Scheda tecnica

GravityZone Security EDR Cloud

Endpoint Detection and Response avanzato

I criminali informatici stanno diventando sempre più sofisticati e i loro attacchi sono sempre più difficili da rilevare. Utilizzando tecniche che individualmente sembrano comportamenti di routine, un aggressore potrebbe accedere alla tua infrastruttura e restare nascosto per mesi, aumentando sensibilmente il rischio di una costosa violazione dei dati. Se la tua soluzione di sicurezza per endpoint non garantisce il rilevamento e la risposta sugli attacchi avanzati di cui hai bisogno, GravityZone EDR Cloud può rafforzare rapidamente ed efficacemente le tue operazioni di sicurezza.

GravityZone EDR Cloud monitora la tua rete per svelare attività sospette e fornirti gli strumenti necessari per affrontare gli attacchi informatici. Integrando le pluripremiate funzionalità di machine learning, scansione cloud e sandbox analyzer può rilevare tutte le attività che eludono i tradizionali meccanismi di prevenzione degli endpoint. Fornisce una visibilità completa su tecniche, tattiche e procedure (TTP) usate negli attacchi attivi fornendo al tempo stesso capacità di ricerca complete per determinati indicatori di compromissione (IoC), tecniche MITRE ATT&CK e altri artefatti, così da scoprire gli attacchi nella fase iniziale.

GravityZone EDR Cloud fornisce una visualizzazione innovativa e di facile comprensione con un ricco contesto e informazioni sulle minacce, che aiutano il personale IT a comprendere i percorsi dell'attacco e identificare le lacune nella protezione. La visualizzazione semplifica l'indagine e la risposta, riducendo il carico lavorativo del personale IT. La Sandbox Analyzer consente al personale di eseguire automaticamente payload sospetti in un ambiente virtuale e confinato per isolare e neutralizzare i file sospetti. Le capacità di GravityZone EDR Cloud proteggono le organizzazioni dalle minacce avanzate, consentendo al tempo stesso una caccia proattiva alle minacce e un'analisi delle cause principali.

In che modo GravityZone EDR Cloud può aiutarti?

- **Rilevamento e risposta agli attacchi avanzati.** Monitora la tua rete per svelare attività sospette in anticipo e fornirti gli strumenti per consentirti di affrontare gli attacchi informatici.
- **Colmare il divario di competenze di sicurezza.** Consente ai team di rispondere in maniera efficace dando una priorità alle allerte in maniera automatica e una risposta immediata.
- **Ridurre i rischi per l'organizzazione.** Analizza continuamente la tua infrastruttura per identificare i rischi tra centinaia di fattori. Aiuta a mitigare i rischi derivanti da sistema operativo, rete e utenti.
- **Minimizzare il carico operativo.** Fornito via cloud e con scarsa manutenzione, dotato di agenti facilmente impiegabili e integrabili nella tua architettura di sicurezza esistente e pienamente compatibile con la tua soluzione antivirus per endpoint.

Bitdefender
BUILT FOR RESILIENCE

In sintesi

GravityZone EDR Cloud rileva in tempo reale le minacce avanzate, incluso attacchi privi di file, ransomware e altre minacce zero-day. La sua analisi delle minacce e il suo raccoglitore di eventi basato su cloud monitorano gli endpoint e priorizzano gli eventi di sicurezza in un elenco di incidenti per ulteriori indagini e risposte. Bitdefender EDR fornisce una visualizzazione innovativa e di facile comprensione con un ricco contesto e informazioni sulle minacce che aiutano il personale IT a comprendere i percorsi dell'attacco e identificare le lacune nella protezione. La visualizzazione semplifica l'indagine e la risposta, riducendo il carico lavorativo del personale IT.

Benefici principali

- Rilevamento leader di settore - Visibilità e rilevamento delle minacce migliorati che sfruttano i punti di forza di XDR per proteggere gli endpoint. Funzionalità di ricerca complete per determinati indicatori di compromissione (IoC), tecniche MITRE ATT&CK e altri artefatti per scoprire gli attacchi nella fase iniziale.
- Indagine e risposta mirate: la visualizzazione degli incidenti a livello organizzativo consente di rispondere in modo efficiente, limitare la diffusione laterale e fermare gli attacchi in corso.
- Massima efficienza - Il nostro agente leggero e facile da implementare garantisce massima efficienza e protezione con il minimo sforzo. Per una soluzione completamente gestita, puoi passare facilmente a Bitdefender Managed Detection and Response (MDR)

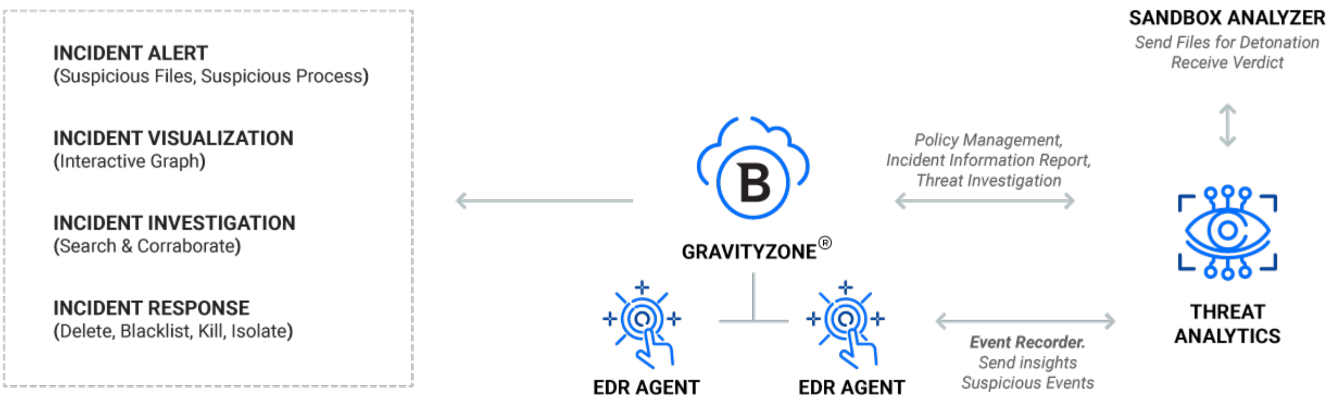
"Le capacità EDR di GravityZone ci forniscono rapporti dettagliati su come i processi vengano influenzati nell'intera sequenza dell'incidente. Ciò ci consente di risparmiare molto tempo per le indagini, poiché il lavoro manuale viene eliminato."

Sascha Neuhaus,
IT Security Officer, Louis

Innovazione per efficacia ed efficienza

La tecnologia di correlazione cross-endpoint di Bitdefender porta la visibilità e il rilevamento delle minacce a un nuovo livello sfruttando le capacità di rilevamento degli attacchi avanzati XDR che riguardano più endpoint in infrastrutture ibride (workstation, server o container, con vari SO). Estende la visibilità, le analisi e le capacità di correlazione degli eventi di EDR oltre i confini di un singolo endpoint, per consentire ai team di sicurezza di affrontare con maggiore efficacia gli attacchi informatici complessi che riguardano più endpoint. Questa tecnologia di correlazione cross-endpoint combina la granularità e il ricco contesto di sicurezza di EDR con le analisi a livello di infrastruttura di Extended Detection and Response (XDR). Fornendo una visualizzazione delle minacce a livello organizzativo, XDR aiuta le organizzazioni a concentrarsi sulle indagini e rispondere con maggiore efficacia.

Come funziona



GravityZone EDR Cloud è una soluzione fornita tramite cloud e basata sulla piattaforma di Bitdefender GravityZone XDR. Ogni agente EDR impiegato sugli endpoint della tua azienda ha un registratore di eventi che monitora costantemente l'endpoint e invia in modo sicuro approfondimenti e dettagli di eventi sospetti al Control Center centralizzato di GravityZone. Nel Control Center, il motore di correlazione cross-endpoint di Bitdefender raccoglie ed estrae gli eventi degli endpoint, generando visuali prioritarie e a livello aziendale degli incidenti di sicurezza, consentendo così agli amministratori di indagare rapidamente e rispondere con efficacia alle minacce.

Bitdefender
BUILT FOR RESILIENCE

3945 Freedom Circle
Ste 500, Santa Clara
California, 95054, USA

Bitdefender-BSG-GZ-EDRCloud-Datasheet-DEX4610-it_IT
CD-Apr/12/2022 • MD-Apr/12/2022