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

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

GravityZone offre livelli di sicurezza multipli per gli endpoint: antimalware con monitoraggio comportamentale, protezione da minacce zero-day, blacklist delle applicazioni e sandbox, firewall, controllo dei dispositivi e dei contenuti.

2. LIVELLI DI PROTEZIONE DI GRAVITYZONE

GravityZone ti offre i seguenti livelli di protezione:

- Antimalware
- Advanced Threat Control
- Anti-exploit avanzato
- Firewall
- Controllo contenuti
- Patch Management
- Controllo dispositivi
- Full Disk Encryption
- 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. 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.

2.4. 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.

2.5. 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.

2.6. 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.

2.7. 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.

2.8. 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.).

2.9. 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.

2.10. 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.

2.11. 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.

2.12. 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)
- Agenti di sicurezza

3.1. 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

3.1.1. 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
- Firewall
- Controllo contenuti
- Network Attack Defense
- Patch Management
- Controllo dispositivi
- Full Disk Encryption
- 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 reti distribuite, gli agenti relay aiutano a ridurre il consumo di banda, prevenendo agli endpoint protetti di connettersi direttamente a GravityZone.

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

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

- Scoprire tutti gli endpoint non protetti nella rete.
- 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.

3.1.2. 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

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.

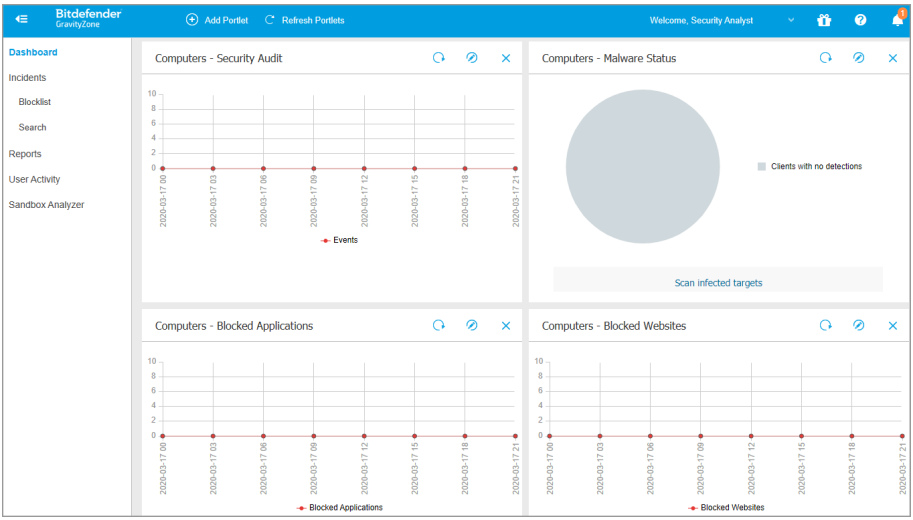
Al primo accesso, devi accettare le Condizioni d'uso di Bitdefender. Clicca su **Continua** per iniziare a usare GravityZone.

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.

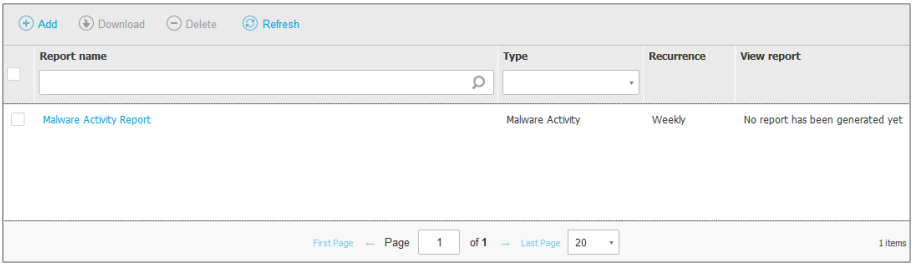
- **Uscita**. Clicca su questa opzione per uscire dal tuo account.

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

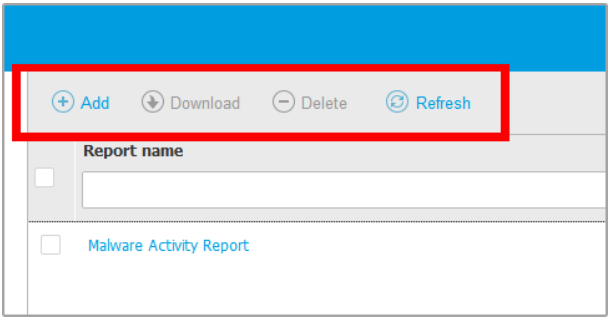
Per assicurarsi che la console mostri i dati più aggiornati, clicca sul pulsante **Aggiorna** nel lato superiore della tabella.

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:

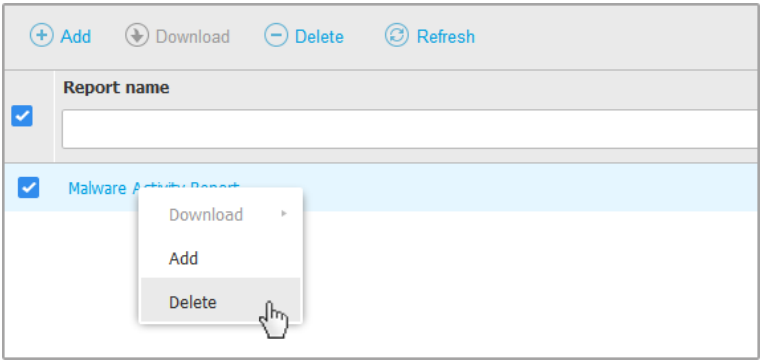
- Crea un nuovo rapporto.
- Scarica un rapporto programmato.
- Elimina un rapporto programmato.



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.

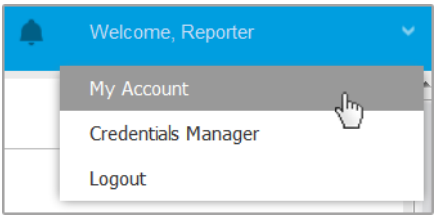
Per modificare la password di accesso:

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
Il tuo amministratore aziendale può rendere obbligatoria l'autenticazione a due fattori per tutti gli account di GravityZone. In questo caso, all'accesso ti

sarà chiesto di configurare la tua 2FA. Allo stesso tempo, non potrai disattivare la 2FA per il tuo account, finché questa funzionalità viene applicata dal tuo amministratore aziendale.
Tieni presente che, se la 2FA attualmente configurata viene disattivata per il tuo account, il codice segreto non sarà più valido.

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

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

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

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

Nota
Non puoi eliminare il tuo account personale.

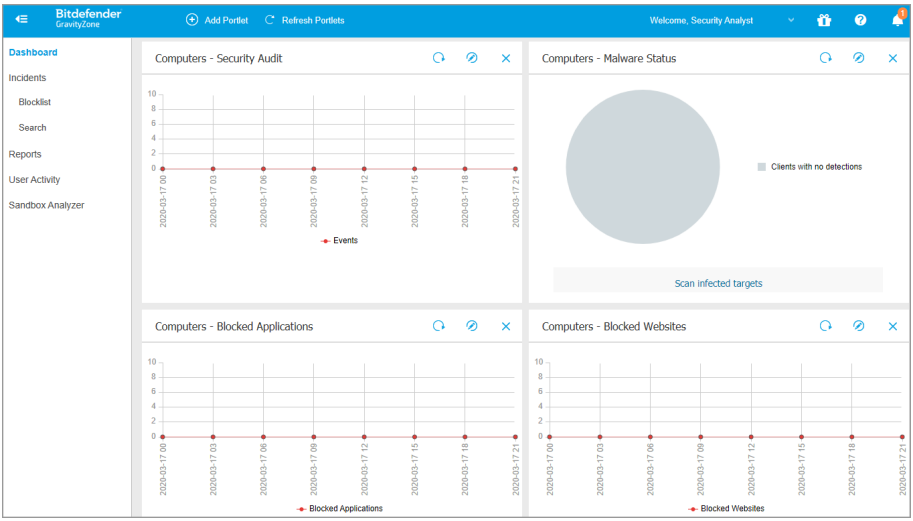
5. INTERFACCIA DI MONITORAGGIO

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.

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 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. 27).
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

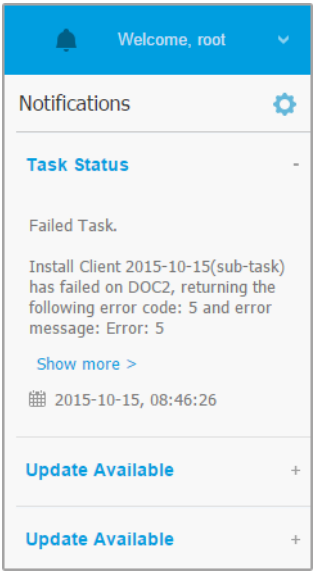
Puoi riorganizzare i portlet della dashboard per adattarsi meglio alle tue esigenze. Per riorganizzare i portlet:

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. 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.

6.1. 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.

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. 24).

Accesso da nuovo dispositivo

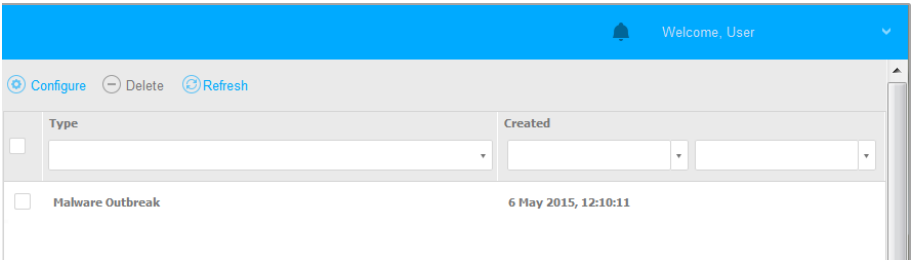
Questa notifica ti informa che il tuo account GravityZone è stato usato per accedere a Control Center da un dispositivo che finora non hai mai utilizzato a tale scopo. La notifica viene configurata automaticamente per essere visibile sia in Control Center che via e-mail, e solo tu potrai visualizzarla.

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.

6.2. 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.

6.3. 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.

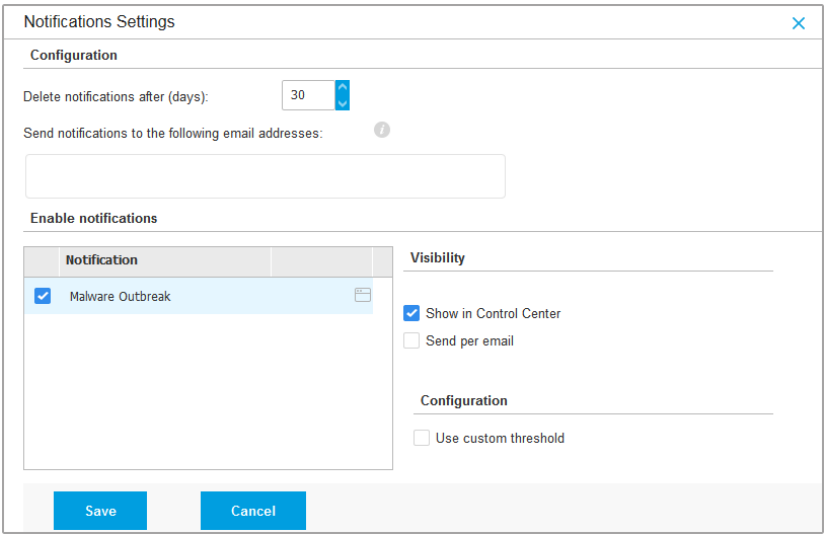
Puoi anche configurare le notifiche per essere eliminate automaticamente dopo un determinato numero di giri. Per maggiori informazioni, fai riferimento a «Configurare le impostazioni di scansione» (p. 24).

6.4. 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. 22). 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**.

7. 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).

7.1. Tipo di rapporto

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

Attività antiphishing

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

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

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.

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.

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
-
-
-
-
- Eventi di Network Attack Defense

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.

Stato dell'Aggiornamento

Ti mostra lo stato di aggiornamento dell'agente di sicurezza installato 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.

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.

7.2. Creare i rapporti

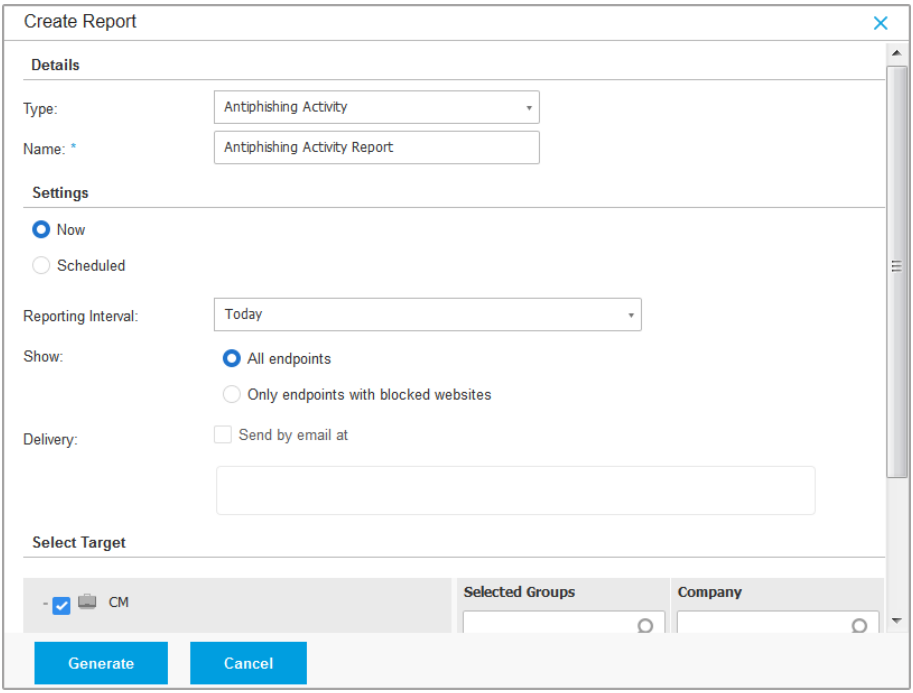
Puoi creare due categorie di rapporti:

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

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

Per creare un rapporto:

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



Opzioni rapporto

3. Seleziona il tipo di rapporto desiderato dal menu. Per maggiori informazioni, fai riferimento a «Tipo di rapporto» (p. 27).
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).

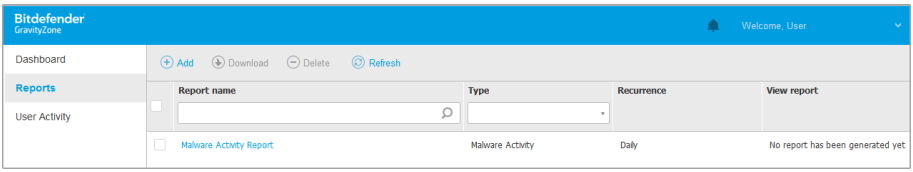
- Settimanale, nei giorni della settimana indicati e all'orario di inizio selezionato (ora e minuti).
- Mensile, nel giorno del mese indicato e all'orario di inizio selezionato (ora e minuti).

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**.

7.3. 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.

7.3.1. 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. 37)

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.

7.3.2. 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.

7.3.3. 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.

7.4. 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

7.4.1. 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.

7.4.2. 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.

7.5. 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.

7.6. Stampare i rapporti

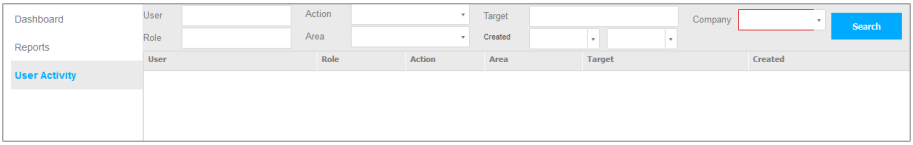
Control Center non supporta attualmente la funzionalità del pulsante Stampa. Per stampare un rapporto, prima è necessario salvarlo sul proprio computer.

8. 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.

9. OTTENERE AIUTO

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

9.1. 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.

Il modo più semplice per raggiungere la documentazione è dalla pagina **Aiuto e supporto** di Control Center. 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.

Puoi anche consultare e scaricare la documentazione nel Centro di supporto, nella sezione **Documentazione** disponibile in ciascuna pagina di supporto del prodotto.

A. Appendici

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.