

# McAfee Host Intrusion Prevention for Server

## Protezione avanzata contro le vulnerabilità per server e applicazioni

I server aziendali contengono le risorse informative più preziose dell'azienda e la mantengono operativa. Una delle principali problematiche IT è quella di proteggere in modo efficace tali server e le applicazioni che vi risiedono da attacchi noti e sconosciuti che minacciano l'attività dell'azienda stessa.

### McAfee Host Intrusion Prevention for Server

McAfee® Host Intrusion Prevention for Server offre protezione specifica per server database e web per mantenere l'operatività dei sistemi e la business continuity insieme all'unico firewall stateful dinamico del settore per proteggere dalle minacce avanzate e dal traffico dannoso. Inoltre, offre protezione tramite firme e sistemi comportamentali IPS (Intrusion Prevention System). McAfee Host Intrusion Prevention for Server 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.

### Protezione per server e applicazioni contro gli attacchi e prevenzione della perdita di dati

I server sono sempre più nel mirino degli attacchi perché ospitano grandi quantità di dati aziendali e sono fondamentali per l'esecuzione delle attività quotidiane.

McAfee Host Intrusion Prevention for Server protegge i server mission-critical per mantenere l'operatività e la produttività dei sistemi.

- Protezione dei server web:
  - Filtra le richieste HTTP per prevenire attacchi di tipo directory traversal, Unicode e denial-of-service (DoS).
  - Utilizza policy e regole di schermatura predefinite per prevenire gli attacchi e la perdita dei dati.
- Protezione dei server database:
  - Esamina le query del database per prevenire gli attacchi, come quelli di tipo SQL injection
  - Utilizza policy e regole di protezione predefinite per garantire un comportamento normale e prevenire la manomissione dei dati

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

A differenza dei firewall di sistema tradizionali che si basano su regole specifiche, McAfee Host Intrusion

## 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.

### 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

## SCHEDA TECNICA

Prevention for Server ha integrato la reputazione delle connessioni di rete di McAfee Global Threat Intelligence (McAfee GTI) per proteggere i server 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 la protezione più sofisticata che tu possa distribuire.

### 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 Server colma il vuoto di protezione, semplificando e rendendo più efficiente il processo di applicazione delle patch.

- La protezione è garantita per le 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.

### I server non sono più vulnerabili durante la fase di avvio

I server sono vulnerabili durante la fase di avvio perché le policy di sicurezza non sono state ancora applicate.

Durante questo periodo di avvio vulnerabile, potrebbero subire attacchi di rete mentre i servizi di sicurezza potrebbero essere disabilitati. McAfee Host Intrusion Prevention for Server 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.

### Gestione semplificata e ottimizzata

All'interno di una grande azienda è necessario creare e mantenere molteplici policy firewall e IPS (Intrusion Prevention System) ma è solitamente un'attività noiosa e dispendiosa in termini di tempo. I cataloghi di policy e IPS di McAfee Host Intrusion Prevention for Server ottimizzano tale processo, consentendoti di creare e mantenere molteplici policy firewall e IPS che possono essere applicate 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 piena integrazione con il software McAfee ePO permette di risparmiare tempo e denaro con significative efficienze operative.

Per maggiori informazioni, contattare un rappresentante o visitare il nostro sito web [www.mcafee.com/it](http://www.mcafee.com/it).

## Requisiti di sistema

### Requisiti hardware minimi

- Intel o AMD x86 e x64
- Spazio libero su disco (client): 15 MB, 100 MB durante l'installazione
- Memoria: 256 MB di RAM
- Ambiente di rete: Reti Microsoft o Novell NetWare. Le reti NetWare richiedono TCP/IP
- Scheda di rete Scheda interfaccia di rete; 10 Mbit/s o superiori

### Sistemi operativi supportati

- Microsoft Windows Server 2003 SP2, 2003 R2, 2003 R2 SP2 (tutte le edizioni, 32 e 64 bit)
- Microsoft Windows Server 2008, 2008 SP1, 2008 SP2, 2008 R2 (tutte le edizioni, 32 e 64 bit)
- SPARC Solaris 9 sun4u (32 bit o 64 bit)
- SPARC Solaris 10 sun4u, sun4v (32 bit o 64 bit)
- Red Hat Linux Enterprise 4, 32 bit
  - 2.6.9-5.EL
  - 2.6.9-5.Elhugemem
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 4, 64 bit
  - 2.6.9-5.EL
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 5, 32 bit
  - 2.6.18-8.el5
  - 2.6.18-8.el5PAE
- Red Hat Linux Enterprise 5, 64 bit
  - 2.6.18-8.el5
- SUSE Linux Enterprise 10, 32 bit
  - 2.6.16.21-0.8-bigsm
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp

## SCHEDA TECNICA

### Compatibilità con le principali piattaforme di virtualizzazione

La virtualizzazione è stata adottata praticamente da tutti i dipartimenti IT e la compatibilità con le principali piattaforme di virtualizzazione è essenziale per il

successo di qualsiasi prodotto. McAfee Host Intrusion Prevention for Server 8.0 è compatibile con le tre principali piattaforme di virtualizzazione: VMware, Citrix e Microsoft Hyper-V. La seguente tabella elenca i prodotti supportati da ciascuno di questi tre fornitori.

VMware	Citrix	Microsoft
VMware ESX - 3.5 e 4.0	Citrix XenServer - 5.0 e 5.5	Microsoft Hyper-V Server 2008 e 2008 R2
VMware Vsphere - 4.0	Citrix XenDesktop - 3.0 e 4.0	Microsoft VDI
VMware View - 3.1 e 4.0	Citrix XenApp - 5.0 e 6.0	Microsoft App-V - 4.5 e 4.6
VMware ThinApp - 4.0 e 4.5		Modalità XP su Windows 7
VMware ACE- 2.5 e 2.6		
VMware Workstation 6.5 e 7.0		
VMware Player- 2.5 e 3.0		

### Requisiti di sistema (segue)

#### Sistemi operativi supportati (segue)

- SUSE Linux Enterprise 10, 64 bit
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 11, 32 bit
  - 2.6.27.19-5-default
  - 2.6.27.19-5-pae
- SUSE Linux Enterprise 11, 64 bit
  - 2.6.27.19-5-default

#### Server web supportati

- Microsoft Windows
  - IIS 6.0 e 7.0
- SPARC Solaris
  - Apache 1.3.6 e server web successivi
  - Apache 2.0.42 o server web successivi
  - Apache 2.2.3 o server web successivi
  - Sun Java Web Server 6.1
  - Sun Java Web Server 7.0
- Linux (RHEL e SUSE)
  - Apache 1.3.6 o server web successivi
  - Apache 2.0.42 o server web successivi
  - Apache 2.2.3 o server web successivi

#### Server database supportati

- Microsoft Server Microsoft SQL 2005 e 2008



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

McAfee e il logo McAfee sono marchi registrati o marchi di McAfee, LLC o sue filiali negli Stati Uniti e in altri Paesi. Altri marchi e denominazioni potrebbero essere rivendicati come proprietà di terzi. Copyright © 2017 McAfee, LLC. 17802\_1110B  
NOVEMBRE 2010