Bitdefender

GravityZone Endpoint Security HD

Una piattaforma multilivello di nuova generazione per la sicurezza degli endpoint

Bitdefender Endpoint Security HD protegge le aziende dalla vasta gamma di minacce informatiche sempre più sofisticate con rapidità, accuratezza, basse spese amministrative e un impatto minimo sul sistema. La soluzione di nuova generazione elimina la necessità di eseguire più soluzioni di sicurezza per gli endpoint su una sola macchina, combinando controlli preventivi, tecniche di rilevazione multi-fase e non basate sulle firme e una risposta automatica in una sola piattaforma.

Endpoint Security HD blocca le minacce sconosciute e rileva gli attacchi mirati in grado di eludere le altre soluzioni di sicurezza per endpoint, utilizzando un avanzato apprendimento automatico, un'analisi comportamentale e una vasta gamma di altre tecnologie non basate sulle firme. Una volta rilevata una minaccia, Endpoint Security HD intraprende un'azione immediata, come ripristinare eventuali modifiche risultate dannose per garantire la tua normale operatività.

Punti salienti:

- **Protezione da Ransomware**
- **Prevenzione exploit**
- **Rileva e blocca attacchi privi di file**
- **Ferma attacchi basati su script**
- **Visibilità di attività sospette**

VANTAGGI PRINCIPALI

Rileva e blocca l'intera gamma di minacce sofisticate e malware sconosciuti
GravityZone Security HD sconfigge le minacce avanzate e i malware sconosciuti, tra cui i ransomware, in grado di eludere le soluzioni di protezione per gli endpoint tradizionali. Gli attacchi avanzati, come PowerShell, basati su script, attacchi privi di file e malware sofisticati possono essere rilevati e bloccati prima dell'esecuzione.

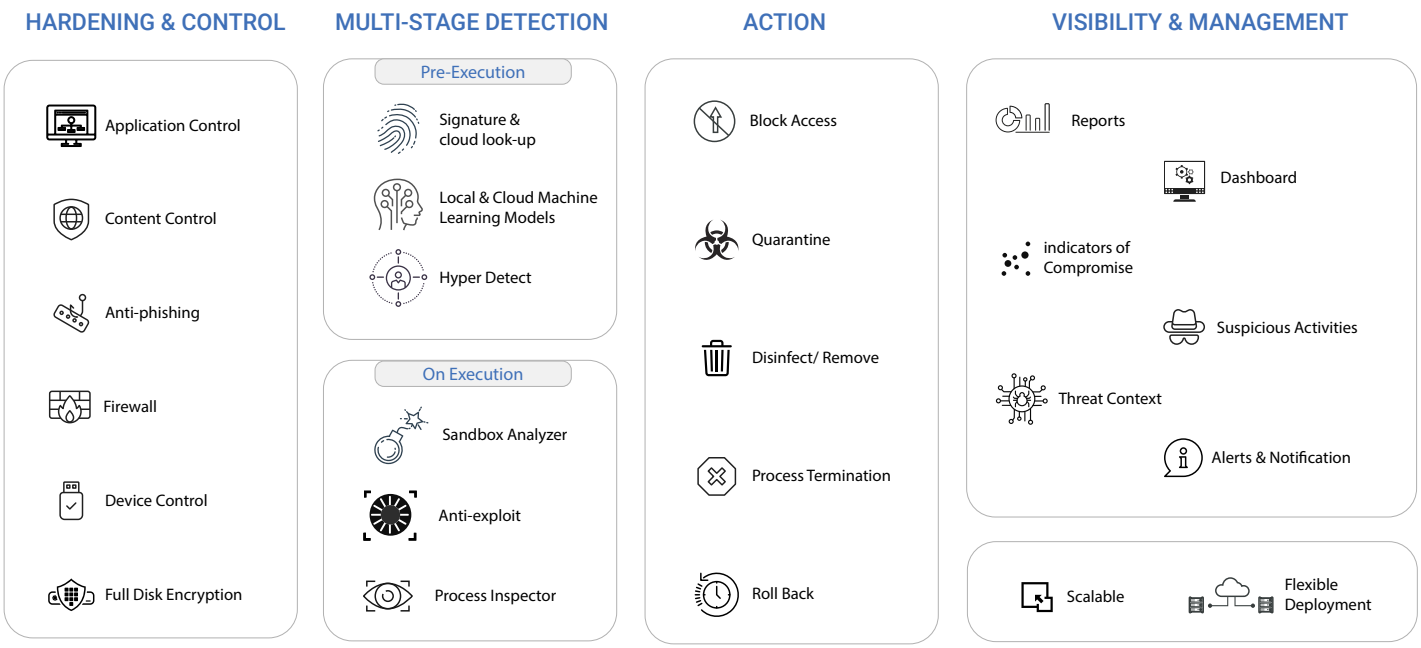
Blocca gli attacchi basati su exploit
Spesso gli attacchi di alto profilo partono da exploit per eseguire codice su sistemi bersaglio. La tecnologia anti-exploit di Bitdefender si concentra su strumenti e tecniche di attacco per rilevare e bloccare attacchi avanzati che sfruttano exploit zero-day e vulnerabilità non risolte da patch, come ROP (Return Oriented Programming), Shellcode e virtual pointer. Previene anche gli exploit del browser.

Migliora l'accuratezza senza falsi positivi
Nell'architettura multilivello flessibile, anti-exploit, apprendimento automatico, analisi comportamentale e sandbox basato su cloud collaborano per ottenere un tasso di rilevazione maggiore con una grande accuratezza, eliminando il fastidio provocato dai falsi positivi.

Azione immediata e automatica (Riparazione e risposta alla minaccia automatiche)
Una volta rilevata una minaccia, Endpoint Security HD la neutralizza subito tramite una serie di azioni, tra cui chiusura dei processi, messa in quarantena, rimozione e ripristino di modifiche risultate dannose. Condivide le informazioni sulla minaccia in tempo reale con la Global Protective Network, il servizio di intelligence delle minacce basato su cloud di Bitdefender, prevenendo attacchi simili ovunque nel mondo.

Ottieni massima visibilità e prospettiva sulle minacce
La capacità unica di Bitdefender Endpoint Security HD di identificare e segnalare le attività sospette dà agli amministratori un avviso preventivo su eventuali comportamenti dannosi, come richieste sospette del sistema operativo, azioni evasive e connessione a centri di comando e controllo.

Migliora l'efficienza operativa con un solo agente integrato
Il singolo agente integrato di sicurezza per gli endpoint di Bitdefender elimina ogni affaticamento dell'agente. La struttura modulare offre massima flessibilità e consente agli amministratori di impostare policy di sicurezza. GravityZone personalizza automaticamente il pacchetto di installazione e minimizza l'impronta dell'agente. Progettato dalla base come architetture di post-virtualizzazione e post-sicurezza cloud, GravityZone offre una piattaforma di gestione unificata per proteggere gli ambienti fisici, virtualizzati e cloud.



La piattaforma multilivello di nuova generazione per la protezione degli endpoint di Bitdefender utilizza un'architettura flessibile e a più livelli, che include funzioni di controllo degli endpoint, prevenzione, rilevazione, riparazione e visibilità.

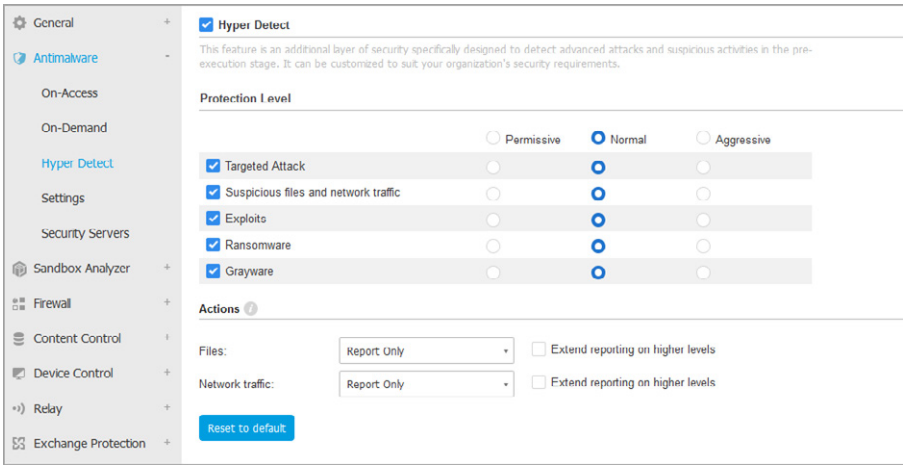
"GravityZone in pratica funziona da solo. Perciò siamo liberi di rivolgere i nostri sforzi alla pianificazione, aiutando le scuole a diventare più efficienti," Rolland Kornblau, Responsabile IT, El Rancho, Unified School District

CARATTERISTICHE

NUOVO HyperDetect

Questo nuovo livello difensivo in fase di pre-esecuzione include modelli di apprendimento automatico in locale e sistemi euristici avanzati addestrati a rilevare strumenti di hacking, exploit e tecniche di offuscamento dei malware per bloccare minacce sofisticate prima dell'esecuzione. Rileva anche tecniche di consegna e siti che ospitano kit di exploit, bloccando il traffico web sospetto.

HyperDetect consente agli amministratori di sicurezza di regolare la difesa per contrastare i tipici rischi che le aziende devono affrontare. Con l'opzione di "sola segnalazione", gli amministratori di sicurezza possono preparare e monitorare la loro nuova policy difensiva prima di impiegarla, eliminando ogni interruzione delle attività. Con una combinazione di alta visibilità e blocco aggressivo unica di Bitdefender, gli utenti possono impostare HyperDetect per operare un blocco a livello normale e permissivo, continuando a segnalare automaticamente il livello aggressivo, esponendo in anticipo gli Indicatori di Compromissione

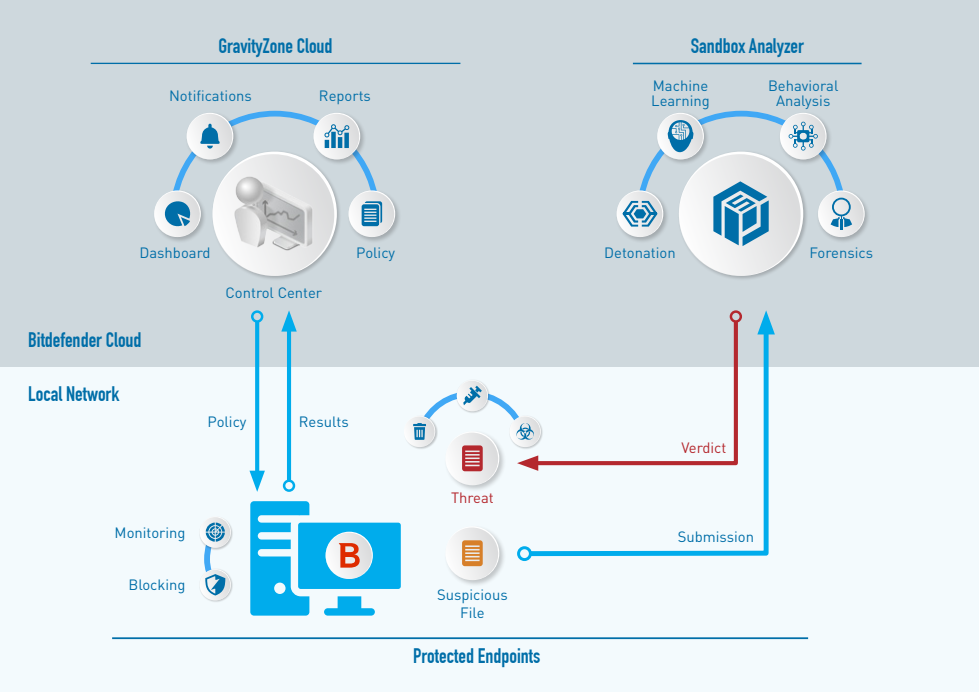


HyperDetect consente agli amministratori di sicurezza di regolare l'aggressività della propria difesa, offrendo una combinazione unica di blocco e visibilità delle minacce. Per esempio, è possibile impostare il blocco a un livello "normale" e la segnalazione a un livello "aggressivo".

NUOVO **Sandbox Analyzer integrato nell'endpoint**
Questo potente livello di protezione dalle minacce avanzate analizza i file sospetti in profondità, attivando i payload in un ambiente virtuale protetto, ospitato da Bitdefender, così da valutarne il comportamento e segnalare eventuali intenzioni dannose.

Integrato con l'agente Endpoint di GravityZone, Sandbox Analyzer invia automaticamente i file sospetti per un'ulteriore analisi. In caso di verdetto negativo da Sandbox Analyzer, Endpoint Security HD blocca subito e automaticamente il file dannoso su tutti i sistemi a livello aziendale. La funzione di invio automatico consente agli amministratori della sicurezza aziendale di scegliere tra la modalità di osservazione e blocco, che previene l'accesso a un file fino all'emissione di un verdetto. Gli amministratori possono inviare i file per l'analisi anche manualmente.

Le ricche informazioni forensi di Sandbox Analyzer danno agli amministratori una chiara prospettiva sulle minacce, aiutandoli a comprenderne il comportamento.



Sandbox integrato nell'endpoint. L'agente endpoint di GravityZone invia automaticamente i file sospetti a Sandbox Analyzer per ulteriori analisi.

Machine Learning
Le tecniche di apprendimento automatico utilizzano modelli e algoritmi automatici ben addestrati per prevedere e bloccare attacchi avanzati. I modelli di apprendimento automatico di Bitdefender utilizzano 40.000 funzionalità dinamiche e statiche, e vengono continuamente addestrati su miliardi di campioni di file puliti e dannosi, raccolti da oltre 500 milioni di endpoint a livello globale. Ciò aumenta notevolmente l'efficacia della rilevazione di malware, minimizzando i falsi positivi.

Anti-exploit avanzato
La tecnologia di prevenzione degli Exploit 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.

Process Inspector
Operando in una modalità zero-trust, Process Inspector monitoracostantemente tutti i processi in esecuzione nel sistema operativo. Rileva attività sospette o comportamenti anomali dei processi, , come tentativi di camuffare il tipo di processo, eseguire codice nello spazio di un altro processo (alterare la memoria del processo per un'escalation di privilegi), replicare, rilasciare file, nascondere applicazioni dall'enumerazione dei processi e molte altre. Esegue le appropriate azioni di risanamento, tra cui la chiusura del processo e l'annullamento delle modifiche fatte dallo stesso. È molto efficace nel rilevare malware sconosciuti e avanzati, oltre ad attacchi privi di file, tra cui i ransomware.

Filtro anti-phishing e sicurezza web
Il filtro della Sicurezza web attiva la scansione di tutto il traffico web in entrata, tra cui il traffico SSL, http e https, in tempo reale per prevenire il download di malware nell'endpoint. La protezione anti-phishing blocca automaticamente pagine web fraudolente e di

phishing. Gli amministratori possono limitare o bloccare in remoto l'accesso di un utente a determinate applicazioni o pagine web, per migliorare la sicurezza di Internet, consentire un miglior uso del web e garantire la conformità.

Risposta e contenimento
GravityZone offre la migliore tecnologia di pulizia sul mercato. Blocca/limita automaticamente le minacce, elimina i processi dannosi e ripristina eventuali modifiche.

Full Disk Encryption
La cifratura completa del disco gestita da GravityZone utilizzando BitLocker di Windows e FileVault di Mac, sfrutta a proprio vantaggio la tecnologia presente nei sistemi operativi.

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

REQUISITI DI SISTEMA E PIATTAFORME SUPPORTATE

Per requisiti di sistema più dettagliati, visita https://www.bitdefender.it/business/elite-security.html
GravityZone Endpoint Security HD
- SO workstation: Windows 10 RS2/RS1/TH2/TH1, Windows 8, 8.1, Windows 7 SP1

- Windows tablet e SO embedded: Windows Embedded 8 Standard, Windows Embedded 8.1 Industry, Windows Embedded Standard 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7

- Sistemi operativi server: Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2, Windows Server 2016 Core

OPZIONI DI LICENZA

GravityZone Endpoint Security HD è incluso nella suite di Bitdefender GravityZone Elite (con gestione cloud) e sarà disponibile anche come prodotto indipendente.

La suite di GravityZone Elite include anche Security for Endpoint per Windows, Mac e Linux
Bitdefender Security for Exchange
Security for Virtualized Environment (Datacenter security)

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-Jul14 2017-Tk#: crea1 287
Bitdefender 2017 NGZ: EndPointHD DS-crea1479-A4-it_IT