

Sophos 与 Symantec 安全产品比较

一、 简介

Sophos 的最新版本为 Endpoint Security 7.0, 包含管理中心, 反病毒, 反垃圾邮件, 个人防火墙, HIPS, 应用程序管理, 2008 年 4 月份将推出 8.0, 集成了 NAC 功能。

网站地址: <http://cn.sophos.com>

Symantec 的最新版本为 11。

二、Sophos 与 Symantec 产品比较

	Sophos	Symantec
反病毒	●	●
反广告, 垃圾邮件, 恶意程序	●	●
个人防火墙	●	●
行为阻止 (HIPS)	●	▲
缓冲区溢出保护	●	▲
应用程序控制	●	▲
单一代理实现反病毒, 反间谍邮件, 应用控制, HIPS	●	
安全面板	●	
多种平台集中管理	●	○
集成域管理实现自动部署	●	
制定策略强制执行	●	
基于状态和策略符合的系统监控	●	○
集中的多平台升级	●	○
远程病毒/恶意程序清除	●	●
远程病毒、恶意程序允许	●	●
最小化快速升级	●	
24/7 技术人员支持	●	
24/7 全球分析中心新病毒快速响应	●	

● 完整实现的功能 ○ 部分实现的功能 ▲ 需要单独购买、安装、管理的模块

二、 Symantec 产品相对于 Sophos 的不足

- 不同功能使用未集成或集成度很低的多个管理界面
- HIPS, 缓冲区溢出保护和应用程序控制需要单独购买、安装、管理, 难于管理
- 病毒扫描速度慢, 影响用户同时做其他工作
- 缺少指定策略强制执行功能
- 缺少实时的端点活动视图
- 新病毒反应能力慢
- 电话中心做技术支持, 非专业技术人员
- 存在误杀 (去年误杀系统文件, 造成系统崩溃)

三、 Sophos 产品的优势

- 集成的统一管理平台 - Sophos 可以协助管理员在一个单一的管理界面下，控制在 Windows/Mac/Linux 上部署的反病毒安全软件。Symantec 需要多个管理平台。
- 一个反病毒客户端实现集成的端点安全 -- Sophos 通过一个反病毒客户端可以实现集成的端点安全，包括反病毒、反间谍邮件、HIPS、缓冲区溢出保护、应用程序控制和个人防火墙。Symantec 客户端只覆盖了反病毒、反间谍邮件和个人防火墙。缓冲区溢出、HIPS 和应用程序控制是单独销售、安装和管理的。
- 更好的用户体验 - Sophos 提供了业界最快的病毒扫描引擎，大约是 Symantec 的 2 倍。Symantec AV 经常找来客户的抱怨，同时占用了 2 倍 sophos 的内存 (95M)。
- 与网络设备的更好集成 - sophos 协助管理人员查明未受保护的计算机，并通过活动目录、IP 地址范围、Windows 域部署。Symantec 缺少活动目录集成，需要额外的工具进行 IP 子网扫描。
- 简单地企业层面策略强制执行 - 通过管理中心中的指定策略，Sophos 可以协助管理员有效的建立和执行策略。Symantec 的管理工具没有策略强制执行概念，导致端点管理复杂。
- 清晰的监控端点活动 - Sophos 管理中心提供的“基于状态的管理“，允许管理员迅速查明需要特别注意的计算机，如感染病毒了或使用了不一致的安全策略。Symantec 只能现实受保护的计算机。
- 快速的新病毒响应 -- SophosLabs 提供的全球分布的 24/7 小时病毒分析服务，可以快速的应对任何地点新发现的病毒。Sophos 至少比 Symantec 的病毒响应速度快 4 个小时。
- 产品内含的 24/7 的专家支持 - 因为 Sophos 只面向企业用户，不提供个人用户产品，所以有更多的精力和资源服务客户，所有 Sophos 的客户都可以得到技术专家的支持，Symantec 只能通过呼叫中心支持用户，24/7 的服务需要额外购买。
- 更宽广的平台支持 - Sophos 通过综合的单一平台可以支持 Windows、Mac、Linux 平台。而 Symantec 的 Mac OS 保护是需要单独购买和管理的，管理平台仅支持 Windows、Linux

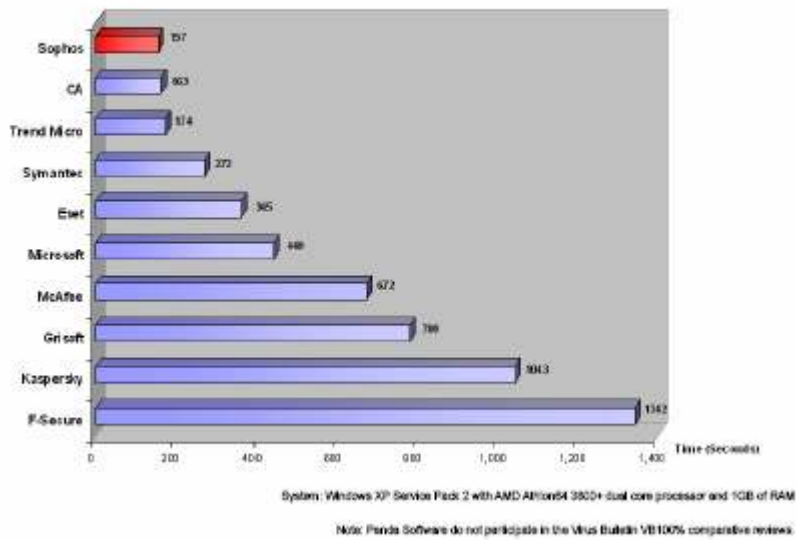
四 附录

- 1、扫描速度比较（来自 Cascadia Labs）

PERFORMANCE RESULTS - Comparison of scanning performance			
Task	McAfee	Sophos	Symantec
Scan of c: drive (No infections)	7 min 33 sec	6 min 50 sec	7 min 49 sec
Scan of c: drive (second run showing impact of caching)	7 min 19 sec	3 min 26 sec	6 min 52 sec
Scan of c: drive (infected with adware)	9 min 12 sec	7 min 38 sec	11 min 9 sec
On-Access Scan of specific folder (contains 3443 files totaling 450 MB with no zip files and no infections)	1 min 37 sec	1 min 26 sec	1 min 33 sec

2、病毒扫描速度比较（来自 VB100%）

Scanning speed comparison – VB100% Review, Virus Bulletin Magazine, June 2007



3、易用性比较（数据来自 Cascadia labs）

USABILITY RESULTS - Comparison of steps & time to perform important tasks			
Activity	McAfee	Sophos	Symantec
Install the product and deploy to 10 endpoints using NetBIOS	115 Steps 38 min 35 sec	39 Steps 20 min 43 sec	53 Steps 23 min 35 sec
Install the product and deploy to 10 endpoints using Active Directory	115 Steps 37 min 50 sec	41 Steps 20 min 39 sec	Feature Not Available
Identify an out-of-date endpoint	1 Step 3 sec	0 Steps Immediate	6 Steps 30 sec
Identify an endpoint out-of-compliance with policy	Feature Not Available	0 Steps Immediate	4 Steps 23 sec
Identify an unprotected endpoint	Feature Not Available	8 Steps 12 sec	6 Steps 48 sec
Create a new policy to detect and block all PUAs	16 Steps 40 sec	11 Steps 16 sec	11 Steps 24 sec
Identify an endpoint that missed a scan or identify last successful on-demand scan	9 Steps 43 sec	2 Steps 4 sec	7 Steps 22 sec

Generate a report of all malware detections in the past 24 hrs for a single endpoint	15 Steps 1 min 10 sec	5 Steps 15 sec	7 Steps 17 sec
Schedule a full system scan, including checks for potentially unwanted applications (PUAs)	27 Steps 1 min 30 sec	9 Steps 20 sec	15 Steps 38 sec
Scan a single system and then authorize a single PUA for all endpoints (scan time not included)	38 Steps 2 min 45 sec	6 Steps 30 sec	6 Steps 9 sec
Authorize a list of 3 PUAs for all endpoints	14 Steps 1 min 20 sec	12 Steps 40 sec	22 Steps 1 min 18 sec
Protect 5 new endpoints	16 Steps 21 min 35 sec	14 Steps 1 min 2 sec	10 Steps 1 min 21 sec
Protect 5 new endpoints automatically using Active Directory	20 Steps 1 min 47 sec	11 Steps 33 sec	Feature Not Available
Authorize outbound Internet access for an application for a management group	18 Steps 1 min 25 sec	6 Steps 10 sec	16 Steps 44 sec
Block execution of well known consumer P2P, VoIP, IM and toolbar applications for a group	27 Steps 1 min 12 sec	6 Steps 16 sec	46 Steps 1 min 57 sec
Configure signature/engine updating frequency	6 Steps 16 sec	11 Steps 37 sec	7 Steps 28 sec