

Symantec™ Network Access Control

全面的端点遵从

概述

Symantec Network Access Control 是全面的端到端网络访问控制解决方案，通过与现有网络基础架构相集成，使企业能够安全有效地控制对企业网络的访问。不管端点以何种方式与网络相连，Symantec Network Access Control 都能够发现并评估端点遵从状态、设置适当的网络访问权限、根据需要提供补救功能，并持续监视端点以了解遵从状态是否发生了变化。从而可以营造这样的网络环境：企业可以在此环境中大大减少安全事故，同时提高企业 IT 安全策略的遵从级别。

Symantec Network Access Control 使企业可以按照目标经济有效地部署和管理网络访问控制。

同时对端点和用户进行授权

在当今的计算环境中，企业和网络管理员面临着严峻的挑战，即为不断扩大的用户群提供访问企业资源的权限。其中包括现场和远程员工，以及访客、承包商和其他临时工作人员。现在，维护网络环境完整性的任务面临着前所未有的挑战。如今无法再接受对网络提供未经检查的访问。随着访问企业系统的端点数量和类型激增，企业必须能够在连接到资源以前验证端点的健康状况，而且在端点连接到资源之后，要对端点进行持续验

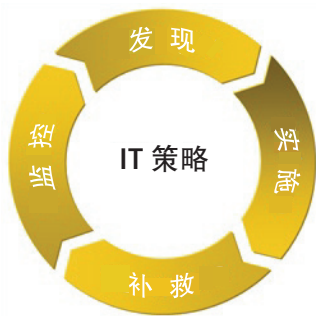
证。Symantec Network Access Control 可以确保在允许端点连接到企业 LAN、WAN、WLAN 或 VPN 之前遵从 IT 策略。

主要优势

部署 Symantec Network Access Control 的企业可以切身体验到众多优势。其中包括：

- 减少恶意代码（如病毒、蠕虫、间谍软件和其它形式的犯罪软件）的传播
- 通过对访问企业网络的不受管理的端点和受管理的端点加强控制，降低风险
- 为最终用户提供更高的网络可用性，并减少服务中断的情况
- 通过实时端点遵从数据获得可验证的企业遵从信息
- 企业级集中管理架构将总拥有成本降至最低
- 验证对防病毒软件和客户端防火墙这样的端点安全产品投资是否得当
- 与 Symantec™ AntiVirus™ Advanced Endpoint Protection 无缝集成

主要功能



Symantec Network Access Control 流程

网络访问控制流程

网络访问控制是一个流程，涉及对所有类型的端点和网络进行管理。此流程从连接到网络之前开始，在整个连接过程中持续进行。与所有企业流程一样，策略可以作为评估和操作的基础。

网络访问控制流程包括以下四个步骤：

- 1. 发现和评估端点。**此步骤在端点连接到网络访问资源之前执行。通过与现有网络基础架构相集成，同时使用智能代理软件，网络管理员可以确保按照最低 IT 策略要求对连接到网络的新设备进行评估。
- 2. 设置网络访问权限。**只有对系统进行评估并确认其遵从 IT 策略后，才准予该系统进行全面的网络访问。对于不遵从 IT 策略或不满足企业最低安全要求的系统，将对其进行隔离，限制或拒绝其对网络进行访问。

- 3. 对不遵从的端点采取补救措施。**对不遵从的端点自动采取补救措施使管理员能够将这些端点快速变为遵从状态，随后再改变网络访问权限。管理员可以将补救过程完全自动化，这样会使该过程对最终用户完全透明；也可以将信息提供给用户，以便进行手动补救。
- 4. 主动监视遵从状况。**必须时刻遵从策略。因此，Symantec Network Access Control 以管理员设置的时间间隔主动监视所有端点的遵从状况。如果在某一时刻端点的遵从状态发生了变化，那么该端点的网络访问权限也会随之变化。

全方位的端点防护

网络由新企业系统、早期企业系统、承包商系统、访客系统、公共服务站、业务合作伙伴以及其它无数未知系统组成。对于其中大部分端点，管理员施加的控制少之又少，甚至不予以控制，但又必须确保网络的安全性和可用性。Symantec Network Access Control 使企业能够将网络访问控制过程应用于受控或不受控的系统、旧系统或新系统以及未知或已知的系统。

可在任何网络中部署

典型的企业用户通过多种访问方法连接到网络；因此，管理员必须拥有足够的灵活性，可以在不考虑连接类型的情况下一致应用评估和连接控制。作为当今市场上最成熟的网络访问控制解决方案之一，Symantec Network

Access Control 使网络管理员能够通过对网络基础架构的现有投资主动实施遵从，而不需要升级网络设备。

不管是使用直接集成到网络中的某个 Symantec Network Access Control Enforcer（仅主机实施选项不要求进行网络集成），还是使用集成到 Web 应用环境中的可分解代理，企业都能够确保最终用户和端点在接入企业网络时保持遵从。

Symantec Network Access Control 架构

Symantec Network Access Control 架构包括以下三个核心组件：策略管理、端点评估和网络实施。这三个组件都作为一个解决方案协同工作，不需要依赖于外部元素来发挥其功能。

集中的策略管理和报告

企业级的管理控制台对任何解决方案的有效运作都至关重要。Symantec Endpoint Protection Manager 提供了一个基于 Java™ 技术的控制台，可以集中创建、部署、管理和报告代理及强制服务器的活动。策略管理器伸缩自如，可以适应当今要求最为苛刻的环境，它在一个可用性极高的架构中为所有管理任务提供了精细的控制。

端点评估

网络访问控制可以保护网络免遭恶意代码以及未知或未授权端点的攻击；此外，它还可以验证与该网络相连的端点是否经过正确配置，以保护其免遭在线攻击。不管目标是什么，该过程都是首先从评估端点入手。尽管检查防病毒软件、反间谍软件和安装补丁程序是允许进行网络访问最常见的几个最低要求，但是在进行了初始网络访问控制部署后，大多数企业很快就超出了这些最低要求。

Symantec Network Access Control 提供了三种不同的端点评估技术来确定端点遵从。

- **永久代理。**企业拥有的系统和其它受控的系统使用管理员安装的代理来确定遵从状态。它检查防病毒软件、反间谍软件和安装的补丁程序以及复杂的系统状态特征，如注册表项、运行进程和文件属性。永久代理还提供最深入、最准确、最可靠的系统遵从信息，同时为评估选项提供最灵活的补救和修复功能。
- **可分解的代理。**对于当前不受管理员管理的非企业设备或系统，基于 Java 的代理是根据要求提供的，不需要管理员权限即可评估端点遵从状况。在会话结束时，这些代理会将其自身从系统中自动移除。

- **远程漏洞扫描。**远程漏洞扫描根据来自 Symantec Network Access Control Scanner 的无证书证明的远程漏洞扫描结果，向 Symantec Network Access Control 实施基础架构提供遵从信息。远程扫描可以将此信息收集功能拓展到当前无基于代理的技术可用的系统。

实施

每个企业网络环境的发展都不尽相同，因此，没有任何一种实施方法能够有效控制对网络上所有点的访问。网络访问控制解决方案必须具有足够的灵活性，这样才能在不增加管理和维护开销的前提下，将多种实施方法轻松集成到现有环境中。Symantec Network Access Control 允许您针对网络的不同部分选择最合适的实施方法，并不会增加操作复杂性或成本。每种基于网络的实施方法要么只以软件的形式提供，要么作为硬件设备交付的组件提供。

- **LAN Enforcer 802.1X** 是带外 802.1X RADIUS 代理解决方案，它与支持 802.1X 标准的所有主要交换供应商协同工作。LAN Enforcer 可以参与对用户和端点进行身份验证的现有 AAA 身份管理架构；对于只要求进行端点遵从验证的环境，也可以充当独立的 RADIUS 解决方案。LAN Enforcer 可根据连接端点的身份验证结果设置交换机端口访问权限。
- 将 **DHCP Enforcer** 以内嵌方式部署在端点和现有 DHCP 服务基础架构之间，充当 DHCP 代理。在对策略遵从

状况进行验证之前，为实施的所有端点提供限制性的 DHCP 租用分配，此时会将一个新 DHCP 租用分配给端点。DHCP Enforcer 与 Microsoft® DHCP Server 插件的集成可以实现网络访问控制的快速部署，而不需要在网络上部署其它设备。

- **Gateway Enforcer** 是在网络瓶颈点处使用的内嵌实施设备。它根据远程端点的策略遵从情况控制通过设备的通信流。不管瓶颈点是位于边界网络连接点上（如 WAN 链接或 VPN），还是位于访问关键业务系统的内部网段上，Gateway Enforcer 都可以对资源和补救服务有效提供可控访问。
- **自我实施**利用了 Symantec Protection Agent 中基于主机的防火墙功能，可以根据端点遵从状态调整本地代理策略。对于像笔记本电脑这样经常在多个网络之间移动的设备，此功能使管理员能够控制对任何网络的访问以及企业网络的开启或关闭。

Cisco Network Admission Control 和 Microsoft Network Access Protection

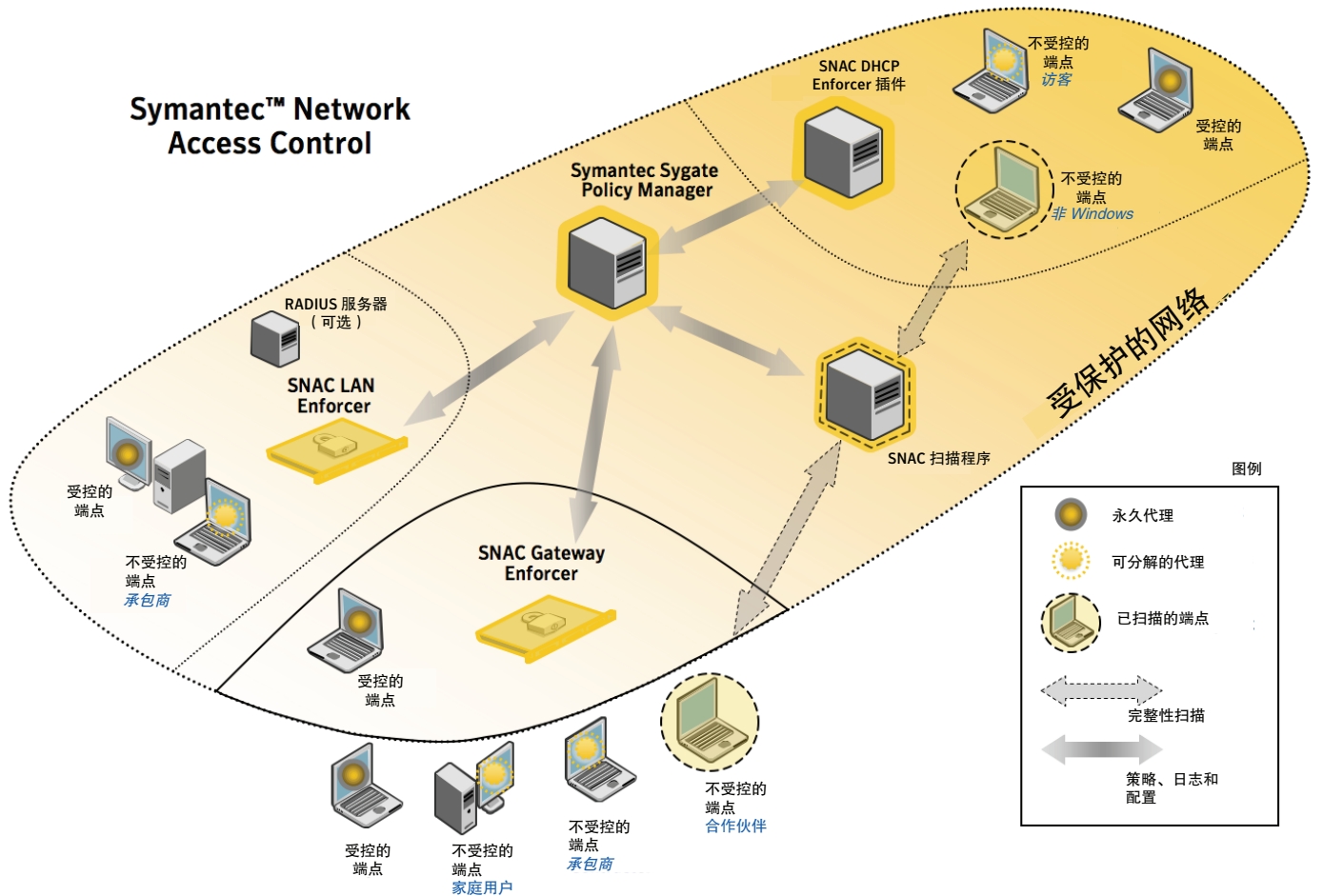
Symantec Network Access Control 不需要外部解决方案即可提供端到端控制功能，此外，它还与其它网络访问控制技术相集成并进行了增强。无论采用何种实施方法，安全管理员都可以确保他们拥有全面的控制。

支持服务

赛门铁克还提供广泛的咨询、技术培训和支服务，可以指导企业完成 Symantec Network Access Control 的迁移、部署和管理，并帮助他们实现投资的全部价值。对于希望外包安全监控和管理的企业，赛门铁克还提供托管安全服务，以提供实时安全防护。

Symantec Network Access Control 产品系列

	Symantec Network Access Control	Symantec Network Access Control Starter Edition
实施		
LAN 802.1x	X	
DHCP	X	
网关	X	X
自我实施	X	X
端点评估		
永久代理	X	X
可分解的代理	X	
远程漏洞扫描	X	



系统要求

平台支持

Symantec Endpoint Protection Manager

- Microsoft® Windows® 2003 (32 位和 64 位)
- Microsoft Windows XP (32 位)
- Microsoft Windows 2000—SP3 及更高版本 (32 位)

Symantec Endpoint Protection Manager 控制台

- Microsoft Vista® (32 位和 64 位)
- Microsoft Windows 2003 (32 位和 64 位)
- Microsoft Windows XP (32 位和 64 位)
- Microsoft Windows 2000—SP3 及更高版本 (32 位)

Symantec Network Access Control 客户端

操作系统：

- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Datacenter Server
- Windows XP Home Edition 或 Windows XP Professional
- Windows XP Tablet Edition
- Windows Server 2003 Standard 或 Windows Server 2003 Enterprise
- Mac OS X 10.4 或更高版本

Symantec Network Access Control Scanner

操作系统：

- Windows 2000 Server SP4
- Windows 2003 Server SP1

最低处理器要求：Intel® Pentium® 4 1.8 GHz

至少 1 GB 内存

1 GB 可用硬盘空间

Internet Explorer® 5.5 或更高版本 Windows 2000 Professional

Symantec Network Access Control Enforcer 6100 系列

基本硬件设备选件 (网关、局域网和 DHCP)

机架单位	1
尺寸	1.68" x 17.60" x 21.5"
处理器	1 2.8-GHz Intel Pentium 4 处理器
内存	1 GB
存储	1 160-GB (SATA)

故障开放硬件设备选件 (网关、局域网和 DHCP)

机架单位	1
尺寸	1.68" x 17.60" x 21.5"
处理器	1 2.8-GHz Intel Pentium 4 处理器
内存	1 GB
存储	1 160-GB (SATA)

Microsoft DHCP Server 插件选件 (直接安装在 Microsoft DHCP 服务器上，消除了对外部 DHCP Enforcer 设备的需要)

关于赛门铁克

赛门铁克公司是全球领先的基础架构软件供应商，致力于确保企业和个人消费者在互联世界中的信心。赛门铁克公司帮助用户保护基础架构、信息和交互，提供软件和服务来抵御对安全性、可用性、遵从和性能方面的风险威胁。公司总部设在美国加州的 Cupertino，现已在 40 多个国家设有分支机构。要了解更多信息，欢迎访问赛门铁克公司网站：www.symantec.com。

联系我们：赛门铁克中国销售部

如果您需要咨询销售方面的问题，请拨打下面的电话或发送电子邮件，同时请说明信息的来源（“NAC11.0 Data Sheet”）

免费电话： 800 810 8826

电子邮件地址：china-sales@symantec.com

欲知详情，请访问中文网址：www.symantec.com.cn

或垂询各地办事处：

赛门铁克中国地区办事处

北京： 电话：(010)85180008 传真：(010)85186718

电话：(010)85183338 传真：(010)85186928

上海： 电话：(021)32174788 传真：(021)52925291

广州： 电话：(020)38771799 传真：(020)38771877

成都： 电话：(028)86768282 传真：(028)86768598

全国销售热线： 800 810 8826

安全产品售后技术支持热线： 800 810 3992

高可用性产品售后技术支持热线： 800 810 9771

互联世界 · 满怀信心  symantec™