Bitdefender GravityZone Ultra Suite

SVELA E BLOCCA LE MINACCE ELUSIVE CON AGILITÀ E PRECISIONE

GravityZone Ultra, con Endpoint Security XDR, eccelle laddove gli altri principali prodotti EDR sono troppo complessi e fastidiosi, prevenendo, rilevando e rispondendo agevolmente ad attacchi sofisticati in grado di evadere le soluzioni anti-malware tradizionali. In un'unica e compatta suite di sicurezza, GravityZone Ultra fornisce:

- Riduzione della superficie di attacco (tramite firewall, controllo applicazioni, controllo contenuti e gestione delle patch)
- Protezione dei dati (tramite cifratura completa del disco)
- Rilevazione in pre-esecuzione ed eradicazione di malware (tramite apprendimento automatico configurabile, ispezione dei processi in tempo reale e analisi nel sandbox)
- Rilevazione automatica, facile indagine e bonifica immediata tramite il nuovo registratore di eventi per endpoint e l'analisi delle minacce in Endpoint Security XDR

Il risultato è una prevenzione costante delle minacce, un'accurata rilevazione degli incidenti e una risposta intelligente per minimizzare l'esposizione all'infezione e bloccare le violazioni.

Come suite di protezione per endpoint integrata, GravityZone Ultra assicura un livello di sicurezza costante per l'intero ambiente IT, così che gli aggressori non possano trovare endpoint scarsamente protetti da usare come punti di partenza per azioni dannose contro l'azienda. GravityZone Ultra si affida a un'architettura semplice e integrata con gestione centralizzata sia per endpoint che data center. Consente alle aziende di impiegare la soluzione di protezione per endpoint rapidamente e richiede meno sforzi amministrativi dopo l'implementazione.

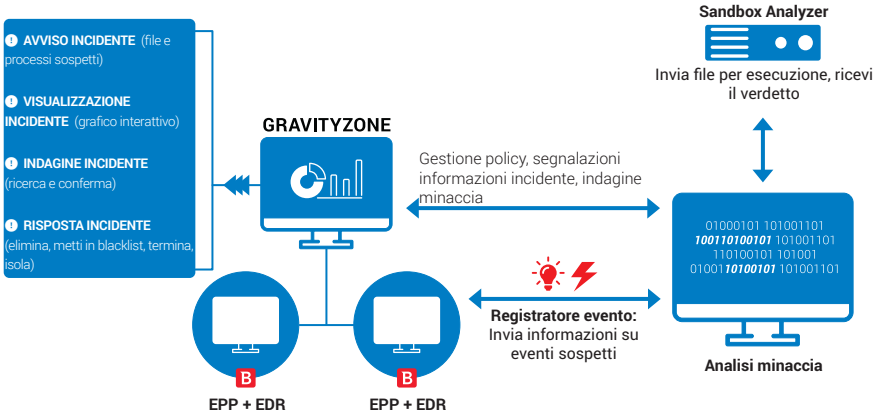


Figura 1. Bitdefender XDR: prevenzione, rilevazione e risposta in un solo agente, gestito dalla console di GravityZone.

EDR reso facile

Con una chiara visibilità degli indicatori di compromissione (IOC) e una visione immediata dei processi di ricerca delle minacce e risposta degli incidenti, GravityZone Ultra riduce i requisiti in termini di risorse e abilità per i team responsabili della sicurezza. Il nuovo registratore di dati per endpoint è un'aggiunta senza interruzioni alla struttura di protezione delle minacce esistenti e include una vasta gamma di attività del sistema (creazione file e processi, installazione programmi, caricamenti moduli, modifiche al registro, connessioni di rete, ecc.) per contribuire a una visibilità a livello aziendale sulla catena di eventi coinvolta nell'attacco.

Il modulo di analisi delle minacce opera nel cloud e filtra gli eventi comportamentali nelle attività del sistema, creando una lista di incidenti prioritari per un'ulteriore indagine e risposta.

Vantaggi principali

Espandendo le funzionalità EPP tradizionali, Endpoint Security XDR offre ai team responsabili delle analisi della sicurezza e della risposta agli incidenti gli strumenti necessari per analizzare le attività sospette e indagare, oltre che rispondere adeguatamente alle minacce avanzate:

- Visibilità endpoint in tempo reale
- Esponi le attività sospette
- Indagini immediate
- Smistamento allarmi e visualizzazione analisi incidenti
- Monitora gli attacchi e i movimenti laterali in tempo reale
- Risposta rapida
- Riduce il tempo di permanenza con risoluzione, contenimento e riparazione rapidi

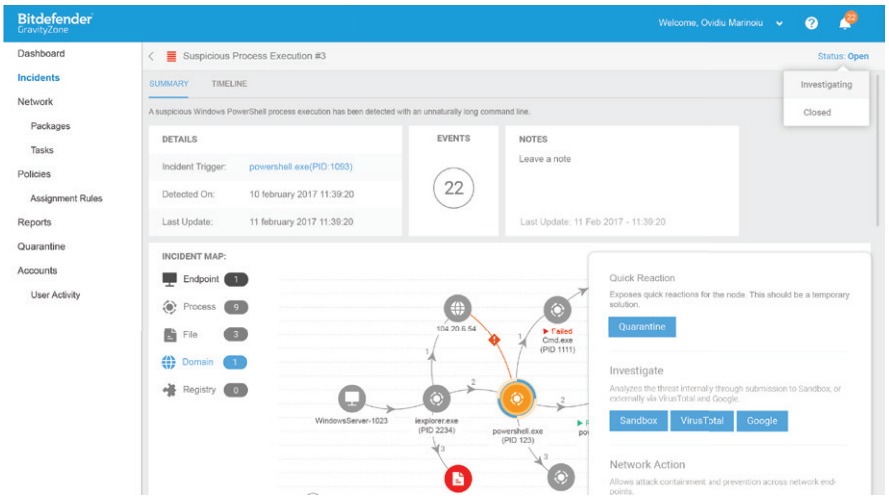


Figura 2. La pagina dei dettagli relativi all'incidente fornisce una chiara panoramica sul "raggio d'azione" degli incidenti. Il professionista può facilmente acquisire prove a supporto e rispondere.

Migliora la visione della sicurezza. Evita gli sforzi sugli allarmi.

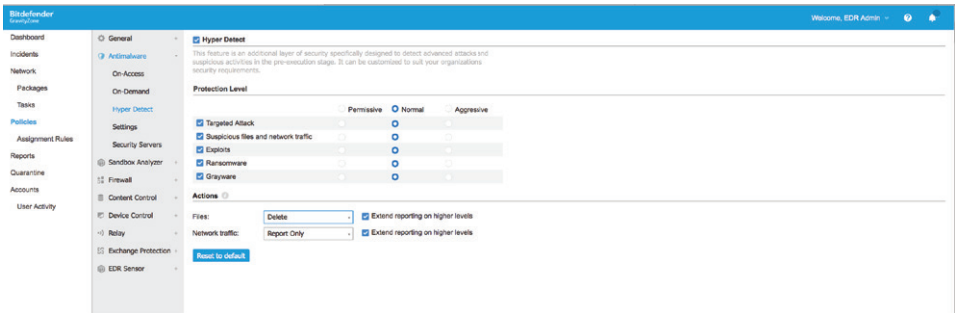
Solo gli eventi importanti, correlati e di una certa severità vengono presentati per l'analisi e la risoluzione manuale. Le informazioni ripetitive e fastidiose vengono mantenute al minimo, mentre la maggior parte degli attacchi e degli attacchi avanzati vengono bloccati in fase di esecuzione o pre-esecuzione. Minacce elusive, tra cui malware prive di file, exploit, ransomware e malware oscurati vengono neutralizzati da efficaci tecnologie di prevenzione per endpoint multilivello e di nuova generazione e da un'analisi dei processi in esecuzione basata sul comportamento. Una risposta e riparazione automatiche eliminano ogni necessità di intervento umano negli attacchi bloccati.

Una rilevazione ad alta fedeltà consente al personale di concentrarsi solo su vere minacce e incidenti:

- Minimizza il rumore e le distrazioni dei falsi allarmi
- Riduci il volume di incidenti con una prevenzione dalle minacce efficace
- Elimina la bonifica manuale degli attacchi bloccati con riparazione e bonifica automatiche

Una risposta intelligente significa una prevenzione evoluta

Poiché GravityZone Ultra è una soluzione integrata di prevenzione-rilevazione-risposta, ti consente di rispondere rapidamente e ripristinare gli endpoint a una "migliore fase precedente". Sfruttando le informazioni sulle minacce ottenute dagli endpoint durante la fase di indagine, una sola interfaccia fornisce gli strumenti per modificare immediatamente la policy e correggere le vulnerabilità, così da impedire incidenti futuri, migliorando la sicurezza del proprio ambiente.



Una piattaforma di sicurezza per endpoint completa in un agente e una console

GravityZone Ultra eredita tutti i controlli di rafforzamento e prevenzione di nuova generazione inclusi in Endpoint Security HD e nella suite di GravityZone Elite.

- Minimizza l'esposizione con una forte prevenzione
- La rilevazione basata su apprendimento automatico e analisi comportamentale blocca le minacce sconosciute in fase di esecuzione e pre-esecuzione
- Rileva e blocca malware basati su script, privi di file, offuscati e personalizzati con una bonifica automatica
- Protezione della memoria per prevenire gli exploit
- Riduci la superficie d'attacco attivando i controlli di sicurezza IT
- Firewall integrato nel client, controllo dispositivi, filtro dei contenuti web, controllo applicazioni, gestione patch e molto altro.

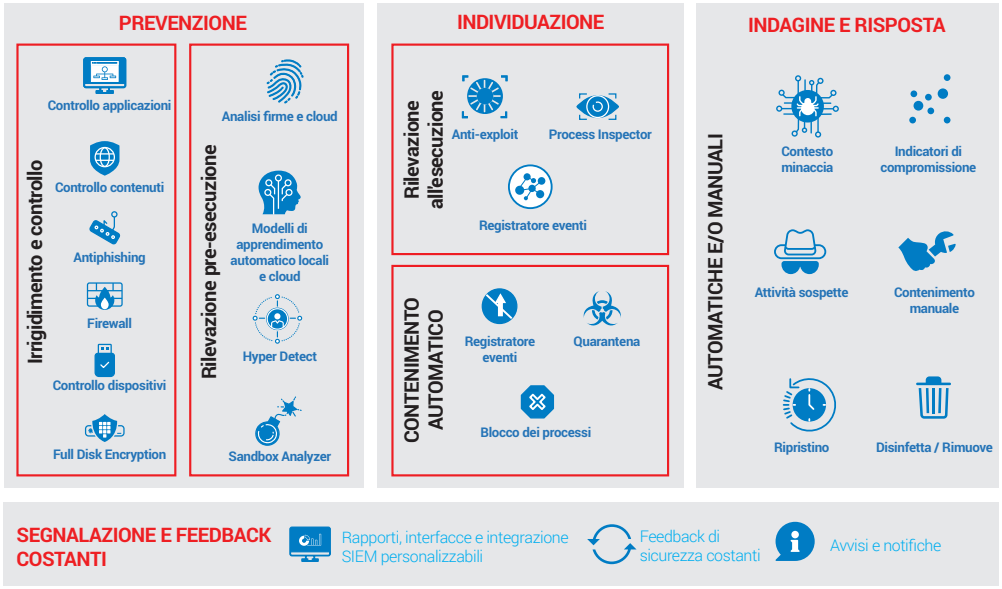
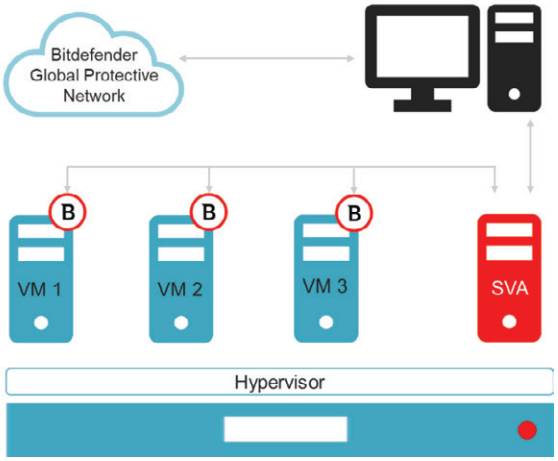


Figura 3. Bitdefender XDR: la piattaforma di sicurezza per endpoint completa

Proteggere i data center

Integrandosi completamente con Bitdefender Endpoint Security XDR, la componente di protezione dei Data center della suite di GravityZone Ultra è Security for Virtualized Environments (SVE). Si tratta della soluzione di sicurezza per Data center virtualizzati più avanzata sul mercato nella protezione antimalware per virtual machine, andando a ottimizzare non solo i tassi di consolidamento ma anche i costi operativi. GravityZone SVE è una soluzione aziendale in grado di supportare persino i maggiori data center. L'integrazione in un ambiente produttivo è estremamente semplice e questa tecnologia garantisce vantaggi ad ambienti virtuali di ogni dimensione.

Vantaggi principali



Agilità
SVE attiva l'automazione della sicurezza nel ciclo di vita del data center durante il lancio e le operazioni di sicurezza quotidiane di un ambiente virtuale altamente dinamico. Si integra con (vCenter, vShield, NSX), Citrix XenCenter e la Nutanix Enterprise Cloud Platform, consentendo un rapido provisioning automatizzato.

Efficienza operativa
La console di gestione unificata del Control Center di GravityZone semplifica la distribuzione di sicurezza, manutenzione e upgrade, fornendo visibilità centralizzata in tutti i server e le workstation virtuali e fisiche. Supporta la creazione centralizzata e l'amministrazione automatica delle politiche di sicurezza, che aiutano a ottimizzare le operazioni IT, riuscendo al tempo stesso a migliorare la conformità.

Utilizzo migliorato dell'infrastruttura
La scansione centralizzata e un agente dall'impronta minima riducono sensibilmente l'uso di memoria, spazio su disco, processo e attività di I/O sui server host, aumentando la densità della VM e il ROI nell'infrastruttura IT.

Compatibilità universale
Compatibile con tutte le principali piattaforme hypervisor (VMware ESXi, Microsoft Hyper-V, Citrix Xen, Red Hat KVM e Nutanix AHV) e sia Windows che Linux, come sistemi operativi guest.

Scalabilità lineare illimitata
Più SVA possono essere utilizzate per aumentare la capacità di scansione man mano che il data center cresce e vengono create più VM. Poiché una SVA esistente richiede una determinata soglia di carico, è possibile impiegarne di nuove per gestire la crescita. Un ulteriore vantaggio di impiegare più SVA è la migliore resistenza e condivisione dei carichi: il carico da una SVA fallita/sovraccaricata può essere supportato da un'altra SVA attiva o meno carica.

Difese multilivello di nuova generazione
GravityZone Security for Virtualized Environments include tutti i livelli chiave di sicurezza di Endpoint Security, tra cui HyperDetect, Sandbox Analyzer e i metodi di rilevazione degli attacchi privi di file per offrire una protezione leader alle risorse digitali delle aziende memorizzate o elaborate nei data center.

Caratteristiche

- Progettato per consentire la trasformazione del data center: SDDC, hyper-convergence e cloud ibrido
- Integrazioni complete con VMware, Nutanix, Citrix, AWS e Microsoft per protezione dell'investimento, automazione dell'impiego e dell'inventario, e gestione della licenza
- Supporto di più ambienti cloud e di virtualizzazione da un solo impiego
- Un unico pannello di controllo e gestione centralizzata attraverso il cloud ibrido
- Architettura basata su SVA efficiente, resistente e scalabile, in grado di supportare tutti gli hypervisor
- Densità VM massimizzata, bassa latenza di avvio e prestazioni delle applicazioni ottimali
- Sicurezza multilivello avanzata con costante copertura nel cloud ibrido

GravityZone Control Center

GravityZone Control Center è una console di gestione integrata e centralizzata che offre una visione unica per tutte le componenti di gestione della sicurezza, tra cui sicurezza per endpoint, datacenter, Exchange e dispositivi mobile. Può essere impiegato a livello locale o tramite cloud. Il centro di gestione di GravityZone include più ruoli e contiene il server del database, il server di comunicazione, il server di aggiornamento e la console web. Il Control Center viene fornito come un'immagine di appliance virtuale e può essere impiegato in meno di 30 minuti. Per aziende di maggiori dimensioni, può essere configurato per utilizzare più appliance virtuali con istanze multiple di ruoli specifici con bilanciatore di carico incorporato per la massima scalabilità e disponibilità.

Per requisiti di sistema più dettagliati, visita www.bitdefender.com/business/ultra-security

Bitdefender

Bitdefender è una società leader mondiale nelle tecnologie di sicurezza che fornisce soluzioni di sicurezza informatica end-to-end innovative e una protezione avanzata da ogni minaccia a oltre 500 milioni di utenti in più di 150 paesi. Dal 2001, Bitdefender produce costantemente le più premiate tecnologie di sicurezza per utenti consumer e aziendali, oltre a essere uno dei migliori fornitori sia nelle infrastrutture ibride di sicurezza che nella protezione degli endpoint. Attraverso Ricerca e Sviluppo, partnership e collaborazioni, Bitdefender è nota per il suo approccio innovativo e per offrire una sicurezza sempre affidabile. Maggiori informazioni sono disponibili alla pagina http://www.bitdefender.it/

BD-NGZ-Nov20.2017-IT-#.new0.ret
Bitdefender-NGZ-UltraSuite-Datasheet-creat2199-a4-it_IT