Bitdefender GravityZone Ultra Suite

SVELA E BLOCCA LE MINACCE ELUSIVE CON AGILITÀ E PRECISIONE

GravityZone Ultra è una soluzione Endpoint Security completa, progettata da zero come EPP integrata di prossime generazione e EDR facile da usare. Offre capacità di prevenzione, rilevamento delle minacce, risposta automatica, visibilità in pre e post compromissione, identificazione degli allarmi, indagine, ricerca avanzata e risanamento immediato.

GravityZone Ultra si affida a tecnologie automatizzate ed altamente efficaci di prevenzione, rilevamento e risposta alle minacce e limita drasticamente il numero di incidenti che richiedono un'analisi manuale, riducendo gli sforzi operativi richiesti per la gestione di una soluzione EDR. Basato su cloud e progettato da zero come soluzione unifica con un unico agente e un'unica console, è anche facile da implementare e integrare nell'architettura di sicurezza già esistente.

GravityZone Ultra consente ai clienti aziendali di proteggere accuratamente risorse digitali anche dalle minacce informatiche più elusive, rispondendo al tempo stesso in modo efficace a ogni fase di un attacco, tramite:

- Una riduzione della superficie di attacco (tramite firewall, controllo applicazioni, controllo contenuti e gestione delle patch)
- Protezione dei dati (tramite il modulo aggiuntivo di Full Disk Encryption)
- Una rilevazione in pre-esecuzione e un'eliminazione del malware (tramite apprendimento automatico configurabile, ispezione dei processi in tempo reale e analisi nel sandbox)
- Rilevamento in tempo reale delle minacce e risanamento automatizzato
- Visibilità pre e post compromissione (analisi delle cause principali)
- Identificazione, indagine e risposta rapida agli incidenti
- Ricerca di dati attuali e storici
- Posizione di sicurezza "Meglio di prima" (tramite modulo aggiuntivo Patch management)

Il risultato è una prevenzione costante delle minacce, una visibilità approfondita, 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.

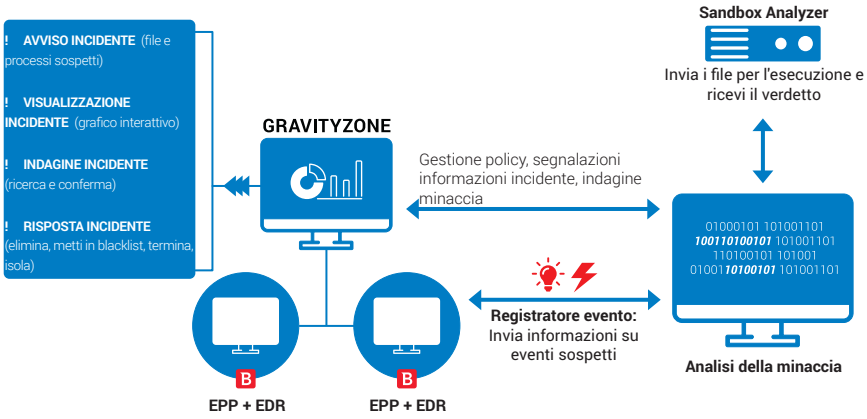


Figura 1. Bitdefender Ultra: prevenzione, rilevazione e risposta in un solo agente, gestito dalla console di GravityZone.

EDR semplificato

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 alla struttura di protezione delle minacce esistenti ed esegue una vasta gamma di attività di sistema (elaborazione file, 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.

Vantaggi principali

Espandendo le funzionalità EPP tradizionali, GravityZone Ultra 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:

- Rilevamento in tempo reale e risanamento automatico
- Identificazione, indagine e risposta rapida agli incidenti

Rilevamento delle attività sospette Verifica delle attività sospette e prioritizzazione degli allarmi Risposta agli incidenti in un clic

- Analisi pre e post compromissione (analisi delle cause principali)
- Ricerca di dati attuali e storici basata su:

IOC Tag MITRE Processi, file, voci di registro o altri parametri

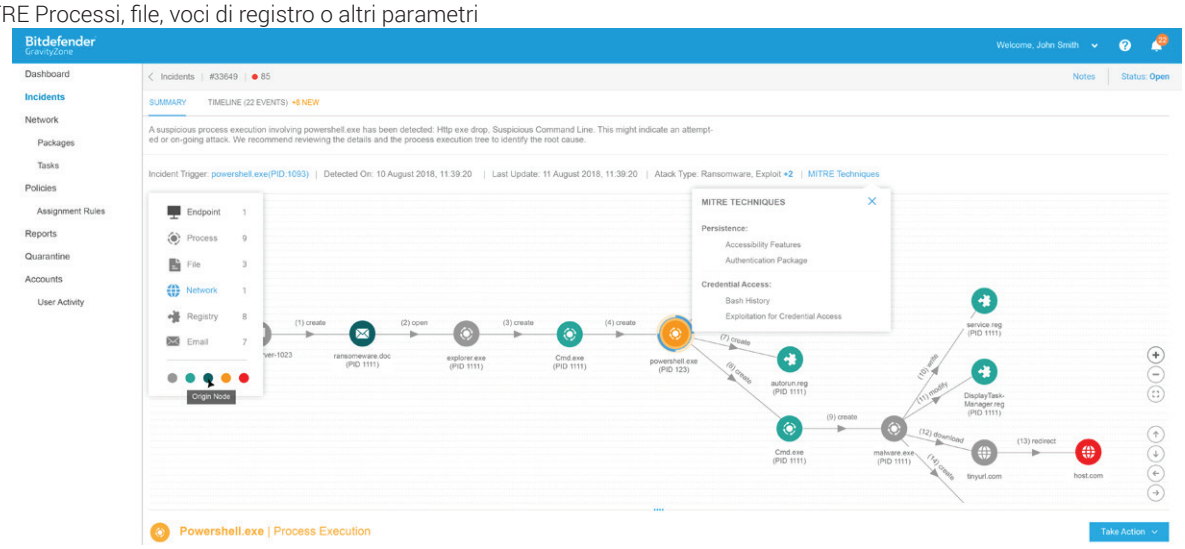


Figura 2. La pagina dei dettagli relativi all'incidente fornisce una chiara panoramica sul "raggio d'azione" degli incidenti. Il professionista può facilmente acquisire prove a supporto e rispondere.

Una rilevazione ad alta fedeltà significa una migliore visione di sicurezza e una maggiore libertà dagli sforzi degli allarmi

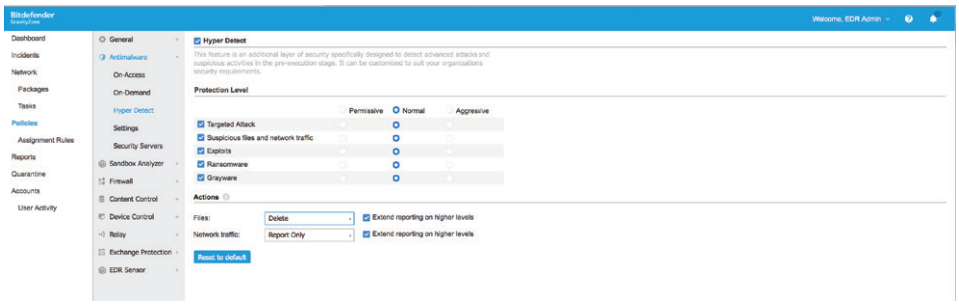
Solo gli eventi importanti, correlati e di una certa severità vengono presentati per l'analisi e la risoluzione manuale. Le informazioni ripetitive e fastidiose vengono mantenute al minimo, mentre la maggior parte degli attacchi e degli attacchi avanzati vengono bloccati in fase di esecuzione o pre-esecuzione. Minacce elusive, tra cui malware privi di file, exploit, ransomware e malware offuscati, vengono neutralizzate 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

Indagine semplice e risposta intelligente agli incidenti per una protezione evoluta

Come soluzione integrata di prevenzione-rilevamento-risposta-evoluzione, GravityZone Ultra garantisce una risposta veloce e il rapido ripristino degli endpoint a una fase migliore di quella iniziale. Strumenti di indagine come l'analisi delle cause principali e i rapporti su sandbox aiutano i team di sicurezza a verificare le attività sospette e a rispondere in modo adeguato alle minacce informatiche. La ricerca avanzata di dati attuali e storici, basata su IOC, tag MITRE e altri artefatti rilevanti permette una rapida identificazione delle minacce che potrebbero nascondersi nell'infrastruttura endpoint.



Sfruttando le informazioni sulle minacce ottenute dagli endpoint durante l'indagine, una sola interfaccia di gestione fornisce gli strumenti per modificare immediatamente la policy e/o correggere le vulnerabilità individuate, così da impedire incidenti futuri, migliorando la sicurezza del tuo ambiente.

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

GravityZone Ultra ha ereditato tutti i controlli di rafforzamento e prevenzione di nuova generazione inclusi 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 un risanamento automatico
- 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 e molto altro.
- Moduli aggiuntivi: Full Disk Encryption, Patch Management

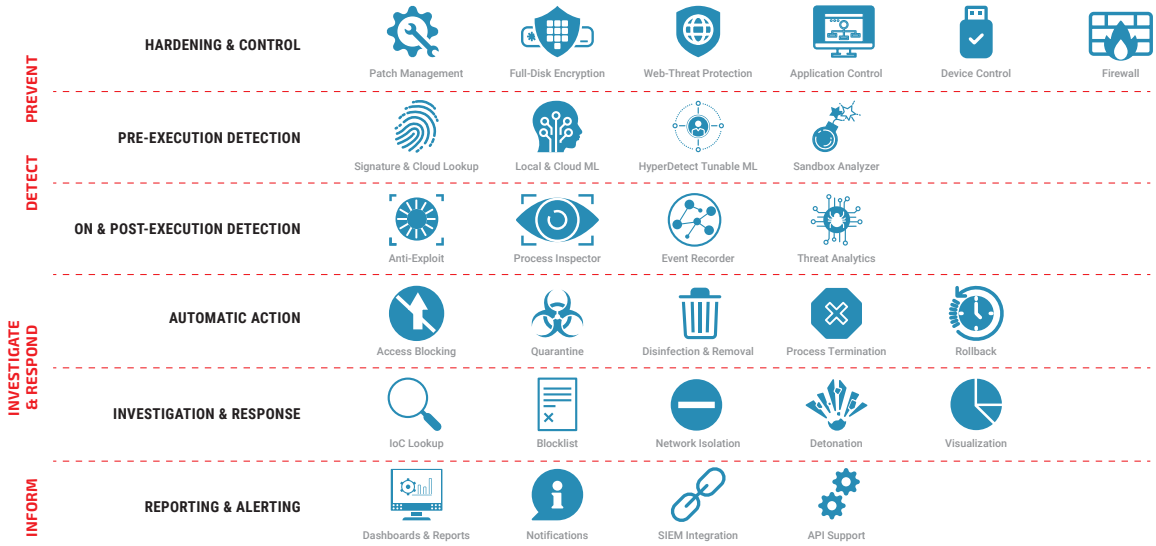
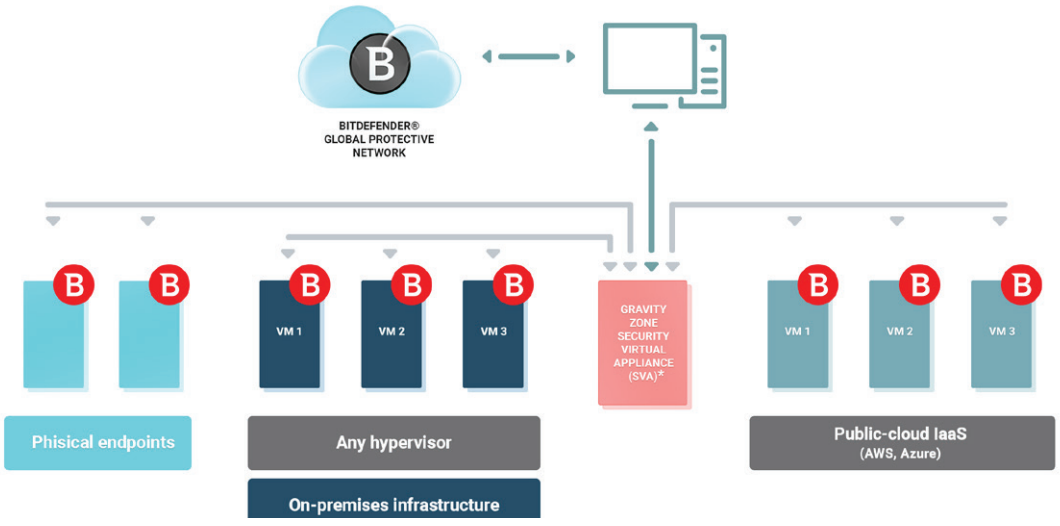


Figura 3. Bitdefender GravityZone Ultra: la piattaforma completa EPP + EDR di sicurezza per gli endpoint

Proteggere i data center e l'infrastruttura cloud

Come parte integrante di GravityZone Ultra, GravityZone Security for Virtualized Environments è la sua componente di sicurezza dei carichi lavorativi VDI e server progettata per garantire agilità, efficacia operativa e contenimento dei costi dell'infrastruttura in ambienti definiti da software hyper-converged e ibridi-cloud.



*** - Inoltre, gli impieghi senza agente sono supportati con VMware® vShieldTM o NSXTM**

Vantaggi principali

Maggiore efficienza e agilità operativa
Compatibile con diverse piattaforme cloud e tutti gli hypervisor (ad esempio, VMware® ESXiTM, Citrix® XenServer®, Microsoft® Hyper-V, Nutanix® AHV, KVM, RedHat® Enterprise Virtualization o una combinazione di essi), GravityZone aiuta a semplificare le operazioni IT e di sicurezza, migliorando al tempo stesso la conformità. La console di gestione unificata di GravityZone semplifica l'impiego e l'amministrazione della sicurezza, consentendo la fornitura automatica della sicurezza, l'applicazione centralizzata della policy e una visibilità tramite un'unica interfaccia in ambienti eterogenei e distribuiti. L'integrazione con gli strumenti di gestione della virtualizzazione (ad esempio, vCenter Server, XenServer e Nutanix Prism) garantisce a GravityZone la conoscenza in tempo reale del contesto operativo dell'infrastruttura sottostante, tra cui l'inventario globale delle virtual machine (VM). Di conseguenza, GravityZone può applicare automaticamente policy di sicurezza appropriate per VM che seguono i carichi di lavoro indipendentemente da dove si trovino nel cloud ibrido, consentendo ai team IT operativi dei clienti di far ruotare migliaia di VM protette in poche ore.

Migliori prestazioni e utilizzo dell'infrastruttura
Gli algoritmi di sicurezza brevettati di Bitdefender e la sua progettazione efficiente, che elimina la necessità di utilizzare agenti esosi in termini di risorse in ciascuna virtual machine, consente una densità di virtualizzazione superiore al 35% e una risposta dell'applicazione più veloce del 17% rispetto ai concorrenti, promuovendo un miglior utilizzo dell'infrastruttura e un'esperienza utente superiore.

Scalabilità lineare illimitata
L'architettura modulare e resiliente di GravityZone offre la scalabilità necessaria per proteggere gli impieghi carrier-grade. La piattaforma può espandersi a richiesta in un modo lineare ed efficiente aggiungendo Security Virtual Appliance o moltiplicando i ruoli server del Control Server, se necessario.

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.

GravityZone Control Center

GravityZone Ultra 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, data center, cloud ed Exchange. Per GravityZone Ultra è disponibile solo una console 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.

GravityZone Ultra è disponibile con la console cloud. Protegge desktop, server e mailbox Exchange. I server devono contare per meno del 35% delle unità totali.

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