WHITE PAPER: ENDPOINT SECURITY

互联世界 · 满怀信心

symantec™

Symantec™ Endpoint Protection

统一、主动的端点安全保障方法

Symantec Endpoint Protection
统一、主动的端点安全保障方法

目录

摘要

企业目前面临着利用端点设备中的漏洞，更为隐蔽、目标性更强、旨在获取经济利益的威胁。多种上述复杂威胁会避开传统的安全解决方案，使企业容易成为数据窃取和操控的受害者、造成关键业务服务中断并导致公司品牌和声誉受损。为了提前应对这些隐蔽多变的新型安全威胁，企业必须升级他们的端点防护措施。

Symantec Endpoint Protection 让企业能够采用更为有效的整体方法，来保护笔记本电脑、台式机和服务器等端点。其中结合了五种基本安全技术，可针对各种已知威胁和未知威胁主动提供最高级别的防护，这些威胁包括病毒、蠕虫、特洛伊木马、间谍软件、广告软件、Rootkit 和零日攻击。该产品将业界领先的防病毒软件、反间谍软件和防火墙与先进的主动防护技术集成到一个可部署代理中，通过中央管理控制台进行管理。而且，管理员可以根据他们的具体需要，轻松禁用或启用上述任何技术。Symantec Endpoint Protection 实现无缝的多层端点防护，可提供：

- **高级威胁防御** — 超越基于特征的传统文件扫描方法，可针对企业内外的各种已知威胁和未知威胁提供全面的端点防护。Symantec Endpoint Protection 通过可自动分析应用程序行为和网络通信的最佳技术提供高级主动防护，同时包含其它多种工具，可限制高风险的设备和应用程序行为。

- **简化的整体端点防护方法** — 通过将多种基本端点安全技术整合为一个代理，Symantec Endpoint Protection 非常便于安装、维护和更新，让企业能够在节省时间和成本的同时保护资产和业务。其自动安全更新可针对最新威胁提供无忧防护。另外，该产品提供统一的管理控制台，它具备图形报告、集中日志记录和阈值警报等功能，为管理员提供全面的端点可见性。

集成的端点防护方法

近几年来，IT 威胁趋势发生了显著的变化。过去，大多数攻击的目的仅仅是出名而已。现在，攻击变得更复杂、更隐蔽，往往以特定企业为目标来获得经济利益。专业黑客会不断开发新的方法，试图做到始终能够未经授权即可访问企业系统和信息，而且不被检测出来。从混合威胁的出现就能看出攻击复杂程度在不断升级，这种威胁集成了蠕虫、特洛伊木马和零日攻击等多种攻击方法。

防病毒软件、反间谍软件和其它基于特征的防护方法主要是反应性方法，它们在几年前可能足以保护企业的重要资源，但已不能满足当前的安全需要。企业目前需要主动的端点安全方法，来防御零日攻击乃至未知威胁。他们需要层次化的端点安全方法，实施不仅能够防御各级威胁，而且可提供互操作性、无缝实施和集中管理的全面解决方案。

Symantec Endpoint Protection 提供全面的多层端点防护方法，满足了这一需要。该产品将 Symantec AntiVirus™ 与高级威胁防御相结合，可以为笔记本、台式机和服务器提供无与伦比的恶意软件防护能力，这些已知和未知的恶意软件包括病毒、蠕虫、特洛伊木马、间谍软件和广告软件。它甚至可以防御复杂攻击，这些攻击能够躲避传统的安全措施，如 Rootkit、零日攻击和不断变化的间谍软件。

Symantec Endpoint Protection 不仅提供了世界一流、业界领先且基于特征的防病毒和反间谍软件防护。它还提供了久经考验的主动防护技术，能够保护端点免遭目标性攻击以及之前没有发现的未知攻击侵扰。它包括即刻可用的主动防护技术以及管理控制功能；主动防护技术能够自动分析应用程序行为和网络通信，以检测并阻止可疑活动，而管理控制功能让管理员能够拒绝对企业来说被视为高风险的特定设备和应用程序活动。这些功能甚至可以根据用户位置阻止特定操作。

赛门铁克解决方案的多层方法可以显著降低风险，同时能够充分保护企业资产，从而使您高枕无忧。这款全面的产品不仅提供了企业需要的功能，而且让企业有能力根据需要自定义解决方案。无论攻击是由恶意的内部人员发起，还是来自于外部入侵者，端点都会受到充分保护。

简化端点保护 — 多重技术、一个产品

为抵御日益增加的以 IT 基础架构为目标的威胁，管理员了解端点防护技术的重要性。不过，这通常意味着确保在每个端点上安装防病毒软件、反间谍软件、台式机防火墙、入侵防御和设备控制技术。在每个端点上分别部署这些安全产品时，不仅需要很长时间，而且还会增加 IT 复杂性和成本。于是，企业需要提供为各类不同的端点安全解决方案提供管理、培训和支持。另外，不同技术往往会相互妨碍，或者由于资源消耗较大而对系统性能造成不良影响。

为了降低与部署和管理多个解决方案相关的复杂性和成本，赛门铁克将多种一流的端点防护技术整合为一个集成代理，可通过一个统一管理控制台进行管理。Symantec Endpoint Protection 不仅可以增强防护，而且可以降低多个安全性产品的相关管理开销和成本。不仅如此，该产品还让管理员能够随时间推移灵活地扩展防护解决方案。他们可以从少数几种防护技术开始，然后根据需要启用其它技术。Symantec Endpoint Protection 甚至可以配置为与其他供应商的技术一起工作，如台式机防火墙或防病毒解决方案。这让企业可以轻松实施和配置需要的解决方案，从而满足他们的需要。

一个端点防护代理

与竞争对手的解决方案不同的是，Symantec Endpoint Protection 将防病毒软件、反间谍软件、防火墙、设备控制和先进的入侵防御集成为一个代理，让企业能够自定义端点防护的级别以及一起工作的技术。Symantec Endpoint Protection 需要更少内存、占用更少资源，同时可增强防护。另外，管理员可以对该代理进行优化，以减少它在用户活动较多的时段内使用的资源，从而保证端点性能。

通过将多种功能整合到一个端点安全代理，可以提高操作效能，如在所有安全技术中使用单一通信方法和内容交付系统。可以使用客户端或管理服务器，在一个位置执行全局服务配置和排除。另外，代理的自动安全更新可针对最新威胁提供无忧防护。

Symantec Endpoint Protection 在客户端上提供一个简化的用户界面。管理员能够自定义该界面，所以他们可以决定在客户端上运行哪些技术，以及哪些配置选项对最终用户不可用。管理员还可以选择对用户完全隐藏该界面。这些功能为管理员提供灵活性和控制能力，让他们能够按照符合企业特有需要的方法保护端点设备。另外，管理员可以随时打开或关闭各种功能和选项。

一个统一管理控制台

Symantec Endpoint Protection 提供通过一个统一控制台管理所有服务的功能，让管理员可通过整体方法来管理端点安全。通过使用 Symantec Endpoint Protection Manager，控制台管理员可以创建和管理各种策略、将策略分配给代理、查看日志并运行端点安全活动报告。它通过图形报告、集中日志记录和阈值警报等功能提供全面的端点可见性。统一控制台不仅简化了端点安全管理，而且还提供了出色的操作效能，如集中软件更新、策略更新、报告和许可维护。

该控制台采用企业级的管理架构，可进行扩展以适合最高要求的环境。它可以提供对管理任务的更细致控制，同时简化并统一管理工作以降低总拥有成本。它采用灵活的管理结构，可以根据不同管理员的角色和职责，为他们授予不同级别的管理系统访问权限。另外，它支持从 Active Directory 导入 Organization Units，而且可与 SMS 等领先软件部署工具一起工作，可为管理员进一步增强管理功能。

与竞争对手的解决方案不同的是，这一多层端点安全方法在一个代理部署中提供世界一流的成熟解决方案，可显著降低风险且不增加资源开销，所以企业能够高效地管理安全，同时确信他们的公司资产和业务已得到全面保护。

降低总拥有成本

Symantec Endpoint Protection 在一个产品中提供多种基本端点安全技术的优势，可以降低总体拥有成本，让企业能够减少管理开销以及管理多个端点安全产品引发的成本。该产品还可以利用现有 IT 投资。

- **减少管理开销** — 减少管理多点解决方案需要的人手和工作量
- **降低成本** — 减少管理端点安全、用户和网络停机时间以及补救工作的相关工作量
- **利用现有 IT 投资** — 可与领先的软件部署工具、补丁程序管理工具、SIM 工具、数据库和操作系统一起工作

最全面的端点安全

Symantec Endpoint Protection 将一流的防护机制无缝结合到一个代理中，可提供最全面的端点安全：

- 防病毒软件/反间谍软件
- 网络威胁防护
- 主动威胁防护

此外，Symantec Endpoint Protection 支持进行网络准入控制。可以启用该代理的网络准入控制功能，让企业能够确保各个端点符合公司的安全策略，然后为其授予网络访问权限。通过使用 Symantec Endpoint Protection，将无需在企业的端点设备上部署其它网络准入控制软件。

防病毒和反间谍软件

防病毒和反间谍软件解决方案一般采用基于扫描的传统技术，来识别端点设备上的病毒、蠕虫、特洛伊木马、间谍软件和其它恶意软件。典型的防病毒和反间谍软件解决方案会在系统中搜索与已知威胁的特点（或称威胁特征）匹配的文件，从而检测这些威胁。在检测到威胁

后，该解决方案会对其进行补救，通常是删除或控制威胁。多年来，该方法在针对已知威胁保护端点时一直非常有效。虽然该方法不足以防御未知威胁和零日威胁，但它仍然是整体端点安全中的基本要素。

由于整个行业日益重视端点安全，所以防病毒和反间谍软件市场中最近新出现了各种产品。在这些第一代和第二代解决方案中，虽然有许多产品可以提供一定程度的防护，但它们往往无法提供全面防护。许多技术仅在一种操作系统上工作。其它技术缺少与防火墙、设备控制和入侵防御等其它基本端点安全技术互操作的功能。

无论是从质量还是级别来看，Symantec Endpoint Protection 提供的防护都远远超越了竞争对手的产品。与第一代打包解决方案相比，Symantec Endpoint Protection 提供更高级别的实时防护，而且赛门铁克的表现比许多老牌安全解决方案提供商更胜一筹。例如，赛门铁克是 1999 年以来唯一连续获得 30 多项 VB100 奖的供应商。AV-Comparatives 在 2007 年 2 月进行了一项测试研究，在进行多态病毒测试的 15 种防病毒解决方案中，只有赛门铁克和另一家供应商在所有类别中均获得 100 分的分数。根据 AV-Comparatives，多态测试可确定防病毒扫描引擎的灵活性和检测复杂病毒的性能。另外，AV-Comparatives 认为 100 分以下的所有多态测试分数都属于失败或不可靠检测，因为即使只漏过一次复制攻击，也会导致再感染病毒。

Thompson Cyber Security Labs 在 2006 年 9 月进行的一次研究显示，赛门铁克提供的 Rootkit 检测和删除性能超越了竞争的供应商。Rootkit 是一种隐蔽的应用程序或脚本，黑客使用它逃避系统检测，同时获得对系统的管理员级别访问权限。互联网上随处可见现成的 Rootkit 应用程序，即使经验不足的黑客也能使用 Rootkit，而不必了解它是如何工作的。Rootkit 通常用于收集用户 ID、帐号和密码等机密信息。要检测和删除 Rootkit，需要对操作系统执行全面分析和修复。为此，Symantec Endpoint Protection 中包含了 Veritas Raw Disk Scan，与其它任何解决方案相比都可提供更深入的文件系统检查，实现通过进行必要地分析和修复来防御最复杂的 Rootkit 攻击。

另外，Symantec Endpoint Protection 由赛门铁克全球情报网络提供支持，该集成式服务为客户提供了必需的情报，让他们能够降低安全风险、提高法规遵从性并改善整体安全状况。赛门铁克全球情报服务提供了对全球、行业和本地最新威胁与攻击的洞察，以便企业可以主动响应新出现的威胁。通过将威胁预警和赛门铁克托管安全服务完美结合，赛门铁克全球情报服务可以对整个企业中的恶意活动进行实时分析，从而帮助企业保护关键信息资产。

网络威胁防护

端点上的网络威胁防护对于防御混合型威胁和阻止爆发至关重要。为保证有效性，绝不能仅仅依赖防火墙。网络威胁防护应包含多种先进防护技术，包括入侵防御以及先进的网络通信控制功能。

过去，安全专家争论的焦点是：是否需要在企业网络边界本身或个别台式机上部署防火墙。由于目前的威胁极为复杂，而且移动办公人员已经扩展到企业计算基础架构的边界以外，所以端点已成为漏洞利用和攻击的主要目标。威胁通常首先感染网络边界以外的一台笔记本电脑，之后，在这台笔记本电脑连接到内部网络时，该威胁就会传播到其它端点。可以利用端点防火墙，不仅阻止内部网络攻击入侵连接到网络的任何端点，甚至阻止这些威胁离开最初感染的端点。

Symantec Endpoint Protection 端点安全代理结合最佳的防火墙解决方案，兼备赛门铁克客户端防火墙与 Sygate™ 防火墙的功能。其中包括：

- 基于规则的防火墙引擎
- 预定义的防病毒、反间谍软件和个人防火墙检查
- 按应用程序、主机、服务和时间触发的防火墙规则
- 全面 TCP/IP 支持（TCP、UDP、ICMP、Raw IP Protocol）
- 用于允许或禁止网络协议支持的选项，包括以太网、令牌环、IPX/SPX、AppleTalk 和 NetBEUI

- 阻止 VMware 和 WinPcap 等协议驱动程序的功能
- 特定于适配器的规则
- 检查加密和明文网络通信的功能
- 数据包和数据流入侵防御系统 (IPS) 阻止、自定义 IPS 特征阻止以及一般漏洞利用禁止实现主动威胁防御
- 网络准入控制的自我实施

入侵防御对解决方案的网络威胁防御方案具有重要作用，对于使用一般特征并基于漏洞的入侵更是如此。基于漏洞的入侵防御系统可使用一个一般特征阻止攻击漏洞的数百种潜在漏洞利用，在网络层遏止攻击，使其根本无法感染端点。

虽然传统 IPS 解决方案能够检测到特定的已知漏洞利用，但他们不足以针对构成当前威胁主流的多种漏洞攻击变种来保护公布的软件漏洞。根据互联网安全威胁报告 (ISTR Vol XI)，操作系统或应用程序提供商平均需要 47 天才能发布公布漏洞的补丁程序。在推出补丁程序之前利用这些漏洞进行的攻击通常称为前所未见的攻击或零日攻击。在检测到第一次漏洞攻击之后的几小时，IPS 供应商会发布特征，以防御利用特定漏洞的进一步攻击。

这些反应性方法会让老练的攻击者拥有大量攻击机会。在发布漏洞特征之前发起的第一轮漏洞利用会让企业承受极为惨重的损失。即使已经发布了漏洞利用特征，这些方法对多态或自我突变的漏洞利用变种也是毫无招架能力。另外，这些基于漏洞利用的反应性方法无法防御尚未发现、尚未报告或未知的威胁，例如，通常检测不到以特定公司为目标的隐蔽漏洞利用。为应对前所未见的突变威胁，需要基于漏洞的 IPS 形式的更主动方法。

虽然基于漏洞利用的特征只能检测到特定漏洞利用，但基于漏洞的特征会在更高级别运行，不仅检测到利用一种漏洞的特定攻击，而且能够检测到试图攻击该漏洞的所有漏洞利用。Symantec Endpoint Protection 包括一般漏洞利用禁止 (GEB)，即使用一般特征、基于漏洞的 IPS 技术。当操作系统或应用程序供应商公布可能导致企业面临严重风险的新漏洞时，赛门铁克的工

程师会研究该漏洞的特点，并根据研究结果总结并发布一般特征。由此可帮助在出现漏洞利用之前保护企业。

基于漏洞的入侵防御非常有效，因为一个漏洞定义不仅能防御一种威胁，而且可防御数百种甚至数千种威胁（参见下表）。因为这种防御会查找漏洞特点和行为，所以可防御多种威胁，甚至可防御未知威胁或尚未开发的威胁。

一般漏洞利用禁止可防御数千种漏洞利用变种。

可禁止变种的数量	一个 GEB 特征	威胁
814	MS RPC DCOM BO	Blaster
426	MS_RPC_NETDDE_BO	W32.Mytob.IM@mm
394	MS LSASS BO	Sasser
250	RPC_NETAPI32_BO	W97M.Invert.B
121	NetBIOS MS NO (TCP)	W32.Gaobot.AAY
55	MS IIS Webdav Exploit	Welchia
51	MS Plug and Play BO	W32.Zotob.A
43	MS Locator Service BO	W32.Welchia.C

基于漏洞的保护还可用于防御以特定行业或企业为目标的漏洞利用。有目标的攻击通常比较隐蔽，因为它们的目标是在窃取机密信息时不会被发现，之后还要清除它们自己在系统中留下的痕迹。所以，无法总结出这些有目标漏洞利用的特征，因为企业无法在它们造成破坏之前了解它们。基于漏洞的防护可以识别有目标攻击试图利用的漏洞的高级特征，所以可检测并阻止漏洞利用。

Symantec Endpoint Protection 中的端点安全代理在网络层结合基于漏洞的防护，可阻止前所未见的漏洞利用或其变种进入并感染端点。因为它们没有机会感染端点，所以不会造成损害，也不需要对其进行补救。

Symantec Endpoint Protection 还让管理员有能力创建自定义的入侵防御特征。所以，他们可以定义基于规则的特征，根据他们的特有环境和自定义应用程序的需要而进行量身定制。可以将特征创建为可阻止一些特定操作或更复杂的操作。如果使用 Symantec Endpoint Protection，将无需等待操作系统或应用程序供应商创建已知漏洞的补丁程序，所以管理员可以对端点安全和防护提供全面的主动性控制。

主动威胁防护

虽然基于特征的文件扫描和网络扫描技术覆盖了主要的必备保护领域，但仍然需要并非基于特征的技术，来防御隐蔽攻击使用的不断增多的未知威胁。这类技术被称为主动威胁防护技术。

Symantec Endpoint Protection 包括 Proactive Threat Scan，它是一种主动威胁防护技术，可防御利用已知漏洞的多种变种和前所未见的威胁。它具有独特的主机入侵防御功能，让企业有能力针对未知或零日威胁保护自己。Proactive Threat Scan 基于分析系统所运行进程的行为来检测潜在威胁的启发式技术。大多数基于主机的 IPS 仅检测它们认为的“不良行为”。所以，它们经常会将可接受的应用程序行为识别为威胁并将它们关闭，严重影响用户和技术支持中心的工作效率，让管理员面临着艰巨的挑战。不过，Proactive Threat Scan 会同时记录应用程序的正常行为和不良行为，提供更加准确的威胁检测，可显著减少误报的数量。所以，Symantec Endpoint Protection 让企业能够检测到任何基于特征的技术都检测不到的未知威胁。

Symantec Endpoint Protection 还结合了设备和应用程序控制功能，让管理员能够拒绝被认为存在高风险的特定设备和应用程序活动，使企业能够根据用户位置禁止特定的操作。设备控制技术让管理员能够决定并控制允许哪些设备连接端点。例如，它可以锁定端点，禁止便携硬盘、CD 刻录机、打印机或其它 USB 设备连接到系统，以防止将机密信息从系统复制到其中。禁止设备连接的功能还可以帮助防止端点受来自上述设备以及其它设备的病毒感染。

应用程序控制技术让管理员能够按照用户和其它应用程序，控制对特定流程、文件和文件夹的访问。它提供应用程序分析、流程控制、文件和注册表访问控制、模块和 DLL 控制。如果管理员希望限制被认为可疑或存在高风险的某些活动，则可以使用该高级功能。

支持网络准入控制

Symantec Endpoint Protection 中的端点安全代理支持网络准入控制，这意味着该代理已集成网络准入控制技术，而且通过购买 Symantec Network Access Control 许可证就可以轻松启用该技术。所以，在部署 Symantec Endpoint Protection 后，无需在端点设备上部署其它代理软件即可实施网络准入控制

通过购买附加许可证启用网络准入控制之后，它会控制对公司网络的访问、实施端点安全策略并与现有网络基础架构轻松集成。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、提供自动补救功能，并持续监视端点以了解遵从状态是否发生了变化。另外，为了简化并优化管理，管理员为 Symantec Endpoint Protection 和 Symantec Network Access Control 使用同一管理控制台管理所有功能。

提高端点安全标准

Symantec Endpoint Protection 提供先进威胁防御功能而且便于管理，提高了全面、安全的端点安全解决方案的标准。它是唯一能够在一个集成代理中提供一流基本技术优势的端点安全解决方案，可通过一个管理控制台进行管理并支持进行网络准入控制。

赛门铁克认为，要有效地保证端点安全，需要将端点防护技术与端点遵从性技术结合使用。因此，Symantec Endpoint Protection（端点防护）与 Symantec Network Access Control（端点遵从性）紧密集成，让企业能够采取更为整体化的端点安全方法。这些产品可以无缝地互操作，提

供全面且统一的多层端点安全解决方案，让 IT 管理员能够在最终用户工作效率与安全性之间取得平衡，同时简化端点安全管理（参见图 1）。

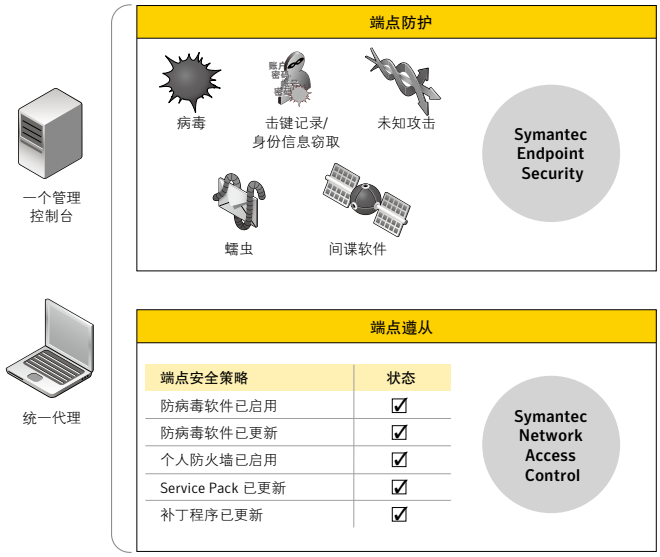

图 1 赛门铁克的端点安全保障方法

对于已经部署赛门铁克的其它市场领先安全产品的企业，利用该集成的端点安全产品可以增强系统防护、简化管理并节约成本。为了简化获得 Symantec Endpoint Protection 的优势的过程，赛门铁克为现有客户提供一系列服务和产品，帮助他们升级为使用这一最新产品，包括用于从 Symantec AntiVirus™ 迁移策略的向导、最佳实践经验指南、知识库文章以及在线培训。

Symantec Endpoint Protection 设计为可与企业的现有安全和 IT 投资一起运行，非常便于实施和部署。但是，为帮助企业更快地获得投资回报，赛门铁克还提供一系列咨询、技术培训和支持服务，来帮助充分挖掘 Symantec Endpoint Protection 的内在优势及其功能的潜力。

为了给客户提供有关通过最佳方式部署、管理和充分利用 Symantec Endpoint Protection 提供的优势与功能的帮助和指导，赛门铁克企业支持服务提供三种级别的保护，旨在满足小型企业到大型企业等各类企业的需求。赛门铁克教育服务提供一系列培训课程，旨在帮助用户和管理员

快速掌握相关技能。赛门铁克咨询服务从防病毒软件部署和迁移帮助入手。赛门铁克还可以提供现场服务，即赛门铁克的顾问与客户的 IT 员工一起工作，还可以提供操作服务，即将全部端点安全职能外包给安全专家赛门铁克。

总结

要应对当前面对的各种复杂、隐蔽而且有目标的攻击，企业不能再单纯依靠传统的防病毒和反间谍软件解决方案。有效端点安全解决方案需要企业实施附加安全层，以主动防御零日威胁。他们需要采取整体方法来确保端点安全，目标是既能够有效地针对各种级别的威胁保护企业，又能提供无缝的互操作性以简化管理并降低总体拥有成本。

Symantec Endpoint Protection 提供无与伦比的、全面且集成的端点安全解决方案，可作为安全端点计算的基础。该产品结合多种基本的最佳安全技术，可针对已知和未知威胁提供高级威胁防御。它能够增强保护，还提供通过一个管理控制台即可管理的一个代理，从而降低因管理多个端点安全产品而引发的管理开销及成本。因此，这一无缝的多层端点防护产品可简化安全管理，让企业能够在节省时间和成本的同时保护资产和业务。

赛门铁克是基础架构软件和端点安全领域的全球领先者，致力于使企业和用户在互联世界中满怀信心。赛门铁克提供业界最为丰富的安全解决方案系列，可针对各类内部和外部的安全风险帮助企业保护端点系统和公司信息。赛门铁克通过提供能够防范安全性、可用性、遵从和性能风险的软件与服务，帮助企业保护基础架构、信息和交互。

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。要了解更多相关信息，欢迎访问赛门铁克公司网站：www.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

赛门铁克公司

全球总部

20330 Stevens Creek Boulevard

Cupertino, CA 95014 USA

+1 (408) 517 8000

1 (800) 721 3934

www.symantec.com

09/07 WP-00163-CN