

Symantec™ Client Security

通过集成的防病毒、防火墙和入侵检测，为远程、移动和联网客户端系统提供威胁防护

集成客户端安全产品的需求

越来越多的移动和远程用户需要访问企业网络，这要求企业为网络和远程系统中的关键业务资产提供保护。许多企业都采用分散于整个企业的点产品，但这一方式却不能提供充分地保护，并且需要较高的实施和管理成本。举例来说，由于混合型威胁（如Nimda、Code Red和Blaster）专门设计来规避当今企业外围的常见安全产品，因而很难防范。此外，由于这些产品缺乏集中式管理功能，安全管理员很难识别并实时响应合法威胁。

通过中央控制台，Symantec Client Security 提供集成的防病毒、防火墙和入侵检测功能，能够主动防御当今不断演进地混合型威胁。

集成的安全管理

通过赛门铁克系统中心™集成的安全管理提供对防病毒、防火墙和入侵检测功能的全面管理。管理能力包括：

- 从一个控制台进行集中管理：通过赛门铁克系统中心，管理员可以从一个管理控制台配置、安装、管理和更新客户端病毒防护、防火墙和入侵检测功能，并配置、实施和执行企业的网络策略。管理员还可以安装 Symantec Client Security，并通过中央管理控制台，在管理服务器之间轻松移动客户端。对每项集成技术的集中日志记录和警报有助于将安全数据转化为可操作信息。可管理的内容执行确保系统具有最新的客户端安全内容更新。
- 客户端安全策略的创建和部署：合并策略文件功能可合并防火墙规则，使管理员不必手动集成或创建新规则。策略测试按钮使部署的客户端防火墙策略能够正常执行。包括以下三种预配置防火墙策略：标准、远程和强化。管理员可以配置和锁定防病毒和客户端防火墙策略，以便控制各种活动，如：何时打开实时扫描程序，检测到病毒、蠕虫或特洛伊木马时将采取什么措施，以及允许终端用户与产品进行哪些交互操作等。
- SYMANTEC™ VPN SENTRY：使管理员能够确保通过 VPN 和登录脚本连接到企业资源的移动和远程系统符合安全策略。此外，它还检查以确保已安装防病毒软件，已打开实时防护，已更新病毒定义，已安装和激活客户端软件，并遵循适当的安全策略。管理员还可以通过 VPN 服务器创建各种策略，使不兼容的系统能够访问网络资源，以帮助解决兼容性问题。

主要特点

- › 保护联网PC、关键系统和移动用户不会遭到网络入侵，并防御病毒、特洛伊木马和蠕虫
- › **新!** Symantec VPN Sentry 可确保远程和移动用户能够完全符合企业策略
- › **新!** 位置意识确保企业安全策略在任何位置都得到遵循
- › **新!** 客户端配置最大限度地减少终端用户的警报数
- › **新!** 威胁跟踪器可识别通过开放式文件共享进行扩散的混合型威胁的来源（如 Nimda）
- › **新!** 出站电子邮件蠕虫启发式检测可防止客户端系统通过电子邮件扩散蠕虫
- › **新!** 扩展的威胁检测可识别不受欢迎的应用程序如 spyware 和 adware
- › **新!** 对通过 pop 3 邮件客户端（如 Microsoft® Outlook®、Eudora® 和 Netscape Mail）传输的传入邮件，进行附件扫描
- › **新!** 内存中扫描可检测威胁，并在威胁造成破坏之前，终止可疑进程

- **逻辑组管理：**管理员可以创建和管理服务器组中客户端和服务器的逻辑分组，或一台父服务器的多个逻辑组。尤其适用于需要采用同一种方式处理相似功能项（例如部门或业务单位）的企业，可以降低基础架构成本。
- **安装和迁移：**Symantec Client Security 现在包括新的 Microsoft Installer，能够对防病毒、防火墙和入侵检测组件的安装包进行预配置。所需的安装空间大小已经从 50 MB 降低到 25 MB 以下。提供以下三种预配置部署选项：完全管理、部分管理和瘦客户端。此外，安全软件卸载程序最大限度地减少了从第三方防病毒产品转换到 Symantec Client Security 的成本。
- **集中的网络审核：**管理员不但能够确定哪些节点未受保护，容易受到病毒攻击，而且能够确定哪些节点受到了 Symantec AntiVirus、McAfee® VirusScan™、Trend Micro™ Office Scan™、Computer Associates® 或其他第三方防病毒产品的保护。
- **可扩展防护：**通过赛门铁克系统中心，管理员可以管理几十万个客户端。
- **降低总体拥有成本：**通过增强的安全管理，包括集中的事件管理和响应功能，Symantec Client Security 减轻了管理负担，有助于降低网络、移动和远程客户端的安全管理成本。

› 集成式响应

Symantec Client Security 提供了对防病毒、防火墙和入侵检测通用的部署和更新功能，有助于降低更新的成本和风险，并减少更新的管理。此外，集成式响应能力使企业能够更快地响应安全警告和病毒爆发，有效改善网络整体的安全形式。在通过一种响应机制分发之前，赛门铁克已经在集成技术上测试并验证了病毒定义、防火墙规则和入侵特征。以下特性帮助管理员迅速地做出响应，以实现最大程度的遏制和恢复：

- **先进技术的整合：**数字免疫系统 (Digital Immune System™) 可以自动提交潜在的病毒威胁，并自动地将解决方案发送到出现问题的计算机或整个企业。后端基础架构包括硬件资源、体系结构设计以及最新的扫描引擎和网络蜘蛛 (Web crawler)。
- **存储和转发警报：**采用存储和转发警报功能，受感染的移动用户能够存储事件数据，并在重新连接到企业网络之后将其转发到管理服务器，确保关键的事件数据随时可用，以帮助将安全数据转化为可操作信息。
- **对威胁的快速响应：**Symantec Client Security 允许管理员在一台或多台客户端上立即强制执行 LIVEUPDATE 会话，最大限度地缩短对快速扩散威胁的响应时间。为实现速度更快的自动化响应，赛门铁克系统中心的管理服务器中还集成了“推”技术。可以为管理服务器制定计划，使其自动地从赛门铁克或中央 LiveUpdate™ 服务器上获取病毒内容更新。随后，它将这些更新推至二级服务器，二级服务器进而将其推至客户端系统。

› 保护关键系统、远程和移动用户

Symantec Client Security 提供终端保护，防范各种入侵通过不安全的远程和移动用户进入网络和关键系统。它可以保护未受企业防火墙防护的笔记本，防止其被黑客利用，通过拨号、DSL/Cable 和 VPN 连接非法访问企业网络。它可以为位于防火墙内部的台式机客户端提供更好的混合型威胁防护。

- 扩展的威胁检测：扫描可能影响系统安全（如病毒、蠕虫和特洛伊木马）、客户端数据隐私（如 spyware、trackware 和 adware）或者具有恶意目的（例如拨号程序、恶作剧程序、远程访问和黑客工具）的各种程序。
- 位置意识：使客户端防火墙能够根据计算机位置调整策略，以确保能够对任何地方以任何方式连接到企业网络或互联网的计算机执行安全策略。
- 客户端配置：当防火墙应用程序发现应用程序正在通过防火墙访问互联网或网络时，最大限度地减少终端用户看到的弹出消息数。
- 互联网电子邮件附件扫描：对通过 pop 3 邮件客户端（如 Microsoft® Outlook®、Microsoft Outlook Express、Eudora® 和 Netscape Mail）发送的传入邮件的正文和附件进行病毒扫描，以防范快速扩散的、基于电子邮件的威胁。
- 威胁跟踪器：确定通过开放式文件共享进行扩散的混合型威胁攻击（例如 Code Red 和 Nimda）的来源，以防范同一类型的进一步攻击。
- 行为禁止：新的行为禁止功能包括出站电子邮件蠕虫启发式检测和广告禁止。出站电子邮件蠕虫启发式检测可防止客户端系统通过电子邮件扩散蠕虫（如 SOBIG.F）。管理员还可以设置防火墙以禁止不受欢迎的旗帜广告，以确保员工的最大工作效率。
- 增强的防火墙保护：高级功能可确保存储在远程用户计算机或联网客户端中的信息资产的安全。集成的安全端口可禁止对已知特洛伊木马端口的访问。通过检查执行的应用程序及应用程序的子组件 (DLL)，防火墙能够提供更强的应用程序保护。
- 集成式保护：客户端防火墙技术可扫描流经远程用户计算机和联网客户端的所有流量，同时，实时防病毒扫描技术可以扫描被创建、移动、重命名或执行的各种文件。随后，通过防火墙、防病毒和入侵检测技术的智能交互，以检测潜在的威胁，或加强安全措施，阻截企图渗入网络的可疑文件。当不向磁盘写入数据时，即时内存扫描功能可以确定内存中的威胁，并在其扩散或导致破坏之前将其删除。防病毒技术可以终止可疑的进程，并处理受威胁感染的文件。

详细信息，请访问：<http://enterprisecurity.symantec.com>

病毒防护、反垃圾邮件和内容过滤是 SYMANTEC ENTERPRISE SECURITY 的关键组件。赛门铁克企业安全产品结合了世界级的顶尖技术，并拥有全面的服务以及遍布全球的紧急响应队伍，以帮助企业更安全、更自信地运作。

系统要求

SYMANTEC CLIENT SECURITY 2.0

(SYMANTEC CORPORATE EDITION 9.0/SYMANTEC CLIENT FIREWALL 7.0 最低系统要求)

含 MICROSOFT 推荐的有关内存和处理器的系统要求。

用于 32 位 WINDOWS 客户端的 SYMANTEC CLIENT SECURITY:

- Windows 98, Windows 98 SE, Windows Millennium Edition; Windows 2000 Professional; Windows XP Home, Professional.
- 80 MB 磁盘空间
- 128 MB 内存
- Internet Explorer 5.01 SP2 或更高版本
- 150 MHz Intel 奔腾处理器 (推荐使用奔腾 II 或更高)

用于 32 位 WINDOWS 客户端的 SYMANTEC ANTIVIRUS:

- Windows 98, Windows 98 SE, Windows Millennium Edition; Windows NT 4.0 Workstation, Server, and Terminal Server Edition with Service Pack 6a; Windows 2000 Professional, Server, Advanced Server; Windows XP Home, Professional; Windows Server 2003 Web, Standard, Enterprise, and Datacenter Editions.
- 55 MB 磁盘空间
- 32 MB 内存
- Internet Explorer 4.01 或更高版本
- 150 MHz Intel 奔腾处理器 (推荐使用奔腾 II 或更高)

用于 64 位 WINDOWS 客户端的 SYMANTEC ANTIVIRUS:

- Windows XP 64-Bit Edition Version 2003, Windows Server 2003 Enterprise/Datacenter 64 位版本
- 70 MB 磁盘空间
- Intel Itanium 2 处理器
- 64 MB 内存

用于 32 位 WINDOWS 的 SYMANTEC CLIENT SECURITY 管理服务器:

- Windows NT 4.0 Workstation/Server/Terminal Server Edition SP6a, Windows 2000 Professional/Server/Advanced Server, Windows XP Professional, Windows Server 2003 Web/Standard/Enterprise/Datacenter Editions/
- 111 MB 磁盘空间 (65 MB 用于 Symantec AntiVirus Corporate Edition 服务器文件, 46 MB 用于客户端磁盘映像)
- 可选的 AMS2 Server 安装需要 15 MB 磁盘空间
- 64 MB 内存
- Internet Explorer 4.01 或更高版本
- 150 MHz Intel 奔腾处理器 (推荐使用奔腾 II 或更高)

注意: Symantec Antivirus Corporate Edition 不支持在 Windows 服务器上的 Macintosh 卷上扫描 Macintosh 病毒。

关于赛门铁克

作为世界互联网安全技术领导厂商, 赛门铁克公司个人和企业用户提供一个系列内容和网络安全解决方案。赛门铁克公司为企业用户提供病毒防护、安全漏洞检测、入侵检测、互联网内容/电子邮件过滤、远程管理技术和安全服务。赛门铁克旗下的诺顿系列个人用户安全产品领导全球零售市场并且屡次获得行业大奖。赛门铁克公司总部设在加利福尼亚的 CUPERTINO, 现已在 36 个国家设有分支机构。

欲知详情, 请访问中文网址: WWW.SYMANTEC.COM.CN
或查询各地办事处:

北京: 电话: (010) 8518 3338
上海: 电话: (021) 6334 6008
广州: 电话: (020) 8755 3368

传真: (010) 8518 6928
传真: (021) 6334 6006
传真: (020) 8755 6873

Symantec 和 Symantec 徽标均为 Symantec 公司在美国的注册商标。LiveUpdate、NAVEX 和 Symantec Packager 是 Symantec 公司的商标。Microsoft、Windows 和 Windows NT 是 Microsoft 公司在美国和其他国家/地区的注册商标。所有其他品牌和产品都是其各自所有者的商标。2004 年版权所有 © 赛门铁克公司。保留所有权利。04/04 所有产品信息如有更改, 恕不另行通知。
DS-00107-CS

SYMANTEC CLIENT SECURITY 管理服务器 NETWARE:

- NetWare 5.1 SP3 或更高版本、6.0 SP1 或更高版本
- 15 MB RAM (高于标准 NetWare RAM 要求) 用于 Symantec AntiVirus NLM
- 116 MB 磁盘空间 (70 MB 磁盘空间用于 Symantec AntiVirus Corporate Edition 服务器文件, 46 MB 磁盘空间用于 Symantec AntiVirus Corporate Edition 客户端磁盘映像)
- 15 MB 内存 (高于标准 NetWare RAM 要求) 用于 Symantec AntiVirus NLM。
- 150 MHz Intel 奔腾处理器 (推荐使用奔腾 II 或更高)
- Internet Explorer 5.5 SP2
- 可选的 AMS2 Server 安装需要 20 MB 磁盘空间

赛门铁克系统中心:

- Windows NT 4.0 Workstation/Server SP6a, Windows 2000 Professional/Server/Advanced Server, Windows XP Professional, Windows Server 2003 Web/Standard/Enterprise/Datacenter Edition
- Internet Explorer 5.5 SP2
- Microsoft Management Console 1.2. If MMC is not already installed, you will need 3 MB of free disk space (10 MB during installation)
- 36 MB 磁盘空间
- 32 MB 内存
- 150 MHz Intel 奔腾处理器 (推荐使用奔腾 II 或更高)

赛门铁克系统中心管理单元:

- 警报管理系统控制台
- 除赛门铁克系统中心控制台所要求的空间外, 还需要 24 MB 磁盘空间
- Symantec AntiVirus 管理单元
- 除赛门铁克系统中心控制台所要求的空间外, 还需要 6 MB 磁盘空间
- Symantec Client Firewall 管理单元
- 除赛门铁克系统中心控制台所要求的空间外, 还需要 1 MB 磁盘空间
- AntiVirus 服务器分装工具
- 除赛门铁克系统中心控制台所要求的空间外, 还需要 130 MB 磁盘空间
- NT 客户端安装工具
- 除赛门铁克系统中心控制台所要求的空间外, 还需要 2 MB 磁盘空间

隔离区控制台:

- Windows NT 4.0 Workstation/Server SP6a, Windows 2000 Professional/Server/Advanced Server, Windows XP Professional
- Internet Explorer 5.5 SP2
- Microsoft 管理控制台 1.2。如果尚未安装 MMC, 则需要 3 MB 可用磁盘空间 (安装期间需要 10 MB)
- 35 MB 磁盘空间
- 32 MB 内存
- 150 MHz Intel 奔腾处理器 (推荐使用奔腾 II 或更高)

隔离区服务器:

- Windows NT 4.0 Workstation/Server SP6a, Windows 2000 Professional/Server/Advanced Server, Windows XP Professional, Windows Server 2003 Web/Standard/Enterprise/Datacenter Edition
- Internet Explorer 5.5 SP2
- 40 MB 磁盘空间
- 交换文件最小为 250 MB
- 64 MB 内存
- 150 MHz Intel 奔腾处理器 (推荐使用奔腾 II 或更高)

SYMANTEC CLIENT FIREWALL ADMINISTRATOR

- Windows NT 4.0 Workstation/Server SP 6a, Windows 2000 Professional/Server/Advanced Server, Windows XP Professional, Windows Server 2003 Web/Standard/Enterprise/Datacenter Edition
- 80 MB 磁盘空间
- 64 MB 内存

注意: 如果运行的是 Windows ME 或 Windows XP, 并且启用了系统还原功能, 则系统磁盘使用量将增加。有关系统还原功能的原理, 请参阅 Microsoft 操作系统文档。

全球总部

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
Tel: +1.408.253.8600
Fax: +1.800.441.7234

www.symantec.com