Bitdefender Security per Virtualized Environments

Ora disponibile in MSP Security Suite, la migliore del settore

Nonostante la vasta diffusione della virtualizzazione, i Managed Service Provider spesso utilizzano strumenti di sicurezza estremamente inefficienti, che richiedono più copie dell'agente antimalware sull'hardware dei computer di hosting, una per ogni macchina virtuale (VM). Questo approccio soffoca le risorse dell'host, peggiora l'esperienza utente, riduce il numero di macchine virtuali che possono essere eseguite e porta alcuni MSP a lasciare le VM non protette.

Bitdefender Security for Virtualized Environments (SVE) è stato progettato per la virtualizzazione, con un approccio bottom-up. Invece di utilizzare una copia di Bitdfender su ciascuna macchina virtuale, SVE sfrutta una sola VM, trasformandola in una Security Virtual Appliance (SVA) che protegge tutte le altre VM nell'ambiente host. Avere un'unica istanza dell'agente antimalware di Bitdefender in esecuzione nell'ambiente virtualizzato permette di migliorare drasticamente le prestazioni, i tassi di consolidamento e l'esperienza utente.

Punti salienti

- Migliora drasticamente le prestazioni di VS/VDI e l'esperienza utente
- Migliora le prestazioni delle applicazioni
- Sicurezza unificata per MSP in ambienti fisici, virtuali e cloud
- Elimina singoli punti di errore e colli di bottiglia in ambienti virtualizzati
- Sicurezza multilivello completa che include Machine Learning, monitoraggio dei processi e anti-exploit
- Automatizza il provisioning della sicurezza per le VM ed elimina i gap di sicurezza
- Supporta VMware, Citrix, Microsoft e ogni altro hypervisor

Vantaggi principali

Sicurezza per la virtualizzazione con le migliori prestazioni

SVE è progettato per risolvere i problemi legati all'esecuzione di AV in un ambiente virtualizzato. Le nostre estensive sessioni di test delle prestazioni tramite LoginVSI dimostrano che SVE ha un minore impatto sulle prestazioni rispetto a tutte le principali soluzioni AV, garantendo tempi di risposta fino al 17% più rapidi e una migliore implementazione di VM per dispositivo fisico (tassi di consolidamento massimizzati), fino al 35% in più.

Protezione multilivello completa, senza compromessi

Bitdefender offre livelli multipli di protezione per massimizzare la sicurezza, come l'apprendimento automatico, l'antiexploit e il monitoraggio costante dei processi, mentre altre soluzioni includono solo tecnologie di base per evitare di compromettere le prestazioni delle VM.

Sicurezza per MSP in ambienti fisici, virtuali e cloud

Gli MSP possono ridurre gli sforzi e i costi per il monitoraggio, l'amministrazione e la generazione di report con una console di sicurezza dedicata (e centralizzata) per ambienti fisici, virtuali e su cloud ibrido. A differenza di altre soluzioni, Bitdefender supporta qualsiasi hypervisor, è integrato con AWS e supporta tutti gli ambienti cloud.

Architettura altamente flessibile

La Security Virtual Appliance (SVA) è fornita tramite un'appliance virtuale con configurazione automatica basata su Linux Ubuntu. Le funzionalità di failover e il bilanciamento del carico con SVA multiple garantiscono ottime prestazioni e una protezione costante.

Sicurezza pluripremiata

Bitdefender SVE è dotato di una perfetta combinazione di tecnologie di sicurezza in grado di gestire qualsiasi cosa, dal malware di base agli attacchi mirati più avanzati. Nel marzo 2018 Bitdefender ha vinto i prestigiosi premi di AV-TEST per il Best Protection del 2017 e Best Performance del 2017, grazie a tecnologie come Process Inspector,anti-expoit avanzati, un antispam pluripremiato e il filtroggio dei contenuti, oltre alla sua difesa anti-ransomware multilivello.

L'intero arsenale delle pluripremiate tecnologie di protezione dalle minacce di Bitdefender si basa sui motori di sicurezza ed è integrato nell'architettura della virtual appliance. Con SVE, la protezione antimalware è più robusta che mai, offrendo una protezione ottimale, istantanea e disponibile per ogni VM.

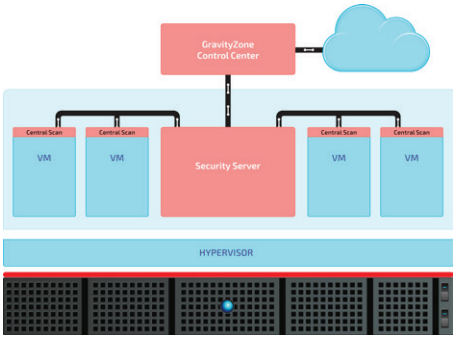
Panoramica della tecnologia

A differenza degli agent antivirus tradizionali, che devono essere presenti su ogni VM, richiedono un monitoraggio e un aggiornamento costanti e consumano una notevole quantità di risorse locali, SVE di Bitdefender permette di garantire la protezione antimalware tramite Security Virtual Appliance (SVA). SVE agisce come punto centralizzato per l'intelligence antimalware, senza la necessità di installare un agente di sicurezza tradizionale su ciascuna VM. Ogni VM si connette a un server di sicurezza per scaricare la maggior parte delle funzionalità antimalware, proteggendo file system, memoria, processi e registro sia su ambienti Windows che Linux.

SVE utilizza un meccanismo di caching multilivello in grado di fornire le migliori prestazioni del settore. Per prima cosa, ciascuna VM è dotata di una cache locale, così che gli elementi vengono esaminati una sola volta. Inoltre, in ciascun server di sicurezza (SVA) vi è una cache condivisa, in modo che gli elementi esaminati su una VM non vengano esaminati su altre. Infine, una serie di chache a livello di blocchi di file deduplica la scansione anche dei frammenti di file, il che significa che questi file non vengono riesaminati completamente. Il risultato finale di queste tecnologie esclusive di Bitdefender è il segreto che si cela dietro le massime prestazioni offerte da SVE.

Central Scan in sintesi

Affinché il server di sicurezza possa accedere al file system di ogni VM, oltre che a memoria, registro, processi in esecuzione e altre funzionalità richieste, è necessario impiegare su ogni VM un agente di comunicazione, noto come Central Scan. Le caratteristiche principali dell'agente Central Scan sono:



Impatto minimo sul sistema:

- Meno di 110 MB di memoria durante l'esecuzione (inclusa la cache di esecuzione)
- 10-20 MB di memoria locale durante l'esecuzione (scansione all'accesso)
- Carico massimo della CPU di 1-2%, su una sola CPU virtuale per la scansione all'accesso

Funzioni principali:

- Stabilisce la connessione a un server di sicurezza disponibile e autorizzato (SVA), consentendo l'accesso locale a file system, registro, memoria e processi.
- Attiva la connessione a server di sicurezza alternativi in caso di tempo di risposta molto lento o indisponibilità improvvisa.
- Gestisce la disinfezione, la quarantena e il blocco dei processi in locale.
- Conserva gli elementi esaminati in una cache locale per migliorare le prestazioni.
- Viene eseguito come servizio locale con tutti i privilegi di amministratore rimossi, proteggendo da attacchi che tentano di disattivare la protezione a livello locale.
- Fornisce opzionalmente un'interfaccia utente nella VM con notifiche pop-up sul desktop.
- L'implementazione di Central Scan (disponibile sia per Windows che per Linux) è semplice e non richiede il riavvio di alcuna macchina virtuale. Inoltre l'implementazione del server di sicurezza non richiede il riavvio delle macchine di hosting delle VM.
- Central Scan può anche essere fornito in template e immagini VDI per ridurre al minimo il sovraccarico gestionale.

Architettura dal design avanzato

- Le macchine virtuali non hanno alcun motore di scansione antimalware locale e neppure le definizioni, perciò saranno sempre protette da un server di sicurezza disponibile
- Elimina la possibilità di eventuali AV Storm
- Il caching multilivello tramite una singola VM e il server di sicurezza assicura che i file unici vengano esaminati una sola volta
- Elimina ogni eventuale gap in fatto di sicurezza e prestazioni in fase di avvio incontrato durante il lancio delle VM
- Nessun singolo punto di errore nella protezione, poiché Central Scan si connette o riconnette automaticamente a un server di sicurezza disponibile, come definito dalla policy
- Protezione centralizzata senza bottlenecks, poiché Central Scan può passare automaticamente a un altro server di sicurezza con un tempo di risposta più veloce
- Le macchine virtuali non persistenti sono protette automaticamente e disciplinate dalla corretta policy di sicurezza
- Aumenta la densità della macchina virtuale, tramite meno memoria, spazio su disco, processore e attività di I/O
- Le VM sono sempre protette dalle più recenti e aggiornate tecnologie Bitdefender, anche se ripristinate da una precedente immagine/backup o se avviate dopo un lungo periodo offline

Prova Bitdefender Cloud Security per MSP gratuitamente: visita la pagina www.bitdefender.com/msp o contattaci telefonicamente: (+1) 954 776 6262 x 10116

Bitdefender

Bitdefender è una società di tecnologia di sicurezza globale che fornisce soluzioni di sicurezza informatica end-to-end innovative e protezione avanzata contro le minacce a oltre 500 milioni di utenti in più di 150 paesi. Dal 2001, Bitdefender produce costantemente tecnologie pluripremiate per la sicurezza aziendale e dei consumatori ed è un fornitore di riferimento sia per la sicurezza dell'infrastruttura ibrida che per la protezione degli endpoint. Attraverso Ricerca e Sviluppo, partnership e collaborazioni, Bitdefender è affidabile di essere all'avanguardia e di offrire una sicurezza solida su cui fidarsi. Maggiori informazioni sono disponibili sul sito http://www.bitdefender.it/