McAfee Network Security Platform

全面、智能的高级威胁防护平台

McAfee® Network Security Platform 是下一代入侵检测与防护系统 (IDPS)，它能够发现并阻止网络中复杂的恶意软件威胁。该平台利用高级检测和模拟技术，超越了单纯的模式限制，从而以高准确性抵御隐匿攻击。为了满足要求苛刻的网络的需求，该平台只需单台设备即可将速度扩展至 30 Gbps 以上，当多个设备堆叠在一起时，最多可将速度扩展至 100 Gbps。这种集成的 McAfee 解决方案组合通过将实时 McAfee® Global Threat Intelligence 信息与丰富的用户、设备和应用程序环境数据相结合来简化安全操作，从而快速准确地对网络传播带来的攻击作出响应。

主要优势

- 快速检测和阻止威胁以保护应用程序和数据
- 面向动态环境的高性能可扩展解决方案
- 可见性和控制性良好的集中式管理
- 高级检测，包括无特征码恶意软件分析
- 可检测网络流量的入站和出站 SSL 解密
- 高可用性和灾难恢复保护
- 虚拟设备可用
- 与 McAfee 解决方案产品组合集成，保护设备到云安全

抵御当今的隐匿威胁

数字化使安全态势发生了显著变化。云、移动性和物联网 (IoT) 将互联性推向了新高度，而要保护的领域已扩展到没有实际“边际”或边界的程度。安全风险的数量和严重性几乎在一夜之间成倍增长。许多企业已将注意力转移到保护数据上。因此，强大的网络安全策略是保护数据的关键所在。您的网络面临一些高级的隐匿攻击，这些攻击能够避开传统检测方法，从而使您的应用程序和数据面临严重的违规和中断风险。遗憾的是，大部分企业缺乏财务和运营资源，无法实施和管理提供充分安全防护所需的工具和技术。

McAfee Network Security Platform 将智能威胁防御功能与直观的安全管理相结合，从而提高检测准确度并简化安全操作。任何一项恶意软件检测技术均无法抵御所有攻击，这也正是 McAfee Network Security Platform 综合运用多个特征码和无特征码检测引擎，以共同防止有害恶意软件破坏网络的原因。它使用高级技术组合（包括完整协议分析、威胁信誉和行为分析）对网络流量进行深度检测，从而检测和防御恶意软件回拨、拒绝服务 (DoS)、零日攻击和其他高级威胁。

集成式安全

McAfee Network Security Platform 与 McAfee® Advanced Threat Defense 进行了集成，从而将深度静态代码分析、动态分析（恶意软件沙盒）和机器学习相结合，以便检测零日威胁，包括使用规避技术的威胁和勒索软件。McAfee Network Security Platform 还结合了 McAfee Global Threat Intelligence 的文件信誉功能，并与 McAfee® ePolicy Orchestrator® 软件和 McAfee® Enterprise Security Manager

联系我们

进行了集成，从而实时关联所有相关来源的网络事件。这种综合性解决方案充分利用设备详细信息、用户信息、终端安全状况、漏洞评估及其他丰富的信息，帮助组织更深入地了解威胁的严重性和业务风险因素。

性能和可用性

McAfee Network Security Platform 可提供最佳安全保护和高性能优势。该平台将基于协议的单通道检测体系结构与专门构建的运营商级别硬件完美结合，实现了超过 100 Gbps 的实际检测速度。无论安全设置如何，这种高效的体系结构都能持续保持高性能；而其他 IPS 解决方案在采用“注重安全防护而舍弃性能”的策略后，吞吐量会降低高达 50%。

McAfee Network Security Platform 还提供具有状态故障转移的“主动-主动”和“主动-被动”模式，让您能够满足高可用性 SLA 的要求，同时避免陷入低性能设备或负担过重的独立解决方案的瓶颈。

可扩展的硬件平台能够提供投资保护

McAfee NS7500 和 NS9500 系列设备为客户提供了灵活性，使客户能够购买当前所需的产品，并且可以通过软件许可证轻松地按需扩展吞吐量。对于 McAfee NS9500 设备，还可以通过堆叠多个 McAfee NS9500 设备来增加容量。

可见性和控制性

做出有关网络上的应用程序和协议的明智决策。McAfee Network Security Platform 是第一款将高级威胁防护和应用程序感知技术融入单一安全决策引擎的 IDPS 解决方案。我们将威胁活动与应用程序使用情况（包括对 2000 多个应用程序和协议的 7 层监控）关联起来，以便您能够对网络上允许使用哪些应用程序做出更加明智的决策。

除应用程序标识外，McAfee Network Security Platform 还可提供用户和设备可见性。通过识别异常网络行为对主机和用户面临的风险进行优先级排序，包括活跃的僵尸网络。

智能化可扩展安全管理

通过智能网络安全管理，充分利用您的安全投资。McAfee Network Security Manager 提供基于 Web 的可扩展式管理，可对两台至数百台网络安全设备进行管理。它提供了直观的渐进式披露工作流程，能够指导管理员通过相关警报及易于使用的安全信息显示板，根据警报严重性和相关性自动确定事件优先顺序。

其他功能

高级威胁防护

- 入站安全套接字层 (SSL) 解密支持使用基于代理的共享密钥解决方案的 Diffie-Hellman (DH) 和椭圆曲线 Diffie–Hellman (ECDH) 加密，而对传感器性能几无影响（对于 NS 系列，正在申请专利）。
- 出站 SSL 解密（NS 系列）
- McAfee® Gateway Anti-Malware 模拟引擎
- PDF JavaScript 模拟引擎
- Adobe Flash 行为分析引擎
- Microsoft Office 深度文件检查引擎
- 高级抗逃避防护
- 移动威胁信誉和云分析

僵尸网络及恶意软件回拨保护

- DNS/DGA 快速通量回拨检测
- DNS 排除
- 启发式僵尸程序检测
- 多种攻击关联
- 命令和控制数据库

高级入侵防护

- IP 碎片整理和 TCP 流重组
- McAfee 特征码、用户定义的特征码和开源特征码
- Snort 特征码的本地支持（NS 系列）
- 增强允许列表/阻止列表以支持 Structured Threat Information eXpression (STIX)（McAfee NS 系列）
- 主机隔离和速率限制
- 虚拟环境检测
- 与 McAfee Advanced Threat Defense 集成
- HTTP 响应解压支持

DoS 和 DDoS 预防

- 阈值和启发式检测
- 基于主机的连接限制
- 基于配置文件的自学习检测

McAfee Global Threat Intelligence

- 文件、IP 和 URL信誉
- 应用程序和协议信誉
- 地理位置
- 根据 McAfee Global Threat Intelligence 类别列入允许列表

高可用性

- 具有状态故障转移的“主动-主动”和“主动-被动”模式
- 外部失效开放（主动）
- 内置失效开放

协议隧道支持

- IPv6
- V4-in-V4、V4-in-V6、V6-in-V4 和 V6-in-V6 隧道
- MPLS
- GRE
- Q-in-Q 双 VLAN

McAfee Network Security Manager

- 分层管理（多达 1000 个传感器）
- 用户身份验证（RADIUS 和 LDAP）
- 自动故障转移和故障恢复
- 关键配置数据的灾难恢复
- 集中式分层策略管理
- 内存信息显示板详细说明了设备内存利用情况

了解更多

有关物理设备选项的更多详细信息，请参阅 McAfee Network Security Platform 规格表。

了解有关 What To Look For in an IDPS（要在 IDPS 中查找的内容）的更多信息。

McAfee 技术的特性和优势取决于系统配置，并且可能需要已启用硬件、软件或服务激活。请访问 www.mcafee.com/cn 了解更多信息。没有绝对安全的网络。

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