 10 endpoint più infettati in base al numero totale di rilevazioni in un determinato periodo di tempo tra gli endpoint selezionati.

Nota
La tabella dei dettagli mostra tutti i malware rilevati nei 10 principali endpoint infetti.

Stato dell'Aggiornamento

Ti mostra lo stato di aggiornamento dell'agente di sicurezza o del Security Server installati sui bersagli selezionati. Lo stato di aggiornamento si riferisce alle versioni del prodotto e del contenuto di sicurezza.

Utilizzando i filtri disponibili, puoi facilmente scoprire quali client sono stati aggiornati e quali no nelle ultime 24 ore.

In questo rapporto, puoi rapidamente portare gli agenti alla versione più recente. Per farlo, clicca sul pulsante **Aggiorna** dalla barra degli strumenti sopra la tabella dei dati.

Stato aggiornamento

Ti mostra gli agenti di sicurezza installati sui bersagli selezionati e se è disponibile oppure no una soluzione più recente.

Per gli endpoint con agenti di sicurezza più datati installati, puoi rapidamente installare l'agente di sicurezza supportato più recente cliccando sul pulsante **Aggiorna**.

Nota
Questo rapporto è disponibile solo quando è stato reso disponibile un upgrade della soluzione GravityZone.

Attività ransomware

Ti informa sugli attacchi ransomware che GravityZone ha rilevato sugli endpoint che gestisci e ti fornisce gli strumenti necessari per ripristinare i file interessati dagli attacchi.

Il rapporto è disponibile come una pagina in Control Center, distinto dalle altre segnalazioni e accessibile direttamente dal menu principale di GravityZone.

La pagina **Attività ransomware** è costituita da una griglia che, per ogni attacco ransomware, elenca i seguenti dati:

- Il nome, l'indirizzo IP e il FQDN dell'endpoint in cui è avvenuto l'attacco
- L'azienda a cui appartengono gli endpoint
- Il nome dell'utente che ha effettuato l'accesso durante l'attacco
- Il tipo di attacco, rispettivamente uno in locale o remoto
- Il processo in cui è stato eseguito il ransomware per gli attacchi locali o l'indirizzo IP da cui è stato avviato l'attacco per quelli remoti
- Data e ora del rilevamento
- Numero di file cifrati finché l'attacco è stato bloccato
- Lo stato dell'azione di ripristino per tutti i file sull'endpoint bersaglio

Di norma, alcuni dettagli sono nascosti. Clicca sul pulsante **Mostra/Nascondi colonne** nella parte in alto a destra della pagina per configurare i dettagli che vuoi visualizzare nella griglia. Se hai troppe voci nella griglia, puoi scegliere di nascondere i filtri usando il pulsante **Mostra/Nascondi filtri** nella parte in alto a destra della pagina.

Sono disponibili ulteriori informazioni cliccando sul numero per i file. Puoi visualizzare un elenco con l'intero percorso ai file originali e ripristinati, e lo stato di ripristino per tutti i file coinvolti nell'attacco ransomware selezionato.

Importante
Le copie di backup sono disponibili per un massimo di 30 giorni. Cerca di ricordarti la data e l'ora fino a cui i file potranno ancora essere ripristinati.

Per ripristinare i file dal ransomware:

1. Seleziona gli attacchi che desideri nella griglia.
2. Clicca sul pulsante **Ripristina file**. Comparirà una finestra di conferma.

   Sarà creata un'attività di ripristino. Puoi controllarne lo stato nella pagina **Attività**, proprio come per qualsiasi altra attività in GravityZone.

Se i rilevamenti sono il risultato dei processi legittimi, segui questi passaggi:

1. Seleziona le voci nella griglia.
2. Clicca sul pulsante **Aggiungi eccezione**.
3. Nella nuova finestra, seleziona le policy a cui applicare l'eccezione.
4. Clicca su **Add** (Aggiungi).

   applicherà tutte le possibili eccezioni: sulla cartella, sul processo e sull'indirizzo IP.

   Puoi controllarle o modificarle nella sezione della policy **Antimalware > Impostazioni > Eccezioni personali**.

Nota
Attività ransomware tiene traccia degli eventi per due anni.

8.1.2. Rapporti server Exchange

Si tratta dei tipi di rapporto disponibili per i server Exchange:

Exchange - Contenuti e allegati bloccati
Ti fornisce informazioni su email o allegati che il Controllo contenuti ha eliminato dai server selezionati durante un determinato intervallo di tempo. Le informazioni includono:

- Gli indirizzi email del mittente e dei destinatari.

Quando l'email ha più destinatari, invece degli indirizzi email, il rapporto mostra il numero di destinatari con un link a una finestra contenente l'elenco degli indirizzi email.

- Oggetto e-mail.
- Il tipo di rilevamento, indicando quale filtro del Controllo contenuti ha rilevato la minaccia.
- L'azione intrapresa sul rilevamento.
- Il server in cui la minaccia è stata rilevata.
- L'azienda che possiede il server mail.

Exchange - Allegati non esaminabili bloccati

Ti fornisce informazioni sulle email contenenti allegati non esaminabili (super-compressi, protetti da password, ecc.), bloccati sui server mail Exchange in un determinato periodo di tempo. Le informazioni fanno riferimento a:

- Gli indirizzi email del mittente e dei destinatari.

  Quando l'email viene inviata a più destinatari, invece degli indirizzi email, il rapporto mostra il numero di destinatari con un link a una finestra contenente l'elenco degli indirizzi email.
- Oggetto e-mail.
- Le azioni intraprese per rimuovere gli allegati non esaminabili:
  - **Email eliminata**, indicando che l'intera email è stata rimossa.
  - **Allegati eliminati**, un termine generico per tutte le azioni che rimuovono allegati da un messaggio email, come eliminare l'allegato, metterlo in quarantena o sostituirlo con un avviso.

  Cliccando sul link nella colonna **Azione**, puoi visualizzare maggiori dettagli su ogni allegato bloccato e la corrispondente azione intrapresa.
- Data e ora di rilevamento.
- Il server in cui l'email è stata rilevata.
- L'azienda che possiede il server mail.

Exchange - Attività scansione e-mail

Mostra statistiche sulle azioni intraprese dal modulo Protezione Exchange in un determinato intervallo di tempo.

Le azioni sono raggruppate per tipo di rilevamento (malware, spam, allegato vietato e contenuti vietati) e server.

Le statistiche fanno riferimento ai seguenti stati dell'email:

- **In quarantena.** Queste email sono state messe nella cartella Quarantena.
- **Eliminate/Respinte.** Queste email sono state eliminate o respinte dal server.
- **Reindirizzate.** Queste e-mail sono state reindirizzate all'indirizzo e-mail indicato nella policy.
- **Pulite e consegnate.** Queste email sono state ripulite dalle minacce e successivamente passate attraverso i filtri.

  Un'email viene considerata come pulita quando tutti gli allegati rilevati sono stati disinfettati, messi in quarantena, eliminati o sostituiti con un testo.
- **Modificate e consegnate.** Le informazioni della scansione sono stati aggiunti alle intestazioni delle email, passando queste ultime tramite i filtri.
- **Consegnate senza nessun'altra azione.** Queste email sono state ignorate dalla Protezione Exchange e sono state analizzate dai filtri.

Exchange - Attività malware

Ti fornisce informazioni sulle email con minacce malware, rilevate sui server mail Exchange selezionati in un determinato periodo di tempo. Le informazioni fanno riferimento a:

- Gli indirizzi email del mittente e dei destinatari.

  Quando l'email viene inviata a più destinatari, invece degli indirizzi email, il rapporto mostra il numero di destinatari con un link a una finestra contenente l'elenco degli indirizzi email.
- Oggetto e-mail.
- Stato dell'email dopo la scansione antimalware.

  Cliccando sul link dello stato, puoi visualizzare maggiori dettagli sui malware eliminati e l'azione intrapresa.
- Data e ora di rilevamento.
- Il server in cui la minaccia è stata rilevata.
- L'azienda che possiede il server mail.

Exchange - Utilizzo licenza mensile

Fornisce informazioni dettagliate relative all'utilizzo della licenza Security for Exchange per le aziende da te gestite in un determinato periodo di tempo.

La tabella sotto il grafico fornisce dettagli relativi al nome dell'azienda, codici di licenza, mese e numero mailbox protette, appartenenti a ciascuna delle tue aziende gestite.

Il numero di utilizzo della licenza per un'azienda è collegato a una nuova finestra, in cui è possibile trovare informazioni dettagliate sull'uso, come domini in licenza in quella società e le relative mailbox.

Exchange - Top 10 malware rilevati

Ti informa sulle 10 minacce malware più rilevate negli allegati email. Puoi generare due visualizzazioni contenenti statistiche diverse. Una visualizzazione mostra il numero di rilevamenti dai destinatari interessati e una dai mittenti.

Per esempio, GravityZone ha rilevato un'email con un allegato infetto inviata a cinque destinatari.

- Nella visualizzazione dei destinatari:
  - Il rapporto mostra cinque rilevamenti.
  - I dettagli del rapporto mostrano solo i destinatari, non i mittenti.
- Nella visualizzazione dei mittenti:
  - Il rapporto mostra una rilevazione.
  - I dettagli del rapporto mostrano solo il mittente, non i destinatari.

Oltre alla combinazione mittente/destinatari e il nome del malware, il rapporto fornisce anche i seguenti dettagli:

- Il tipo di malware (virus, spyware, PUA, ecc.)
- Il server in cui la minaccia è stata rilevata.
- Le misure intraprese dal modulo antimalware.
- Data e ora dell'ultimo rilevamento.

Exchange - Top 10 destinatari malware

Ti mostra i 10 destinatari email più colpiti dai malware in un determinato intervallo di tempo.

I dettagli del rapporto ti forniscono l'intero elenco dei malware che hanno colpito tali destinatari, oltre alle azioni intraprese.

Exchange - Top 10 destinatari spam

Ti mostra i 10 destinatari email più colpiti per numero di email spam o phishing rilevate in un determinato intervallo di tempo. Il rapporto fornisce informazioni anche sulle azioni intraprese alle rispettive email.

8.2. Creare i rapporti

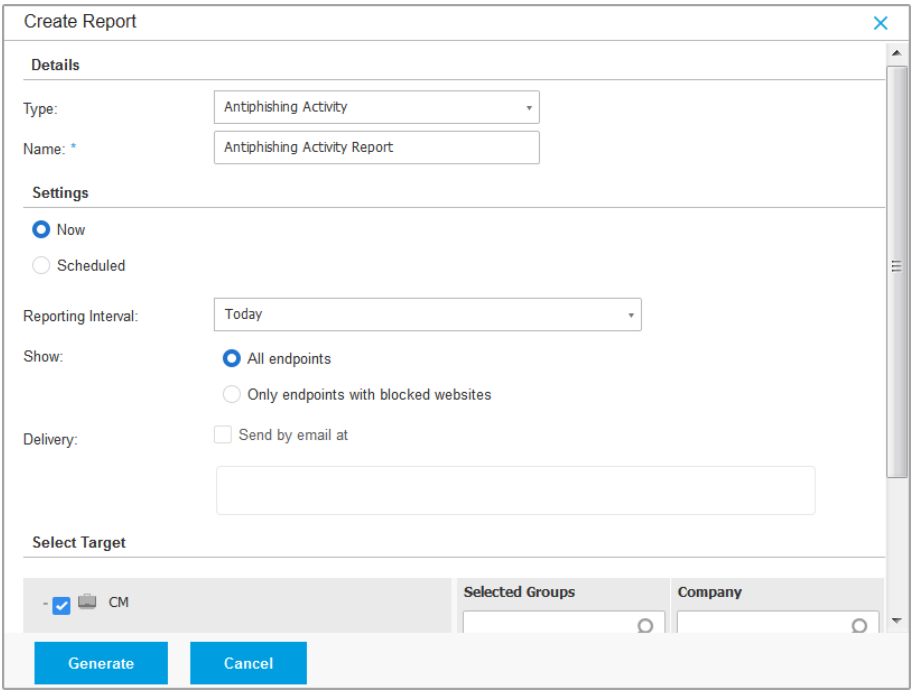
Puoi creare due categorie di rapporti:

- **Rapporti istantanei.** I rapporti istantanei vengono mostrati automaticamente dopo averli generati.
- **Rapporti programmati.** I rapporti programmati possono essere configurati per essere eseguiti periodicamente, in una determinata ora e data. Un elenco di tutti i rapporti programmati viene mostrato nella pagina **Rapporti**.

Importante
I rapporti istantanei vengono eliminati automaticamente alla chiusura della pagina del rapporto. I rapporti programmati vengono salvati e mostrati nella pagina **Rapporti**.

Per creare un rapporto:

1. Vai alla pagina **Rapporti**.
2. Clicca sul pulsante **Aggiungi** nel lato superiore della tabella. Apparirà una finestra di configurazione.



3. Seleziona il tipo di rapporto desiderato dal menu. Per maggiori informazioni, fai riferimento a «Tipo di rapporto» (p. 101)
4. Inserisci un nome specifico per il rapporto. Scegliendo un nome, considera il tipo e il bersaglio del rapporto, e possibilmente le opzioni del rapporto.
5. Configura la ricorrenza del rapporto:
   - Seleziona **Ora** per creare un rapporto istantaneo.
   - Seleziona **Programmato** per configurare la generazione automatica del rapporto nell'intervallo di tempo desiderato:
     - Orario, nell'intervallo specificato tra le ore.
     - Giornaliero. In questo caso, puoi anche impostare l'ora di inizio (ora e minuti).

- Settimanale, nei giorni della settimana indicati e all'orario di inizio selezionato (ora e minuti).
- Mensile, nel giorno del mese indicato e all'orario di inizio selezionato (ora e minuti).

6. Per la maggior parte dei tipi di rapporto devi indicare l'intervallo di tempo a cui si riferiscono i dati contenuti. Il rapporto mostrerà solo i dati di quel periodo di tempo selezionato.
7. Diversi tipi di rapporto offrono opzioni di filtraggio per aiutarti a trovare facilmente le informazioni di tuo interesse. Usa le opzioni di filtraggio nella sezione **Mostra** per ottenere solo le informazioni desiderate.

   Per esempio, per un rapporto di **Stato aggiornamento**, puoi scegliere di visualizzare solo l'elenco degli elementi di rete che non sono stati aggiornati, o quelli che devono essere riavviati per completare l'aggiornamento.
8. **Consegna**. Per ricevere un rapporto programmato via email, seleziona la casella corrispondente. Inserisci gli indirizzi email desiderati nel campo sottostante. Di norma, l'email contiene un archivio con entrambi i file del rapporto (PDF e CSV). Usa le caselle nella sezione **Allega file** per personalizzare il tipo di file e come inviarli via email.
9. **Seleziona bersaglio**. Scorri in basso per configurare il bersaglio del rapporto. Seleziona uno o più gruppi di endpoint che vuoi includere nel rapporto.
10. In base alla ricorrenza selezionata, clicca su **Genera** per creare un rapporto istantaneo o **Salva** per creare un rapporto programmato.
    - Il rapporto istantaneo sarà visualizzato immediatamente dopo aver cliccato su **Genera**. Il tempo richiesto per la creazione dei rapporti potrebbe variare in base al numero di elementi di rete gestiti. Attendi la creazione del rapporto richiesto.
    - Il rapporto programmato sarà mostrato nell'elenco della pagina **Rapporti**. Una volta generata l'istanza del rapporto, puoi visualizzare il rapporto cliccando sul link corrispondente nella colonna **Vedi rapporto** nella pagina **Rapporti**.

8.3. Visualizzare e gestire i rapporti programmati

Per visualizzare e gestire i rapporti programmati, vai alla pagina **Rapporti**.

La pagina dei rapporti

Tutti i rapporti programmati vengono mostrati in una tabella con una serie di informazioni utili al riguardo:

- Nome e tipo del rapporto
- Ricorrenza del rapporto
- Ultima istanza generata.

Nota
I rapporti programmati sono disponibili solo per l'utente che li ha creati.

Per ordinare i rapporti in base a una determinata colonna, clicca semplicemente sull'intestazione della colonna. Clicca nuovamente sull'intestazione della colonna per modificare l'ordine selezionato.

Per trovare facilmente ciò che stai cercando, usa le caselle di ricerca o le opzioni di filtraggio sotto le intestazioni della colonna.

Per cancellare il contenuto di una casella di ricerca, posiziona il cursore su di essa e clicca sull'icona × **Elimina**.

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

8.3.1. Visualizza rapporti

Per visualizzare un rapporto:

1. Vai alla pagina **Rapporti**.
2. Ordina i rapporti per nome, tipo o ricorrenza per trovare facilmente il rapporto che stai cercando.
3. Clicca sul link corrispondente nella colonna **Vedi rapporto** per mostrare il rapporto. Sarà mostrata l'istanza del rapporto più recente.

   Per visualizzare tutte le istanze di un rapporto, fai riferimento a«Salvare i rapporti» (p. 123)

Tutti i rapporti hanno una sezione di sommario (la metà superiore della pagina del rapporto) e una di dettagli (la metà inferiore della pagina del rapporto).

- La sezione del sommario fornisce dati statistici (grafici e diagrammi) per tutti gli elementi della rete bersaglio, oltre a informazioni generali sul rapporto, come il periodo interessato (ove applicabile), il bersaglio del rapporto, ecc.
- La sezione dei dettagli fornisce informazioni su ciascun elemento di rete bersaglio.

Nota

- Per configurare le informazioni mostrate dal grafico, clicca sui valori della legenda così da mostrare o nascondere i dati selezionati.
- Clicca sull'area grafica (sezione del diagramma, barra) di tuo interesse per visualizzare i relativi dettagli nella tabella.

8.3.2. Modificare i rapporti programmati

Nota
Quando si modifica un rapporto programmato, ogni aggiornamento sarà applicato a partire dalla prossima ricorrenza del rapporto. I rapporti generati in precedenza non saranno influenzati dalla modifica.

Per modificare le impostazioni di un rapporto programmato:

1. Vai alla pagina **Rapporti**.
2. Clicca sul nome del rapporto.
3. Modifica le impostazioni del rapporto in base alle esigenze. Puoi modificare:
   - **Nome del rapporto**. Seleziona un nome specifico per il rapporto, così da identificarne facilmente le caratteristiche. Scegliendo un nome, considera il tipo e il bersaglio del rapporto, e possibilmente le opzioni del rapporto. I rapporti generati da un rapporto programmato vengono chiamati allo stesso modo.
   - **Ricorrenza del rapporto (programma)**. Puoi programmare il rapporto per essere generato automaticamente a cadenza oraria (in un determinato intervallo orario), giornaliera (in una determinata ora di inizio), settimanale (in una determinata giornata della settimana e ora di inizio) o mensile (in una determinata giornata del mese e ora di inizio). In base al programma

selezionato, il rapporto includerà dati rispettivamente solo dell'ultimo giorno, settimana o mese.

- **Impostazioni**
  - Puoi programmare il rapporto per essere generato automaticamente a cadenza oraria (in un determinato intervallo orario), giornaliera (in una determinata ora di inizio), settimanale (in una determinata giornata della settimana e ora di inizio) o mensile (in una determinata giornata del mese e ora di inizio). In base al programma selezionato, il rapporto includerà dati rispettivamente solo dell'ultimo giorno, settimana o mese.
  - Il rapporto includerà solo i dati dell'intervallo di tempo selezionato. Puoi modificare l'intervallo a partire dalla prossima ricorrenza.
  - La maggior parte dei rapporti forniscono opzioni di filtraggio per aiutarti a trovare facilmente le informazioni che ti interessano. Visualizzando il rapporto nella console, tutte le informazioni saranno disponibili, indipendentemente dalle opzioni selezionate. Tuttavia, se scarichi il rapporto o lo invii via email, nel file PDF saranno incluse solo le informazioni selezionate e il sommario del rapporto. I dettagli del rapporto saranno disponibili solo in formato CSV.
  - Puoi scegliere di ricevere il rapporto via email.
- **Seleziona bersaglio**. L'opzione selezionata indica il tipo di bersaglio del rapporto attuale (gruppi o singoli elementi della rete). Clicca sul link corrispondente per visualizzare il bersaglio del rapporto attuale. Per modificarlo, seleziona i gruppi o gli elementi di rete da includere nel rapporto.

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

8.3.3. Eliminare i rapporti programmati

Quando un rapporto programmato non è più necessario, è meglio eliminarlo. Eliminare un rapporto programmato cancellerà tutte le istanze che ha generato automaticamente fino a quel momento.

Per eliminare un rapporto programmato:

1. Vai alla pagina **Rapporti**.
2. Seleziona il rapporto che vuoi eliminare.
3. Clicca sul pulsante ⊖ **Elimina** nel lato superiore della tabella.

8.4. Salvare i rapporti

Di norma, i rapporti programmati vengono salvati automaticamente in Control Center.

Se hai bisogno di avere a disposizione i rapporti per periodi di tempo superiori, puoi salvarli nel computer. Il sommario del rapporto sarà disponibile in formato PDF, mentre i dettagli del rapporto saranno disponibili solo in formato CSV.

Hai due modi per salvare i rapporti:

- Esporta
- Download

8.4.1. Esportare i rapporti

Per esportare il rapporto sul tuo computer:

1. Seleziona un formato e clicca su **Esporta CSV** o **Esporta PDF**.
2. In base alle impostazioni del tuo browser, il file potrebbe essere scaricato automaticamente in un percorso di download predefinito, oppure si aprirà una finestra di download, in cui devi specificare la cartella di destinazione.

8.4.2. Scaricare i rapporti

Un archivio del rapporto include sia il sommario del rapporto che i suoi dettagli.

Per scaricare un archivio del rapporto:

1. Vai alla pagina **Rapporti**.
2. Seleziona il rapporto che vuoi salvare.
3. Clicca sul pulsante **Scarica** e seleziona **Ultima istanza** per scaricare l'ultima istanza generata dal rapporto o **Archivio completo** per scaricare un archivio contenente tutte le istanze.

   In base alle impostazioni del tuo browser, il file potrebbe essere scaricato automaticamente in un percorso di download predefinito, oppure si aprirà una finestra di download, in cui devi specificare la cartella di destinazione.

8.5. Inviare i rapporti via email

Puoi inviare i rapporti via email usando le seguenti opzioni:

1. Per inviare via e-mail il rapporto che stai visualizzando, clicca sul pulsante **E-mail**. Il rapporto sarà inviato all'indirizzo e-mail associato al tuo account.
2. Per configurare l'invio via email dei rapporti programmati desiderati:
   a. Vai alla pagina **Rapporti**.
   b. Clicca sul nome del rapporto desiderato.
   c. In **Impostazioni > Consegna**, seleziona **Invia per e-mail a**.
   d. Inserisci l'indirizzo e-mail desiderato nel campo sottostante. Puoi aggiungere quanti indirizzi e-mail desideri.
   e. Clicca su **Salva**.

> **Nota**
> Solo il sommario del rapporto e il grafico saranno inclusi nel file PDF inviato via email. I dettagli del rapporto saranno disponibili nel file CSV.

I rapporti vengono inviati via email come archivi .zip.

8.6. Stampare i rapporti

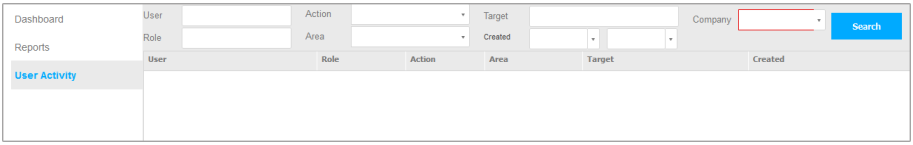
Control Center non supporta attualmente la funzionalità del pulsante Stampa. Per stampare un rapporto, prima è necessario salvarlo sul proprio computer.

9. RAPPORTO ATTIVITÀ UTENTE

Control Center registra tutte le operazioni e azioni eseguite dagli utenti in un rapporto. L'elenco delle attività dell'utente include i seguenti eventi, in base al tuo livello di permesso amministrativo:

- Accedere e uscire
- Creare, modificare, rinominare ed eliminare i rapporti
- Aggiungere e rimuovere i portlet della dashboard
- Avviare, terminare, annullare e bloccare processi di risoluzione dei problemi sulle macchine interessate
- Modificare le impostazioni di autenticazione per gli account di GravityZone.

Per esaminare i valori delle attività dell'utente, vai alla pagina**Attività utente**.



La pagina attività utente

Per mostrare gli eventi registrati a cui sei interessato, devi definire una ricerca. Inserisci i criteri di ricerca nei campi disponibili e clicca sul pulsante **Cerca**. Tutte le voci che corrispondono ai tuoi criteri saranno mostrate nella tabella.

Le colonne della tabella di forniscono alcune informazioni utili sugli eventi elencati:

- Il nome utente di chi ha eseguito l'azione.
- Ruolo dell'utente.
- L'azione che ha causato l'evento.
- Il tipo di elemento della console influenzato dall'azione.
- Lo specifico elemento della console influenzato dall'azione.
- Il momento in cui si è verificato l'evento.

Per ordinare gli eventi in base a una determinata colonna, clicca semplicemente sull'intestazione di quella colonna. Cliccaci nuovamente per invertire l'ordine selezionato.

Per visualizzare informazioni dettagliate su un evento, selezionalo e controlla la sezione sotto la tabella.

10. OTTENERE AIUTO

Per eventuali problemi o domande relative a GravityZone, contatta un amministratore.

10.1. 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.

A. Appendici

A.1. Oggetti Sandbox Analyzer

A.1.1. 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.1.2. 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.1.3. Eccezioni predefinite all'invio automatico

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

Glossario

Adware

La modalità adware è spesso combinata con un'applicazione che viene fornita gratuitamente se l'utente accetta l'adware. Considerando che le applicazioni adware vengono di solito installate dopo che l'utente ha accettato l'accordo di licenza, dove viene spiegato il proposito dell'applicazione, non viene commessa alcuna infrazione.

Comunque, le finestre pop-up di avvertimento possono essere fastidiose e in alcuni casi ridurre le prestazioni del sistema. Inoltre, le informazioni che vengono raccolte da alcune di queste applicazioni possono causare inconvenienti riguardo la privacy degli utenti, non sempre completamente informati sui termini dell'accordo di licenza.

Aggiornamento

Una nuova versione di un prodotto software o hardware creato per sostituire la versione precedente. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul computer, diversamente non sarà possibile installare l'aggiornamento.

Bitdefender ha un proprio modulo di aggiornamento che consente la verifica manuale degli aggiornamenti oppure l'aggiornamento automatico del prodotto.

Archivio

Un Disco, un nastro o una cartella che contiene file memorizzati.

Un file che contiene uno o più file in forma compressa.

Area di notifica

Introdotta con Windows 95, l'area di notifica è situata nella barra delle applicazioni di Windows (in genere in basso vicino all'orologio) e contiene icone miniaturizzate per un accesso veloce a funzioni di sistema come fax, stampante, modem, volume e molto altro. Clicca due volte o clicca con il pulsante destro su un'icona per visualizzare e accedere ai dettagli e i controlli.

Attacchi mirati

Gli attacchi informatici che puntano principalmente a guadagni finanziari o a rovinare una reputazione. Il bersaglio può essere un individuo, un'azienda, un

software o un sistema, ben studiato prima che l'attacco avvenga. Questi attacchi vengono eseguiti per un lungo periodo di tempo e per fasi, usando uno o più punti d'infiltrazione. Vengono notati difficilmente, e la maggior parte delle volte quando il danno è già stato fatto.

Backdoor

Una breccia nella sicurezza di un sistema deliberatamente lasciata dal programmatore o dal manutentore. La presenza di tali "brecce" non sempre è dolosa: su alcuni sistemi operativi, ad esempio, vengono utilizzate per l'accesso con utenze privilegiate per servizi tecnici o per i programmatori del produttore a scopo di manutenzione.

Bootkit

Un bootkit è un programma dannoso che ha la capacità di infettare il master boot record (MBR), il volume boot record (VBR) o il settore di boot. Il bootkit resta attivo anche dopo un riavvio del sistema.

Browser

Abbreviazione di browser web, un'applicazione software utilizzata per localizzare e visualizzare pagine web.

Cookie

Nell'industria di Internet, i cookie vengono descritti come piccoli file contenenti informazioni relative ai computer individuali che possono essere analizzate e utilizzate dai pubblicitari per tenere traccia di interessi e gusti online degli utenti. In questo settore, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di fornire offerte pubblicitarie personalizzate in base agli interessi degli utenti. Per molte persone è una lama a doppio taglio, poiché da una parte è efficace e consente di far vedere solo ciò che viene dichiarato interessante. Ma dall'altra, implica in effetti un "tracciamento" di dove si va e di cosa si seleziona. In considerazione di questo è in atto un dibattito relativo alla riservatezza e molte persone si sentono offese all'idea di essere visti come un "codice SKU" (il codice a barre sul retro delle confezioni che viene letto dalle casse). Se questo punto di vista può essere considerato estremo, in alcuni casi può essere corretto.

Estensione del nome di un file

Porzione del nome di un file che segue il punto finale e che indica il tipo di dati inclusi nel file.

Molti sistemi operativi utilizzano estensioni di file, come Unix, VMS e MS-DOS. Sono normalmente composti da una a tre lettere (alcuni vecchi sistemi operativi non ne supportano più di tre). Esempi: "c" per codici sorgente C, "ps" per PostScript, "txt" per testi semplici.

Euristico

Un metodo basato su regole per l'identificazione di nuovi virus. Questo metodo di scansione non si basa su specifiche firme dei virus. Il vantaggio della scansione euristica è di non essere ingannata dalle nuove varianti dei virus esistenti. Tuttavia, può occasionalmente segnalare una parte di codice sospetto in programmi normali, generando i cosiddetti "falsi positivi".

Eventi

Un'azione oppure un evento segnalato da un programma. Gli eventi possono essere azioni dell'utente, come cliccare con il mouse o premere un tasto sulla tastiera, oppure del sistema, come l'esaurimento della memoria.

Exploit

In genere, un exploit è un qualsiasi metodo usato per ottenere accesso non autorizzato ai computer o una vulnerabilità nella sicurezza di un sistema che rende vulnerabile il sistema a un attacco.

Falso positivo

Appare quando un prodotto di analisi antivirus individua un documento come infettato quando di fatto non lo è.

File di rapporto

Un file che elenca le azioni avvenute. Bitdefender crea un rapporto che elenca i percorsi controllati, le cartelle, il numero di archivi e file esaminati, oltre a quanti file infetti e sospetti sono stati trovati.

File sospetti e traffico di rete

I file sospetti sono quelli con una reputazione piuttosto dubbia. Questa classifica è data da molti fattori, tra cui: l'esistenza della firma digitale, il numero di occorrenze nelle reti di computer, il packer usato, ecc. Il traffico di rete viene considerato sospetto quando si discosta dal modello. Per esempio, una sorgente inaffidabile, richieste di connessione a porte insolite, un maggiore uso della banda, tempi di connessione casuali, ecc.

Firma malware

Le firme malware sono frammenti di codice estratti da campioni attuali di malware. Sono usate dai programmi antivirus per eseguire confronti di esempi e rilevare i malware. Le firme vengono usate anche per rimuovere il codice malware dai file infetti.

Il database di firme malware di Bitdefender è una raccolta di firme malware aggiornato continuamente dai ricercatori malware di Bitdefender.

Grayware

Una classe di applicazioni software tra software legittimi e malware. Anche se non sono dannosi come i malware che possono influenzare l'integrità del sistema, il loro comportamento è comunque fastidioso, portando a situazioni non desiderate, come furto di dati, uso non autorizzato e pubblicità non gradita. Le applicazioni grayware più comuni sono spyware e adware.

IP

Internet Protocol – protocollo di instradamento nella suite di protocollo TCP/IP, responsabile dell'indirizzamento IP, dell'instradamento, della frammentazione e della ricomposizione dei pacchetti IP.

Keylogger

Un keylogger è un'applicazione che registra ogni informazione digitata.

I keylogger non sono dannosi di natura. Possono essere usati anche per scopi legittimi, come monitorare le attività di dipendenti o bambini. Tuttavia, sono utilizzati anche dai criminali informatici per scopi dannosi (per esempio, ottenere dati personali, come credenziali o codici di accesso).

Linea di comando

In un'interfaccia a linea di comando, l'utente digita i comandi nello spazio previsto direttamente sullo schermo, utilizzando il linguaggio di comando.

Livelli di protezione

GravityZone fornisce protezione attraverso una serie di moduli e ruoli, collettivamente denominati livelli di protezione, suddivisi in Protezione per Endpoint (EPP) o protezione principale, e vari componenti aggiuntivi. La Protezione per Endpoint include Antimalware, Advanced Threat Control, Advanced Anti-Exploit, Firewall, Controllo contenuti, Controllo dispositivi, Network Attack Defense, Utente esperto e Relay. Gli add-on includono diversi livelli di protezione come Security for Exchange e Sandbox Analyzer.

Per maggiori dettagli sui livelli di protezione disponibili con la tua soluzione GravityZone, fai riferimento a «Livelli di protezione di GravityZone» (p. 2).

Macro virus

Un tipo di virus informatico, codificato come macro all'interno di un documento. Molte applicazioni, come ad esempio Microsoft Word ed Excel, supportano potenti linguaggi macro.

Queste applicazioni consentono di codificare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Malware

Malware è un termine generico per software progettati appositamente per essere dannosi, un'abbreviazione di "software dannoso" (in inglese "malicious software"). Non è ancora usato in maniera universale, ma la sua popolarità come termine generale per indicare virus, Trojan, worm e codice mobile dannoso sta aumentando.

Malware

Un programma o parte di codice caricato sul computer a propria insaputa e che viene eseguito contro la propria volontà. La maggior parte dei virus è anche in grado di auto replicarsi. Tutti i virus informatici sono creati dall'uomo. È relativamente facile produrre un semplice virus in grado di copiare sé stesso innumerevoli volte. Persino un virus così semplice è pericoloso in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di virus ancora più pericoloso è quello in grado di trasmettere sé stesso attraverso le reti superando i sistemi di sicurezza.

Non euristico

Questo metodo di scansione si basa su specifiche firme di virus. Il vantaggio della scansione non-euristica è di non essere ingannata da ciò che potrebbe sembrare un virus, e quindi non genera falsi allarmi.

Phishing

L'atto d'inviare un'e-mail a un utente fingendo di essere una società legittima e affermata, nel tentativo di truffarlo, facendogli cedere informazioni private che saranno usate per furti d'identità. L'e-mail invita gli utenti a visitare un sito web, dove gli sarà chiesto di aggiornare determinate informazioni personali, come password e numero di carta di credito, codice fiscale o coordinate

bancarie, che l'azienda legittima ovviamente possiede già. In ogni caso, la pagina web è falsa e creata solo per rubare i dati personali dell'utente.

Porta

Un'interfaccia su un computer dalla quale è possibile connettere un dispositivo. I personal computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, monitor e tastiere. Esternamente i personal computer hanno porte per la connessione di modem, stampanti, mouse e altre periferiche.

Nelle reti TCP/IP e UDP, un endpoint per una connessione logica. Il numero della porta ne identifica il tipo. Ad esempio, la porta 80 viene usata per il traffico HTTP.

Programma di download Windows

È il nome generico di un programma che ha come funzionalità principale quella di scaricare contenuti a scopi indesiderati o dannosi.

Ransomware

Un malware che ti isola dal tuo computer o blocca l'accesso ai tuoi file e applicazioni. Un ransomware ti chiederà di pagare un determinato costo (riscatto), in cambio di una chiave di decifrazione che ti consente di riottenere l'accesso al tuo computer o ai tuoi file.

Rootkit

Un rootkit è una serie di strumenti software che consente di accedere a un sistema come amministratore. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la propria presenza, in modo da non essere visti dagli amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, gli accessi e i registri. Se incorporano il software adeguato, possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche.

I rootkit non sono dannosi per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando i rootkit. Comunque, vengono principalmente utilizzati per nascondere malware o per celare la presenza di un intruso nel sistema. Se combinati ai malware, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare

il traffico, creare backdoor nel sistema, alterare file e registri, ed evitare il rilevamento.

Script

Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Settore di avvio:

Un settore all'inizio di ogni disco che ne identifica l'architettura (dimensione del settore, dimensione del cluster, ecc.). Nei dischi di avvio, il settore di boot contiene anche un programma che carica il sistema operativo.

Sottrazione di password

Un password stealer raccoglie parti di dati che possono essere nomi di account e le relative password. Tali credenziali rubate vengono poi usate per scopi dannosi, come il furto di account.

Spam

Messaggi di posta elettronica o newsgroup indesiderati. Generalmente conosciuto come e-mail non desiderate.

Spyware

Qualsiasi software che raccoglie segretamente informazioni dell'utente tramite la sua connessone a Internet, senza che questo se ne accorga, di solito per scopi pubblicitari. Le applicazioni spyware in genere sono incluse come componente nascosta di programmi freeware o shareware, che possono essere scaricati da Internet. Tuttavia, occorre segnalare che la maggioranza delle applicazioni shareware o freeware non includono alcun programma spyware. Una volta installato, uno spyware monitora le attività dell'utente su Internet e trasmette di nascosto tali informazioni a qualcun altro. Gli spyware possono anche raccogliere informazioni su indirizzi e-mail o addirittura password e numeri di carta di credito.

Gli spyware sono simili a un cavallo di Troia che gli utenti installano inconsapevolmente con altre applicazioni. Un modo comune per diventare vittima degli spyware è utilizzare i programmi peer-to-peer attuali per condividere e scaricare file.

Oltre a questioni di etica e privacy, gli spyware sottraggono risorse di memoria al computer, "mangiandosi" larghezza di banda poiché inviano informazioni alla propria "base" usando la connessione internet dell'utente. Poiché gli

spyware utilizzano memoria e risorse del sistema, le applicazioni eseguite in background possono provocare instabilità o blocchi del sistema.

Storm di scansione antimalware

Un intenso uso delle risorse del sistema che si verifica quando un software antivirus esamina contemporaneamente più virtual machine su un solo host fisico.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di rete largamente utilizzati su Internet, che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il relativo traffico.

Trojan

Un programma distruttivo che si maschera da applicazione benevola. Diversamente dai virus, i cavalli di Trojan non si replicano ma possono comunque essere altrettanto distruttivi. Un tipo di cavallo di Troia particolarmente insidioso è un programma che dichiara di pulire i virus dal computer, ma al contrario li introduce.

Il termine deriva da una storia dell'Iliade di Omero, in cui i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e conquistare Troia.

Virus di boot

Un virus che infetta il settore di avvio di un disco rigido oppure di un'unità floppy. Qualsiasi tentativo di effettuare il boot da un disco floppy infettato con un virus di boot, farà sì che il virus venga attivato in memoria. Da quel momento in poi, ogni volta che si esegue il boot del sistema, il virus sarà attivo in memoria.

Virus polimorfico

Un virus che modifica la propria forma con ogni file che infetta. Non avendo caratteristiche binarie costanti, questi virus sono difficili da identificare.

Worm

Un programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.