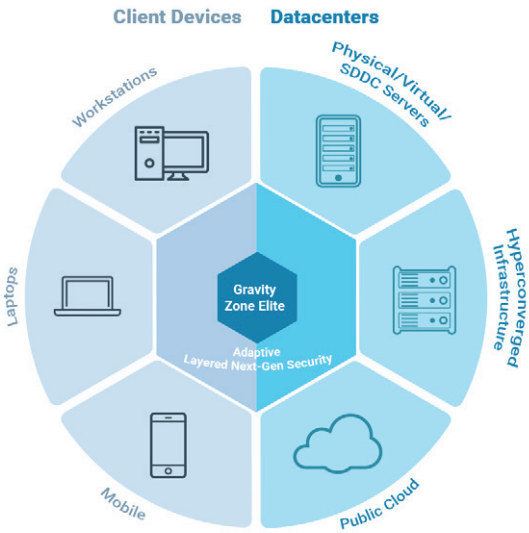
Bitdefender GravityZone Elite Suite

La piattaforma di sicurezza multilivello e di nuova generazione

Bitdefender GravityZone Elite Suite è stata sviluppata per proteggere le aziende dall'intera gamma di minacce informatiche avanzate con velocità e accuratezza. Elite combina il comprovato approccio alla sicurezza multilivello di Bitdefender con i suoi strumenti e le sue tecnologie di nuova generazione per offrire prestazioni e protezione di alto livello per tutti gli endpoint nell'ambiente aziendale: desktop, portatili, dispositivi mobili, server fisici e virtuali.

GravityZone Elite garantisce un costante livello di sicurezza per l'intero ambiente informatico, contenendo gli endpoint poco protetti, che potrebbero essere utilizzati come punti di partenza per azioni ai danni dell'azienda. Si affida a un'architettura semplice e integrata con gestione centralizzata sia per endpoint che data center. Le opzioni della console in locale e cloud si adattano sia ad ambienti rigorosamente disciplinati che cloud-ready.



PUNTI SALIENTI

- Rileva e blocca attacchi di malware privi di file
- Ferma attacchi basati su script
- Smonta e analizza malware sconosciuti in fase di pre-esecuzione
- Un solo agente e impronta minima con basso impatto sul sistema
- Console di gestione integrata per endpoint fisici e virtuali

Protezione degli endpoint

Bitdefender Endpoint Security HD – Il componente di GravityZone Elite dedicato alla sicurezza degli endpoint protegge le aziende dall'intera gamma di minacce informatiche avanzate con velocità, accuratezza, basso sovraccarico amministrativo 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.

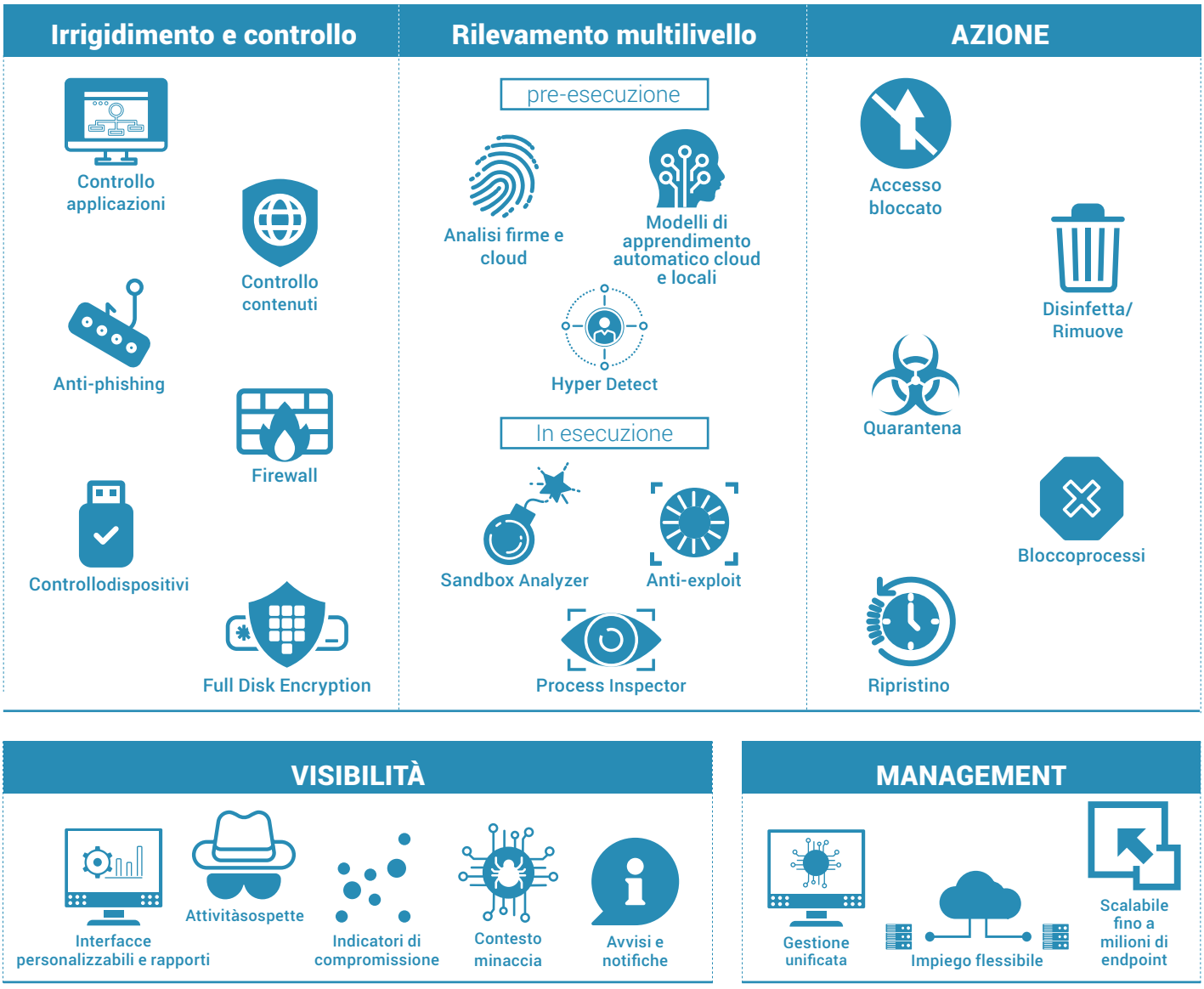
Vantaggi principali

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

Rileva e blocca i malware privi di file
Gli attacchi malware privi di file eseguono codice dannoso direttamente nella memoria. Poiché sul sistema non è presente alcun file, la maggior parte delle soluzioni AV progettate per analizzare i file non rilevano questo tipo di attacco. Bitdefender sfrutta un anti-exploit avanzato, HyperDetect™ e Process Inspector per rilevare, bloccare e interrompere gli attacchi privi di file.

Blocca gli attacchi basati su macro e script
In questo caso, gli aggressori si affidano alle macro di Microsoft Office che utilizzano strumenti di amministrazione di Windows, come PowerShell, per eseguire script e scaricare codice dannoso in grado di eseguire gli attacchi. Poiché si tratta di strumenti di Windows "affidabili", la maggior parte dei prodotti di sicurezza per endpoint, incluso i cosiddetti AV di nuova generazione, non esaminano gli script, come Powershell, WMI, interpreti Javascript, ecc. Bitdefender aggiunge tecniche di Command-line Analyzer per intercettare e mettere in sicurezza script, allertare gli amministratori e bloccare l'esecuzione di script, in caso di comandi dannosi.

Riparazione e risposta alle minacce 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 GPN, il servizio di intelligence delle minacce basato su cloud di Bitdefender, prevenendo attacchi simili in tutto il 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 e una console integrata
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.

Caratteristiche

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.

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 delle minacce unica di Bitdefender, gli utenti possono impostare HyperDetect per operare un blocco a livello normale e permissivo, ma continuando a segnalare automaticamente il livello aggressivo, esponendo in anticipo gli Indicatori di Compromissione

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. Con un verdetto dannoso da parte di Sandbox Analyzer, Endpoint Security HD blocca subito e automaticamente il file dannoso su tutti i sistemi a livello aziendale. La funzione di invio automatica consente agli amministratori della sicurezza aziendale di scegliere tra la modalità "monitoraggio" e "blocco", che impedisce di accedere a un file fino al ricevimento di un verdetto. Gli amministratori possono inviare i file per l'analisi anche manualmente. Le ricche informazioni forensi di Sandbox Analyzer danno una chiara prospettiva sulle minacce e aiutano a comprenderne il comportamento.

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
Process Inspector opera in modalità zero-trust, monitorando continuamente 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 Sicurezza web consente di effettuare una scansione in tempo reale del traffico web in arrivo, tra cui il traffico SSL, ttp e https in tempo reale per impedire il download di eventuali malware. La protezione anti-phishing blocca automaticamente le pagine web phishing e fraudolente.

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. FDE è disponibile come add-on, con una licenza separata.

Controllo degli endpoint e Hardening
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.

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.

Protezione data center

GravityZone Security for Virtualized Environments (SVE) sfrutta le difese multilivello e di nuova generazione di Bitdefender Endpoint Security HD per offrire alle aziende la migliore sicurezza per carichi di lavoro su server, VDI e cloud, massimizzando al tempo stesso le prestazioni e l'efficacia operativa dell'infrastruttura. GravityZone SVE è progettata come una soluzione aziendale in grado di supportare persino i maggiori data center.

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 piattaforme di virtualizzazione (come VMware® ESXiTM, Microsoft® Hyper-VTM, Citrix® XenServer®, Red Hat® Enterprise Virtualization®, KVM e Nutanix® Acropolis), Microsoft Active Directory, e i sistemi operativi guest sia Windows® che Linux®, GravityZone semplifica l'impiego, la scoperta degli endpoint e l'amministrazione delle policy.

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.

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.

Security for iOS and Android Mobile Devices

Questa soluzione è stata progettata per supportare l'adozione controllata del concetto di bring-your-own-device (BYOD), applicando costantemente le politiche di sicurezza a tutti i dispositivi degli utenti. Di conseguenza, i dispositivi mobile sono controllati e le importanti informazioni aziendali su di essi sono protette. Il carico amministrativo viene ridotto con la possibilità di avere lo stato sempre aggiornato dei dispositivi conformi e non conformi.

Security for Exchange Servers

Fornisce più livelli di sicurezza per la messaggistica: antispam, antiphishing, antivirus e antimalware con analisi comportamentale, protezione da minacce zero-day e filtro del traffico e-mail, tra cui filtro dei contenuti e degli allegati. La scansione antimalware può essere scaricata ai server di sicurezza centralizzati dai server mail protetti. Gestione e reportistica sono centralizzate, consentendo politiche unificate per endpoint e messaggistica.

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. 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 https://www.bitdefender.it/business/elite-security.html

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/

Tutti i diritti riservati. © 2017Bitdefender. Tutti i marchi registrati, i nomi commerciali e i prodotti a cui si fa riferimento in questo documento sono di proprietà dei rispettivi titolari. PER MAGGIORI INFORMAZIONI VISITA: bitdefender.it/business

BD-NGZ-Nov06.2017-IT#
Bitdefender-NGZ-Elite-Datasheet-creat2088-A4-it_IT