McAfee Host Intrusion Prevention for Desktop

Protezione avanzata contro le vulnerabilità per desktop e notebook

Gestire la sicurezza e controllare la connettività per computer desktop e notebook all'interno di un'azienda è sempre più complesso dato il crescente numero di criminali informatici orientati al profitto e dalla natura sofisticata delle minacce odierne. Gli impiegati lavorano sempre più in mobilità, il che pone ulteriore pressione sull'IT che deve garantire che gli utenti si colleghino in modo sicuro alla rete aziendale. Inoltre, le aziende hanno bisogno di protezione immediata contro le minacce per guadagnare più tempo per essere in grado di prioritizzare, testare e distribuire in modo adeguato le patch necessarie.

La sfida

L'antivirus da solo non è sufficiente, poiché gli attacchi e gli exploit delle vulnerabilità vengono rilasciati più velocemente e diventano più complessi. La soluzione è implementare una strategia di protezione proattiva che blocchi in primo luogo gli attacchi. Adottando un approccio proattivo per proteggere gli endpoint, i dipartimenti IT possono essere sicuri che tutti gli endpoint e i dati riservati siano protetti e la business continuity sia preservata.

McAfee Host Intrusion Prevention for Desktop

Parte fondamentale delle suite endpoint di McAfee®, McAfee Host Intrusion Prevention for Desktop offre livelli di protezione senza pari dalle minacce note e sconosciute combinando protezione tramite firme e sistemi IPS (Intrusion Prevention System) comportamentali con un firewal stateful dinamico. McAfee Host Intrusion Prevention for Desktop riduce la frequenza e l'urgenza di applicazione delle patch, preserva la continuità operativa e la produttività dei dipendenti, protegge la riservatezza dei dati e semplifica la conformità normativa.

Vantaggi principali

Una protezione maggiore

- Applica la più ampia copertura di protezione IPS e per le minacce zero-day a tutti i livelli: rete, applicazione ed esecuzione di sistema.

Costi ridotti

- Riduci tempi e costi con un'unica potente console unificata per implementazione, gestione, reportistica e verifica di eventi, policy e agent.
- Applica le patch agli endpoint meno frequentemente e con meno urgenza.

Conformità semplificata

- Gestisci la conformità con panoramiche fruibili semplici da comprendere, workflow, monitoraggio degli eventi e reportistica per attività di indagine appropriate.

Protezione avanzata contro le minacce tramite il nostro firewall desktop stateful dinamico

A differenza dei firewall di sistema tradizionali che si basano su regole specifiche, McAfee Host Intrusion Prevention for Desktop ha integrato la reputazione delle connessioni di rete di McAfee Global Threat Intelligence (McAfee GTI) per proteggere desktop e notebook da minacce avanzate quali botnet, attacchi DDoS (Distributed Denial-of-Service) e traffico dannoso prima che si verifichi un attacco.

Con l'aumento delle minacce avanzate, McAfee GTI offre uno dei servizi di protezione più sofisticato che si possa distribuire. Funzioni firewall aggiuntive, come le policy su applicazioni e localizzazione, proteggono ulteriormente notebook e desktop in particolare quando non sono collegati alla rete aziendale.

Applica le patch per sistema operativo e applicazioni meno frequentemente, con meno urgenza e al tuo ritmo

Una grande percentuale di exploit viene rilasciata entro soli tre giorni dalla divulgazione delle vulnerabilità. Inoltre, molte aziende impiegano fino a 30 giorni per testare e implementare le patch su tutti gli endpoint. McAfee Host Intrusion Prevention for Desktop colma il vuoto di protezione semplificando e rendendo più efficiente il processo di applicazione delle patch.

- McAfee Host Intrusion Prevention for Desktop protegge da exploit zero-day e vulnerabilità senza patch. In particolare, protegge dalle vulnerabilità Microsoft e Adobe.
- La schermatura delle vulnerabilità aggiorna automaticamente le firme per proteggere gli endpoint contro gli attacchi derivanti dallo sfruttamento delle vulnerabilità.
- Gli aggiornamenti delle firme possono essere scaricati in modo automatico e regolare per garantire la protezione.

Gli endpoint non sono più vulnerabili durante la fase di avvio

Notebook e desktop sono vulnerabili durante la fase di avvio perché le policy di sicurezza non sono ancora state applicate. Durante questo periodo di avvio vulnerabile, gli endpoint potrebbero subire attacchi di rete mentre i servizi di sicurezza potrebbero essere disabilitati. McAfee Host Intrusion Prevention for Desktop blocca l'esecuzione degli attacchi durante questa finestra vulnerabile con una protezione firewall e IPS (Intrusion Prevention System) dell'avvio.

- La protezione firewall dell'avvio abilita solo il traffico in uscita durante l'avvio fin quando la policy firewall completa viene applicata.
- La protezione IPS dell'avvio evita che i servizi di sicurezza vengano disabilitati durante l'avvio finché la policy IPS completa viene applicata.

Requisiti di sistema

Sistemi operativi supportati

- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 SP1, 32 o 64 bit: Business, Enterprise, Ultimate
- Microsoft Windows Embedded Standard 7 SP1, 32 o 64 bit
- Microsoft Windows Vista, 32 o 64 bit: Business, Enterprise, Ultimate
- Microsoft Windows XP Professional 32 bit
- Microsoft Windows XP Professional for Embedded Systems 32 bit
- Microsoft Windows XP Embedded 32 bit

Gestione semplificata e ottimizzata

All'interno di una grande azienda è necessario creare e mantenere molteplici policy firewall e IPS ma è solitamente un'attività noiosa e dispendiosa in termini di tempo. I cataloghi di policy e IPS di McAfee Host Intrusion Prevention for Desktop ottimizzano tale processo, consentendoti di creare e mantenere molteplici policy firewall e IPS che possono essere applicate a diversi gruppi di utenti e riutilizzate secondo necessità.

Ottimizza e semplifica ulteriormente la gestione con il software McAfee® ePolicy Orchestrator® (McAfee ePO™), la nostra unica console centralizzata che aiuta a supervisionare e amministrare la protezione. La completa integrazione con il software McAfee ePO permette di risparmiare tempo e denaro con significative efficienze operative.

Compatibilità con le principali piattaforme di virtualizzazione

La virtualizzazione offre costi inferiori, flessibilità e una manutenzione più semplice del prodotto. McAfee Host Intrusion Prevention for Desktop è compatibile con molte delle principali piattaforme di virtualizzazione tra cui VMware, Citrix e Microsoft.

Per maggiori informazioni visitare **www.mcafee.com/it/products/host-ips-for-desktop.aspx**.

Requisiti di sistema

Piattaforme di virtualizzazione supportate

- Citrix XenServer: 5.0, 5.5
- Citrix XenDesktop: 3.0, 4.0, 7.5, 7.6
- Citrix XenApp: 5.0, 6.0, 6.5
- Citrix Provisioning Services 6.1
- Microsoft App-V: 4.5, 4.6
- Microsoft Hyper-V Server: 2008, 2008 R2
- Microsoft Windows Server: 2008, Hyper-V 2008, 2008 R2, 2012 R2
- Microsoft VDI (Bundle)
- MED-V: 1.0, 1.0 SP1
- SCVMM: 2008, 2008 R2
- SCCM: 2007 SP2, 2007 R2
- SCOM: 2007, 2007 R2
- VMware ACE: 2.5, 2.6
- VMware ESX: 3.5, 4.0, 5.0
- VMware ESXi 5.1
- VMware Player: 2.5, 3.0, 5.0
- VMware Server: 1.0, 2.0
- VMware ThinApp: 4.0, 4.5
- VMware vSphere 4.0
- VMware View: 3.1, 4.0
- VMware Workstation: 6.5, 7.0, 8.0, 9.0
- Windows 7 in modalità XP: 32 e 64 bit

McAfee
Together is power.

Via Fantoli, 7
20138 Milano
Italy
(+39) 02 554171
www.mcafee.com/it