Bitdefender

Blocca le minacce avanzate e resta un passo avanti agli aggressori con una sicurezza per endpoint flessibile e stratificata

GravityZone Security for Endpoints di Bitdefender sconfigge le minacce avanzate e sofisticate, utilizzando un approccio flessibile e stratificato. Tecnologie brevettate di apprendimento automatico combinate con la capacità di monitorare il comportamento e individuare le tecniche di attacco, consentono a GravityZone di rilevare, prevenire e bloccare le minacce. Quindi intraprende automaticamente ogni azione per consentire alle aziende di mantenere la normale operatività, tra cui il ripristino di modifiche dannose.

La console di GravityZone centralizza la gestione della sicurezza per la protezione degli endpoint in ambienti fisici, virtuali e cloud pubblici. Gli amministratori possono personalizzare l'agente di GravityZone Endpoint in base alle proprie necessità per una protezione completa e un impatto minimo sulle prestazioni.

CASI DI UTILIZZO

- Bloccare i ransomware
- Protezione da minacce avanzate (protezione da attacchi mirati avanzati)
- Prevenzione di exploit - Vulnerabilità a zero-day, vulnerabilità non risolte con patch
- Pulizia - Risanamento automatico
- Sicurezza data center
- Sicurezza per ambienti ibridi (cloud pubblico, data center, fisici, virtuali)

VANTAGGI

Identifica e blocca malware e ransomware sconosciuti
Bitdefender utilizza alcuni algoritmi di apprendimento automatico brevettati in grado di rilevare accuratamente malware sconosciuti, incluso le nuove varianti di ransomware. Questi algoritmi vengono addestrati e perfezionati utilizzando trilioni di campioni da una rete globale di 500 milioni di sensori per prevedere la progressione delle minacce e consentire a Bitdefender di adattare le proprie tecnologie per bloccare gli aggressori.

Blocca attacchi basati su exploit
Gli attacchi sofisticati spesso partono da un exploit per ottenere il controllo dell'endpoint bersaglio.

La tecnologia anti-exploit avanzata di Bitdefender rileva e blocca gli attacchi che sfruttano zero-day e vulnerabilità non risolte da patch con tecniche come il Return-oriented Programming (ROP).

Rileva e blocca gli attacchi avanzati con un monitoraggio in tempo reale
Operando su un presupposto zero-trust, la protezione per endpoint di Bitdefender GravityZone monitora continuamente tutti i processi attivi e può interrompere attività dannose e ripristinare eventuali modifiche. Ciò consente a GravityZone Security for Endpoint di rilevare costantemente malware zero-day e attacchi file-less in grado di violare processi noti e in esecuzione.

Neutralizza le minacce con un risanamento automatico
Bitdefender Security for Endpoint, grazie ai migliori strumenti di rimozione dei malware del settore, neutralizza istantaneamente le minacce, incluso malware basati sul kernel, rimuove tutti i malware, ripristina eventuali modifiche e offre informazioni per la riparazione e l'analisi.

Massime prestazioni - Ottimizzato per virtualizzazione e cloud
L'agente di GravityZone Endpoint è modulare e integrato. Gli amministratori possono personalizzarlo in base alle funzioni e le policy di sicurezza necessarie per una completa protezione con un'impronta minima.

Visibilità e gestibilità in tutto l'ambiente
La piattaforma GravityZone di Bitdefender è stata sviluppata da zero come una piattaforma di gestione della sicurezza unificata per proteggere ambienti fisici, virtualizzati, cloud e mobile. Segnalazioni dettagliate e rapporti intelligenti di eventi offrono una preziosa visione di ogni attacco, come il numero di sistemi interessati, e consentono anche di individuare i file o gli eseguibili coinvolti.

CARATTERISTICHE PRINCIPALI

Le tecniche di apprendimento automatico utilizzano modelli e algoritmi automatici ben addestrati per prevedere e bloccare attacchi avanzati prima della loro esecuzione. I modelli di apprendimento automatico di Bitdefender utilizzano 40.000 funzionalità dinamiche e statiche, e vengono continuamente addestrati su miliardi di file raccolti da oltre 500 milioni di endpoint a livello globale. Ciò aumenta notevolmente la precisione della rilevazione di malware, minimizzando i falsi positivi.

Una tecnologia Anti-Exploit avanzata protegge la memoria e le applicazioni vulnerabili, come browser, lettori di documenti, file multimediali e runtime (ad esempio, Flash, Java). Meccanismi avanzati osservano le routine di accesso alla memoria per rilevare e bloccare tecniche di exploit, come verifica del Caller API, Stack Pivot, Return-oriented Programming (ROP) e altre.

Il monitoraggio in tempo reale dei processi ispeziona tutti i processi nel sistema operativo utilizzando filtri in modalità utente e kernel. Cerca eventuali segni sospetti o comportamenti anomali, intraprendendo eventuali azioni di riparazione, tra cui la conclusione del processo e l'annullamento delle modifiche apportate dallo stesso. È molto efficace nel rilevare malware sconosciuti e avanzati, oltre ad attacchi senza file.

Controllo applicazioni/Whitelist* cattura "un'immagine" di ciascun endpoint, consentendo agli amministratori di creare una whitelist di applicazioni. Supporta entrambe le modalità "Automatica" e "Blacklist", e può essere utilizzato anche in modalità Verifica o Controllo.

Il filtro Sicurezza web consente di effettuare una scansione in tempo reale di e-mail e traffico in arrivo, tra cui il traffico SSL, per impedire il download di eventuali malware. La protezione anti-phishing blocca automaticamente le pagine web phishing.

Tecnologia di scansione intelligente

Ora la scansione centralizzata è possibile sia per computer fisici che virtuali. Gli amministratori possono scaricare le funzioni di sicurezza, come la scansione anti-malware, a una Security Appliance centralizzata per preservare le risorse dell'endpoint. Per i dispositivi in roaming, l'agente consapevole dell'ambiente trova automaticamente il miglior processo di scansione e può decidere se eseguire la scansione a livello locale.

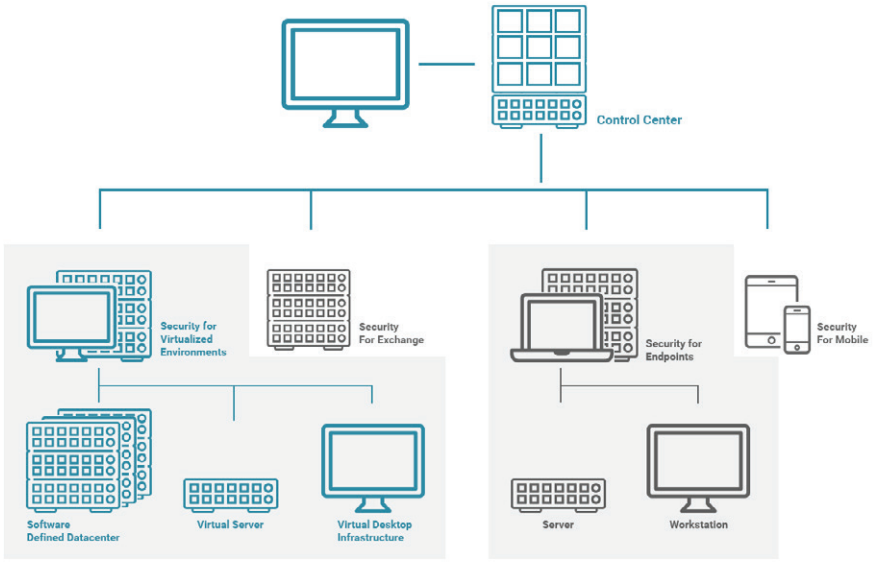
Controllo endpoint

I controlli endpoint basati su policy includono il firewall, il controllo dispositivi con scansione USB e il controllo dei contenuti web con categorizzazione degli URL.

- *Il modulo Controllo dispositivi* impedisce l'infezione di malware e le perdite di dati, consentendo agli amministratori di gestire le autorizzazioni per dispositivi esterni, come unità flash USB, dispositivi Bluetooth, lettori CD/DVD, ecc.
- *Il Firewall* include un firewall personale a due vie e un controllo in grado di rilevare e prevenire intrusioni basato su host. Questo modulo controlla l'accesso delle applicazioni alla rete e a Internet. Può anche proteggere il sistema da port scan, limitare la condivisione della connessione a Internet e avvisare quando nuovi nodi si connettono a una rete Wi-Fi.
- *Il Controllo dei contenuti web* gestisce dinamicamente l'accesso a siti web in base ai contenuti, mentre la barra degli strumenti di Bitdefender informa gli utenti sulla valutazione delle pagine web visualizzate. La policy del Controllo web può impedire l'accesso al web a utenti o applicazioni in determinati momenti.

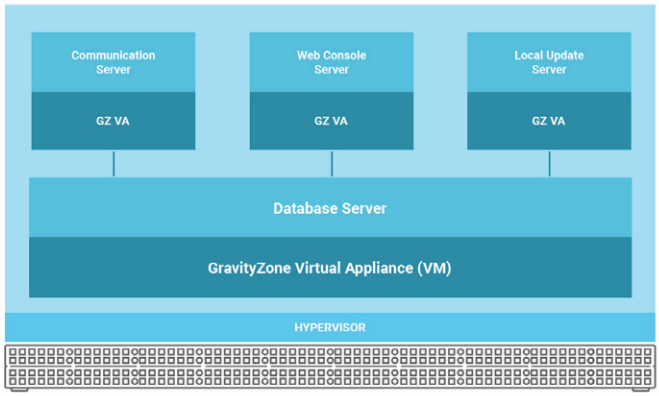
ARCHITETTURA DI GRAVITYZONE

L'architettura scalabile e flessibile di Bitdefender GravityZone include tre componenti principali:
• GravityZone Control Center
• GravityZone Endpoint Agent
• Security Virtual Appliance (opzionale)



GravityZone Control Center
GravityZone Control Center è una console di gestione integrata e centralizzata per le soluzioni di GravityZone, che include strumenti di sicurezza per endpoint, data center, Exchange e dispositivi mobile.

GravityZone Control Center può essere hostato da Bitdefender** o impiegato a livello locale. Control Center incorpora 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, utilizzabile in locale entro 30 minuti. Per aziende di maggiori dimensioni, GravityZone Control Center 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.



GravityZone Endpoint Agent
Il GravityZone Endpoint Agent include cinque moduli: anti-malware, firewall, Sicurezza web/controllo contenuti, controllo dispositivi e controllo applicazioni. La sua struttura modulare consente agli amministratori di impostare policy e servizi di sicurezza, mentre GravityZone personalizza automaticamente il pacchetto di installazione e minimizza l'impronta dell'agente.

Per ambienti distribuiti, gli amministratori possono sfruttare il ruolo di relay e determinati computer per utilizzarli come proxy di comunicazione e server di aggiornamento. Gli agenti relay scoprono automaticamente eventuali computer non protetti nella rete e rilasciano pacchetti di installazione e aggiornamenti per ottimizzare il traffico della rete.

Security Virtual Appliance
La Security Virtual Appliance è una appliance virtuale appositamente realizzata per fornire capacità di scansione centralizzate. La tecnologia di Bitdefender Smart Scanning consente a endpoint fisici e virtuali di scaricare le attività di sicurezza a una Security Virtual Appliance, liberando così risorse di calcolo.

* Non tutte le funzionalità sono disponibili su ogni piattaforma. Il controllo applicazioni e la funzione whitelist sono disponibili come parte di Bitdefender GravityZone Enterprise Security.

** Conosciuto anche come GravityZone Cloud console, disponibile nei bundle Business Security e Advanced Business Security.

REQUISITI DI SISTEMA E PIATTAFORME SUPPORTATE

- GravityZone Security for Endpoint e l'Endpoint Agent (Bitdefender Endpoint Security Tool) funziona con i sistemi operativi Windows, Mac e Linux.
- Bitdefender Security for Virtualized Environment supporta una vasta gamma di Hypervisor, tra cui VMware ESXi, Citrix Xen, Microsoft Hyper-V, Nutanix, Red Hat KVM e Oracle VM.
- Security for Mobile Devices offre una sicurezza Android e una gestione dei dispositivi iOS. Per maggiori informazioni sui requisiti di sistema, fare riferimento alla pagina https://www.bitdefender.it/business/endpoint-security.html

OPZIONI DI LICENZA

Bitdefender Security for Endpoint è una componente di Bitdefender GravityZone Business Security, Advanced Business Security e Enterprise Security. Per maggiori dettagli e confrontare le diverse opzioni, visitare https://www.bitdefender.it/business/compare.html

Bitdefender®

PROTEGGE OLTRE 500 MILIONI DI UTENTI AL MONDO

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/.

Bitdefender®

BD-NGZ-Feb.02.2018-Tk# crea1 287
Bitdefender 2017-NGZ-EndPointSecurity-DS-crea1287-A4-it_IT