

# McAfee Host Intrusion Prevention for Server

## 针对服务器和应用程序的高级漏洞防护

企业服务器用于存储组织最有价值的信息资产并确保业务正常运转。一个最主要的 IT 挑战是成功地防止这些服务器以及服务器上托管的应用程序遭受已知和未知的攻击，否则会有导致业务中断的风险。

### McAfee Host Intrusion Prevention for Server

McAfee® Host Intrusion Prevention for Server 可提供专业的 Web 和数据库服务器保护，从而维持系统运行时间和业务持续性，同时使用行业唯一的动态且有状态的防火墙防范高级威胁和恶意通信。此外，它还提供了特征码和行为入侵防护系统 (IPS) 保护。McAfee Host Intrusion Prevention for Server 可降低发布补丁的频率和紧急程度，保持业务连续性和员工工作效率，保护数据的机密性，并简化监管合规流程。

### 保护服务器和应用程序，防止遭受攻击和造成数据丢失

针对服务器的攻击越来越多，因为服务器上托管了大量的企业数据，并且对于日常活动的执行至关重要。McAfee Host Intrusion Prevention for Server 可保护任务关键型服务器以维持系统运行时间和生产力。

#### ■ Web 服务器保护：

- 过滤 HTTP 请求以防范目录遍历、Unicode 和拒绝服务 (DoS) 攻击。
- 使用预定义的防护策略和规则防止攻击和数据丢失。

#### ■ 数据库服务器保护：

- 检查数据库查询以防范攻击，如 SQL 注入。
- 使用预定义的防护策略和规则来确保行为正常，防止篡改数据。

### 通过动态的有状态的系统防火墙实现高级威胁防护

与依赖特定规则的传统系统防火墙不同，McAfee Host Intrusion Prevention for Server 已经集成了 McAfee Global Threat Intelligence (McAfee GTI) 网络连接信誉功能，可在攻击发生之前为服务器防范高级威胁，如僵尸网络、分布式拒绝服务 (DDoS) 以及新兴恶意通信。随着高级威胁的与日俱增，McAfee GTI 可为您提供最精细的保护，供您部署。

## 主要优势

### 更强大的保护

- 在各个级别均执行最广泛的 IPS 和零日威胁防护：网络、应用程序和执行。

### 成本更低

- 利用一款强大而统计的控制台进行部署、管理、报告并审核事件、策略和代码，可减少时间，降低成本。
- 修补终端的频率更低，且紧迫性也会减弱。

### 简化法规遵从

- 利用简单易懂的可操作视图、 workflow、事件监控和报告来管理合规性，可实现及时有效的调查和签证。

## 产品简介

### 降低应用操作系统和应用程序补丁的频率，减少紧急修补工作，自行管理修补计划

绝大部分对漏洞的利用都发生在披露漏洞信息后三天内。然而，大多数组织可能需要长达 30 天才能对所有终端测试和部署补丁。

McAfee Host Intrusion Prevention for Server 弥补了这一安全缺陷，同时简化了修补过程并提高了效率。

- 对于 Microsoft 和 Adobe 漏洞，保护均有提供。漏洞防护会自动更新特征码，从而防止终端遭受从被利用的漏洞发起的攻击。
- 为了实现妥善的保护，特征码更新既可自动执行，也可以定期执行。

### 服务器在启动时不再容易遭受攻击

服务器在启动时容易遭受攻击，因为这时还没有执行安全策略。在容易遭受攻击的启动期间，服务器可能遭受基于网络的攻击，而安全服务可能处于禁用状态。McAfee Host Intrusion Prevention for Server 利用防火墙和 IPS 启动保护，可在此容易遭受攻击的窗口期内阻止攻击发生。

- 启动防火墙保护在启动过程中仅允许出站通信，直到实施了完整的防火墙策略为止。
- 启动 IPS 保护在启动过程中可阻止禁用我们的安全服务，直到实施了完整的 IPS 策略为止。

### 简化管理

在一个大型组织内，必须创建和维护多个防火墙和入侵防护系统 (IPS) 策略，但这通常会很麻烦而耗时。McAfee Host Intrusion Prevention for Server 策略和 IPS 目录简化了这一过程，允许您创建和维护多个可根据需要维护的防火墙和 IPS 策略。

利用我们统一的集中式 McAfee® ePolicy Orchestrator® (McAfee ePO™) 软件可以进一步优化和简化管理工作，帮助您监督并管理所有保护。与 McAfee ePO 软件的完全集成可提高效率，为您节省金钱和时间。

有关详细信息，请与代表联系，或者访问我们的网站，网址为：[www.mcafee.com/cn](http://www.mcafee.com/cn)。

## 系统要求

### 最低硬件要求

- Intel 或 AMD x86 和 x64
- 可用磁盘空间 (客户端)：15 MB，但在安装期间需要 100 MB
- 内存：256 MB RAM
- 网络环境：Microsoft 或 Novell NetWare 网络。NetWare 网络需要 TCP/IP
- NIC：网络接口卡：10 mbps 或更高配置

### 支持的操作系统

- Microsoft Windows Server 2003 SP2、2003 R2、2003 R2 SP2 (所有版本，32 和 64 位)
- Microsoft Windows Server 2008、2008 SP1、2008 SP2、2008 R2 (所有版本，32 和 64 位)
- SPARC Solaris 9 sun4u (32 和 64 位)
- SPARC Solaris 10 sun4u、sun4v (32 和 64 位)
- Red Hat Linux Enterprise 4, 32 位
  - 2.6.9-5.EL
  - 2.6.9-5.Elhugemem
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 4, 64 位
  - 2.6.9-5.EL
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 5, 32 位
  - 2.6.18-8.el5
  - 2.6.18-8.el5PAE
- Red Hat Linux Enterprise 5, 64 位
  - 2.6.18-8.el5
- SUSE Linux Enterprise 10, 32 位
  - 2.6.16.21-0.8-bigsmpp
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp

## 产品简介

### 与主流虚拟平台兼容

几乎所有 IT 部门都会采用虚拟化技术，那么任何产品要取得成功，与主流虚拟平台的兼容性就成为了关键所在。

McAfee Host Intrusion Prevention for Server 8.0 与三款主流虚拟平台兼容: VMware、Citrix 和 Microsoft Hyper-V。下表列出了这三家供应商分别支持的产品。

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

### 系统要求 (续)

#### 支持的操作系统 (续)

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

#### 支持的 Web 服务器

- Microsoft Windows
  - IIS 6.0 和 7.0
- SPARC Solaris
  - Apache 1.3.6 和更高版本的 Web 服务器
  - Apache 2.0.42 或更高版本的 Web 服务器
  - Apache 2.2.3 或更高版本的 Web 服务器
  - Sun Java Web Server 6.1
  - Sun Java Web Server 7.0
- Linux (RHEL 和 SUSE)
  - Apache 1.3.6 或更高版本的 Web 服务器
  - Apache 2.0.42 或更高版本的 Web 服务器
  - Apache 2.2.3 或更高版本的 Web 服务器

#### 支持的数据库服务器

- Microsoft SQL Server 2005 和 2008



北京市东城区北三环东路 36 号  
北京环球贸易中心 D 座 18 层, 100013  
电话: 8610 8572 2000  
[www.mcafee.com/cn](http://www.mcafee.com/cn)

McAfee、迈克菲和 McAfee 徽标是 McAfee, LLC 或其分支机构在美国和/或其他国家/地区的注册商标或商标。其他商标和品牌可能是其各自所有者的财产。  
Copyright © 2017 McAfee, LLC. 17802\_1110B  
2010 年 11 月