Symantec ™ Endpoint Protection 14

产品资料：Endpoint Security

概述

去年我们发现了 4.31 亿个新的恶意软件变体，勒索软件攻击也是花样层出，而零日威胁数量更翻了一番。[1] 威胁环境快速演变，面对当今网络的规模和复杂性，企业也在力争跟上发展的步伐。供应商和新兴企业试图采用各种方法和提供有限防护的单点解决方案化解恶意软件感染。人人都认为端点安全仍然至关重要，但是推出一款行之有效的解决方案却日益艰难。

为了抵御当今错综复杂的威胁态势，客户就得不遗余力地拦截攻击端点的种种威胁。为此，企业必须部署以下功能：

- 高级技术，检测未知威胁并防范勒索软件等零日攻击
- 内存漏洞利用防护，防止常用应用程序和操作系统遭到攻击
- 访问全球最丰富的威胁情报资源，实时抵御威胁
- 自动协调响应措施，迅速拦截威胁
- 跨所有设备提供不折不扣的卓越防护

Symantec Endpoint Protection 14 专为解决当今威胁态势而设计，在整个攻击链中实行全面保护并提供深层防御。运用全球最大胁情报网络的力量，SEP 14 借助多维机器学习、信誉分析和实时行为监控等新一代技术，有效拦截高级威胁。它可结合同样举足轻重的基本防护技术，为企业提供全面保护。Symantec Endpoint Protection 14 是一款单一管理控制台的轻量型代理，可与安全基础架构中的其他产品集成，从而快速响应威胁，实现最佳的端点防护 [2]，以不折不扣的实力傲视同类产品。

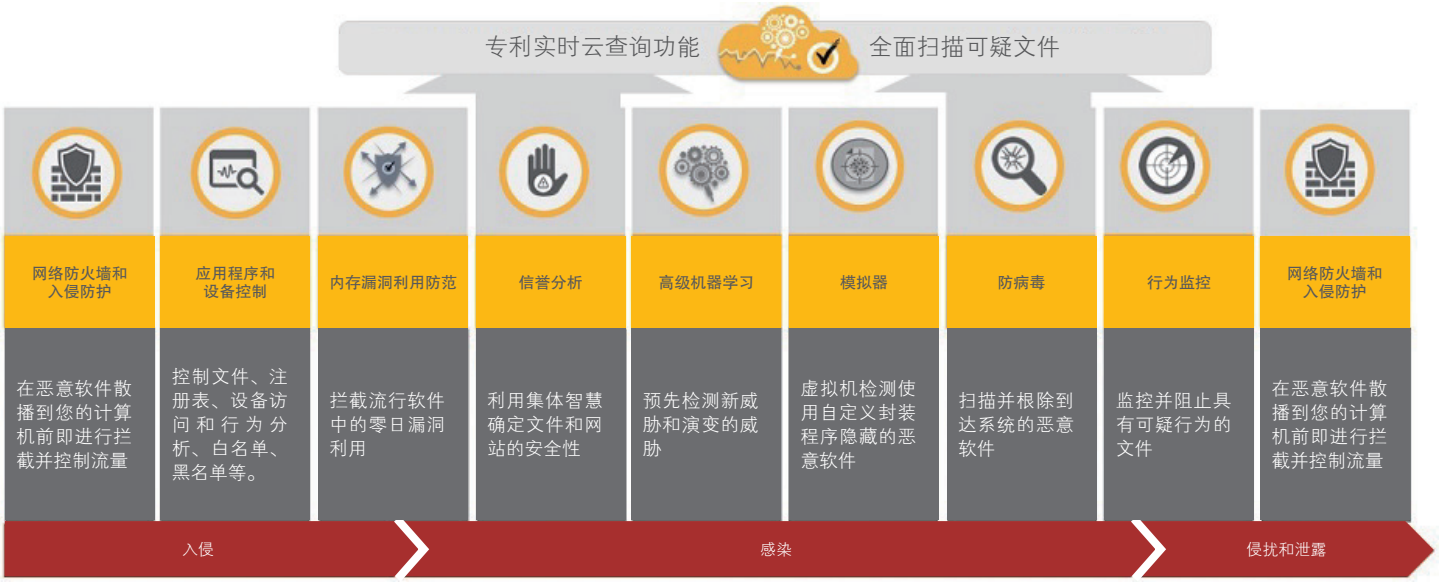
在整个攻击链中提供全面防护

这个卓越性能的轻量型代理将新一代技术与基本技术融为一体，全面拦截攻击端点的高级威胁和快速变异的恶意软件，无论攻击耍出何种手段，都将无法得逞。

入侵：

- **网络入侵防护、URL 和防火墙策略：**赛门铁克的网络威胁防护技术可分析传入和传出数据，及时阻止威胁通过网络攻击端点。这个防护技术同时还包含基于规则的防火墙以及浏览器保护功能，可有效抵御网络攻击。总体而言，借助强大的网络防护技术，一半以上的威胁都会在到达端点前被查杀和拦截。
- **应用程序行为控制：**控制文件和注册表访问权限，以及设置允许进程运行的方式。
- **设备控制：**限制对选定硬件的访问，并控制哪些类型的设备可以上传或下载信息。外设控制可以结合应用程序控制，提供更灵活的控制策略。
- **漏洞利用防护：**根除供应商尚未发布修补程序的流行软件中的零日漏洞利用，包括 Heap Spray、SEHOP Overwrite 和 Java 漏洞利用。这种无特征技术效果显著，有效防止恶意软件利用任何缺陷、错误或漏洞发起攻击。

[1] 2016 年赛门铁克《互联网安全威胁报告》
[2] AV-TEST.Org “2016 最佳防护奖”



感染：

- **漏洞利用防护：**还能有效检测恶意软件，防止出现感染。
- **信誉分析：**赛门铁克独有的信誉分析技术利用我们的情报网络关联用户、文件和网站之间存在的数百亿种关系，可主动拦截更多威胁并快速抵御恶意软件变体。通过分析关键文件属性(例如文件下载的频率、文件存在的时长和下载的源位置)，我们可以在文件传到端点之前，精准判定文件是否安全并指定一个信誉分数。利用文件信誉分析后，用户只需仅扫描有风险的文件，从而显著减少扫描工作量。
- **机器学习：**端点上的多维机器学习技术运用学习到的内容拦截新型威胁和未知威胁，从而极度减少我们在辨别威胁时对特征的依赖程度。机器还经过全球威胁情报网络中数万亿安全文件和恶意文件示例的反复训练，确保将误报率降至最低。
- **模拟：**高速模拟器可检测利用多态自定义封装程序隐藏的恶意软件。静态数据扫描程序在轻量型虚拟机中运行每个文件仅需几毫秒，从而让威胁瞬间原形毕露，不仅提高检测率，而且改善了工作性能。
- **防病毒文件保护：**基于特征的防病毒功能和高级文件启发式技术可发现并根除系统上的恶意软件，从而抵御病毒、蠕虫、特洛伊木马、间谍软件、僵尸程序、广告软件和 Rootkit 等。
- **行为监控：**Symantec Endpoint Protection 中的行为监控功能展现出了极高效率，尽管有极少数的威胁悄无声息地抵达了端点。它利用机器学习提供零日防护，可监控将近 1400 种应用程序并且实时确定文件风险，从而有效阻止最新和未知威胁。

感染和泄露：

- **行为监控：**行为监控还可以有效遏制感染散播。
- **网络入侵防护、URL 和防火墙策略：**分析传入和传出数据，及时拦截威胁通过网络传播。

全球威胁情报：新一代技术充分利用获得专利的实时云查询技术，快速访问全球最大的威胁情报网络。这可新一步提高我们的机器学习功能，深入了解最新的威胁技术，并利用实时更新的云算法，跨所有端点实现全面保护。从遍布于 157 个国家 / 地区的 1.75 亿个端点和 5700 万个攻击传感器收集的数据传送到数千名经验丰富的威胁研究人员手中，研究人员从中剥出蛛丝马迹，形成独特的洞察力并据此开发出前沿的安全创新方案来抵御各类威胁。

高级功能成就卓越性能

虽然 Symantec Endpoint Protection 中融合了大量的检测和防护技术，但整体经过了优化，因此丝毫不会影响网络或用户的工作效率，在第三方性能测试中更是始终表现优异。

- 智能威胁云的快速扫描功能采用流水线、信任传播和批处理查询等高级技术，因此所有特征定义无需下载到端点就可保持较高的效能。结果就是，端点只需下载最新威胁信息，这样一来，特征定义文件占用空间最高可减少 70%，还能进一步降低带宽使用量。
- 继端点上的高级机器学习技术提高了效率之后，不仅下载频率大大降低，而且也极大控制了由于误报造成的中断问题，从而确保效率不受影响。
- 单一的轻量型代理将多种技术和通常只能借助多个代理获得的功能融合于一体，例如机器学习、漏洞利用防范、端点检测和响应 (EDR) 和反恶意软件等。如此一来，企业就能减少端点上托管代理数量，从而可提高工作性能，同时减轻 IT 负担并降低总拥有成本。

轻松集成以协调端点上的响应措施

Symantec Endpoint Protection 以单一控制台和代理跨操作系统和平台在各种规模企业中提供全面防护。

- **强力清除器：**这款主动清理工具可远程触发，从而能够找到高级持续性威胁并删除难以清除的恶意软件。
- **主机完整性检查和策略实施：**通过强制实施策略、检测未经授权的更改、开展损害评估以及隔离不合规端点等功能，确保端点得到妥善保护且合规。结合威胁检测产品使用，可协调响应以隔离受感染端点，从而快速遏制感染传播，便于您修复端点或重建端点映像。
- **系统锁定：**允许运行列入白名单的应用程序（已知为安全）或阻止运行列入黑名单的应用程序（已知为不安全）。Symantec Advanced Threat Protection (ATP) 和 Secure Web Gateway 可利用可编程 API 与 SEP Management (SEPM) Console 进行通信，协调响应措施以通过应用程序控制功能将新发现的恶意应用程序列入黑名单。它可跨 Windows®、Mac®、Linux®、虚拟机和嵌入式系统运行。
- **Secure Web Gateway 集成：**全新可编程 REST API 支持 SEP 与 Secure Web Gateway 等第三方产品集成，协调端点响应措施，快速遏制感染传播。

- **EDR Console (ATP:Endpoint) 集成：**Symantec Endpoint Protection 可与 Symantec EDR Console (Advanced Threat Protection (ATP:Endpoint)) 相集成，强强联合后，产品可更快地检测、响应和拦截目标性攻击和高级持续威胁，并通过划分攻击处理级别来优先处理严重威胁。EDR（端点检测和响应）是 Symantec Endpoint Protection 的内置组件，因此无需部署其他代理。

防护、性能和响应

Symantec Endpoint Protection 连续多年来一直是端点防护领域的领导产品。

- 多次荣获 SE Labs3 最高 AAA 评级[3]
- 防病毒测试 4[4]，连续 18 个月实现对零日攻击 100% 的安全防护
- 连续 14 年入选 Gartner 魔力象限 5[5] 领导者象限

[3] SE Labs 网址：https://selabs.uk/en/reports/enterprise
[4] AV Test 网址：https://www.av-test.org/en/antivirus/business-windows-client/
[5] Gartner 魔力象限，2016 年 2 月

客户端工作站和服务器系统要求 *	
Windows 操作系统	**虚拟环境**
Windows Vista（32 位、64 位）	Microsoft Azure
Windows 7（32 位、64 位、RTM 和 SP1）	Amazon WorkSpaces
Windows 7 Embedded Standard	VMware WS 5.0、GSX 3.2、ESX 2.5 或更高版本
Windows 8（32 位、64 位）	VMware ESXi 4.1 - 5.5
Windows 8 Embedded（32 位）	VMware ESX 6.0
Windows 8.1	Microsoft Virtual Server 2005
Windows 10	Microsoft Enterprise Desktop Virtualization (MED-V)
Windows Server 2008（32 位、64 位，包含 R2）	Microsoft Windows Server 2008、2012 和 2012 R2 Hyper-V
Windows Essential Business Server 2008（64 位）	Citrix XenServer 5.6 或更高版本
Windows Small Business Server 2011（64 位）	Oracle Virtual Box
Windows Server 2012（64 位，包含 R2）	**Linux 操作系统（32 位和 64 位版本）**
Windows Server 2016	Red Hat Enterprise Linux
Windows 硬件要求	SUSE Linux Enterprise（服务器 / 台式机）
1Ghz CPU 或更高	Oracle Linux (OEL)
512 MB 内存（建议使用 1 GB）	CentOS
1.5 GB 的可用硬盘空间	Ubuntu
Macintosh 操作系统	Debian
Mac OS X 10.9、10.10、10.11，Mac OS 10.12	Fedora
Mac 硬件要求	**Linux 硬件要求**
64 位 Intel Core 2 Duo 或更高版本	Intel Pentium 4（2 Ghz CPU 或更高频率）
2 GB 内存	1 GB 内存
500 MB 的可用硬盘空间	7 GB 的可用硬盘空间

管理服务器系统要求	
Windows 操作系统	**硬件**
Windows Server 2008（64 位，包含 R2）	Intel Pentium Dual-Core 或同级处理器
Windows Server 2012 (R2)	2 GB 内存（建议使用 8 GB）
Windows Server 2016	硬盘上有 8 GB 或更高的可用空间
Mac 硬件要求	**数据库**
Microsoft Internet Explorer	所含嵌入式数据库或选用以下所列项：
Mozilla Firefox	SQL Server 2008 R2、SP3、SP4
Google Chrome	SQL Server 2012、RTM - SP1；SP2
Microsoft Edge	SQL Server 2014、RTM、SP1
	SQL Server 2016

* 有关系统要求的完整列表，请访问我们的支持页面

** 在 Symantec ™ Endpoint Protection 12.1.6 MP1a 中添加支持

备注：Symantec ™ Endpoint Protection 12.1.6 MP2 支持 Mac OS X10.11

更多信息

立即免费试用

立即通过以下链接下载免费的 60 天试用版，体验端点保护领域中领先解决方案的优势：

http://www.symantec.com/endpoint-protection/trialware

阅读第三方评测并了解为何 Gartner 将赛门铁克列入端点保护平台魔力象限领导者象限：

http://www.symantec.com/endpoint-protection/news-reviews

请访问我们的网站

http://enterprise.symantec.com or http://go.symantec.com/sep

关于赛门铁克

赛门铁克公司（纳斯达克：SYMC）是全球领先的网络安全企业，旨在帮助个人、企业和政府机构保护无处不在的重要数据安全。全球企业都青睐选用赛门铁克的战略集成式解决方案，跨端点、云和基础架构抵御复杂攻击。同时，全球 5000 多万的个人和家庭也在使用赛门铁克的 Norton 产品，保护家庭各类联网设备安全。在全球规模数一数二的威胁情报网络的支持下，赛门铁克能够发现和抵御最高级威胁。如欲了解其他信息，请访问 http://www.symantec.com.cn 或通过 weibo.com/SymantecChina 联系我们。

赛门铁克中国地区办事处

北京：电话：(010)85183338 传真：(010)85186928
全国销售热线：800 810 8826
安全产品售后技术支持热线：800 810 3992

21320633-6 10/16