



# McAfee Host Intrusion Prevention for Desktop

**Proteção avançada contra vulnerabilidades para desktops e laptops**

## Principais vantagens

### Proteção mais forte

- Imponha a mais ampla cobertura de proteção por IPS e contra ameaças de dia zero em todos os níveis: rede, aplicativo e execução do sistema

### Custos mais baixos

- Reduza o tempo e os custos com um único console poderoso e unificado para distribuição, gerenciamento, geração de relatórios e auditoria de eventos, políticas e agentes
- Aplique patches nos endpoints com menos frequência e menos urgência

### Conformidade simplificada

- Gerencie a conformidade com visualizações decisivas e de fácil compreensão, fluxos de trabalho, monitoramento de eventos e geração de relatórios para investigação e perícia imediatas e adequadas

## Requisitos de sistema

### Sistemas operacionais compatíveis

- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 (SP1, 32 ou 64 bits): Business, Enterprise, Ultimate

O gerenciamento da segurança e o controle da conectividade nos computadores desktop e laptop de uma organização estão cada vez mais difíceis devido ao número crescente de cibercriminosos em busca de lucro e à natureza sofisticada das ameaças atuais. Com o aumento da mobilidade dos funcionários, há uma pressão maior sobre o departamento de TI para assegurar que os usuários se conectem com segurança à rede corporativa. Além disso, as organizações precisam de proteção contra ameaças de dia zero para ter mais tempo para priorizar, testar e distribuir devidamente os patches necessários.

## O desafio

O antivírus sozinho não basta, visto que os ataques e explorações de vulnerabilidades estão sendo lançados mais rapidamente e se tornando mais complexos. A solução é implementar uma estratégia de segurança proativa que evite que os ataques cheguem a acontecer. Com uma abordagem proativa à proteção de endpoints, os departamentos de TI podem assegurar que todos os endpoints e dados confidenciais sejam protegidos e que a continuidade dos negócios seja preservada.

## McAfee Host Intrusion Prevention for Desktop

Como parte integrante dos pacotes de endpoint da Intel® Security, o McAfee® Host Intrusion Prevention for Desktop oferece níveis incomparáveis de proteção contra ameaças de dia zero, conhecidas ou não, ao combinar a proteção de um sistema de prevenção de intrusões (IPS) comportamental e por assinaturas com um firewall dinâmico e com monitoramento de estado. O McAfee Host Intrusion Prevention for Desktop reduz a frequência e a urgência da aplicação de

patches, preserva a continuidade dos negócios e a produtividade dos funcionários, protege a confidencialidade dos dados e simplifica a conformidade regulatória.

## Proteção contra ameaças avançadas através de nosso firewall de desktop dinâmico e com monitoramento de estado

Diferentemente dos firewalls de sistema tradicionais que se baseiam em regras específicas, o McAfee Host Intrusion Prevention for Desktop integra informações sobre reputação das conexões de rede do McAfee Global Threat Intelligence (McAfee GTI) para proteger desktops e laptops contra ameaças avançadas, como redes de bots, negação de serviços distribuída e tráfego malicioso emergente antes que os ataques possam ocorrer. Com o aumento das ameaças avançadas, o McAfee GTI oferece um dos serviços de proteção mais sofisticados que você pode distribuir. Recursos de firewall adicionais, como políticas de aplicativos e localizações, protegem ainda mais os laptops e desktops, especialmente quando estes não se encontram na rede corporativa.

- Microsoft Windows Embedded Standard 7 (SP1, 32 ou 64 bits)
- Microsoft Windows Vista (32 ou 64 bits): Business, Enterprise, Ultimate
- Microsoft Windows XP Professional (32 bits)
- Microsoft Windows XP Professional for Embedded Systems (32 bits)
- Microsoft Windows XP Embedded (32 bits)

### Plataformas de virtualização compatíveis

- 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 (incluído com outro produto)
- 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
- XP Mode Windows 7: 32 e 64 bits

### Aplique patches de aplicativos e do sistema operacional com menos frequência, menos urgência e quando for mais conveniente para você

Uma grande porcentagem de explorações é lançada até três dias após a divulgação das vulnerabilidades. Ainda assim, muitas organizações levam até 30 dias para testar e distribuir patches para todos os endpoints. O McAfee Host Intrusion Prevention for Desktop fecha essa brecha na segurança e torna o processo de aplicação de patches mais fácil e mais eficiente.

- O McAfee Host Intrusion Prevention for Desktop defende contra explorações de dia zero e vulnerabilidades não corrigidas. A proteção é fornecida tanto contra vulnerabilidades da Microsoft quanto da Adobe.
- O isolamento das vulnerabilidades atualiza automaticamente as assinaturas para proteger os endpoints contra ataques resultantes da exploração de vulnerabilidades.
- As atualizações de assinaturas podem ser obtidas automaticamente e regularmente por download para garantir a proteção.

### Os endpoints não ficam mais vulneráveis durante a inicialização

Os laptops e desktops ficam vulneráveis durante a inicialização porque as políticas de segurança ainda não foram impostas. Durante esse tempo de inicialização vulnerável, os endpoints podem estar sujeitos a ataques com base em rede e os serviços de segurança podem ser desativados. O McAfee Host Intrusion Prevention for Desktop impede a ocorrência de ataques durante esse período de vulnerabilidade com a proteção de inicialização oferecida pelo firewall e pelo sistema de prevenção de intrusões (IPS).

- A proteção por firewall na inicialização só permite tráfego de saída durante a inicialização, até que política de firewall completa tenha sido imposta.
- A proteção por IPS na inicialização impede que seus serviços de segurança sejam desativados durante a inicialização, até que a política de IPS completa tenha sido imposta.

### Gerenciamento simplificado e otimizado

A criação e a manutenção de múltiplas políticas de firewall e IPS são necessárias em uma grande organização, mas isso costuma ser tedioso e demorado. Os catálogos de IPS e as políticas do McAfee Host Intrusion Prevention for Desktop simplificam esse processo, permitindo que você crie e mantenha múltiplas políticas de IPS e firewall que podem ser aplicadas a diferentes grupos de usuários e reutilizadas conforme a necessidade.

Otimize e simplifique ainda mais o gerenciamento com o software McAfee ePolicy Orchestrator® (McAfee ePO™), nosso console único e centralizado que ajuda a supervisionar e a administrar toda a sua proteção. Uma integração completa com o software McAfee ePO economiza dinheiro e tempo, com eficiências operacionais significativas.

### Compatibilidade com as principais plataformas de virtualização

A virtualização oferece custos mais baixos, flexibilidade e manutenção mais fácil do produto. O McAfee Host Intrusion Prevention for Desktop é compatível com muitas das principais plataformas de virtualização, incluindo VMware, Citrix e Microsoft.

Para obter mais informações, visite [www.mcafee.com/br/products/host-ips-for-desktop.aspx](http://www.mcafee.com/br/products/host-ips-for-desktop.aspx).



McAfee. Part of Intel Security.

Av. das Nações Unidas, 8.501 - 16º andar  
CEP 05425-070 - São Paulo - SP - Brasil  
Telefone: +55 (11) 3711-8200  
Fax: +55 (11) 3711-8286  
[www.intelsecurity.com](http://www.intelsecurity.com)