

Sophos 杀毒软件竞争对比分析报告

一、 Sophos 简单介绍

Sophos, 意思是智慧, 是来自英国的具有 25 年历史的世界级杀毒产品提供商。它专门为商业、教育和政府机构提供防御病毒、间谍软件和广告等垃圾邮件的完整解决方案, 它拥有全球大小, 来自各行各业的一亿多企业用户, 包括通用电气, 宝马, 戴姆勒, 西门子, 东芝, 哈佛大学, 牛津大学等典型客户, 年销量位居全球前四。

网站地址: www.sophos.com

二、 权威机构对业界杀毒软件的评比

AV-test 是业界最权威和公正的第三方杀毒软件评比机构, 从各方面分析对比杀毒软件:

	Sophos	Rising	Kaspersky	Mcafee	Trend	Symantec
病毒检测	++ 98.1%	○ 94.1%	+ 97.17%	+ 95.58%	++ 98.72%	+ 95.70%
广告软件/ 间谍软件	++ 98.83%	+ 95.9%	○ 92.02%	++ 98.56%	+ 95.14%	++ 98.62%
误杀率	+	+	○	++	+	++
扫描速度	+	○	--	○	+	++
预判杀毒 (针对新病毒, zero-day, 变种)	++	○	+	+	+	+
新病毒响应时间	+ 2~4 小时	○	++0~2 小时	○	+	○
AntiRootkits	+	○	+	+	++	'++
病毒清除	+	+	+	++	+	'++
	'++ 最好 + 好 ○ 一般 - 差 -- 最差					
Sophos 比较于 kaspersky	*Sophos 在杀病毒, 杀广告软件、间谍软件, 杀新病毒/变种病毒/未知病毒, 误杀率、扫描速度上都远远超过 kaspersky *同时 kaspersky 在广告软件间谍软件、误杀率、扫描速度上都低于业界平均水平 * Kaspersky 杀毒速度慢, 杀毒时严重影响客户正常工作, 产品以单机版为主, 企业版管理能力差					
Sophos 比较于 Mcafee	*sophos 在杀病毒, 杀广告软件、间谍软件, 杀新病毒/变种病毒/未知病毒, 扫描速度, 新病毒相应时间上都远远超过 mcafee *Mcafee 的扫描速度和新病毒相应只是业界一般水平, 病毒查杀率只有 95.58% *Mcafee 的企业版管理特别复杂, 对于 200 用户以下的客户, 很难使用其管理中心。					
Sophos 比较于 Trend	*sophos 在杀广告软件、间谍软件、新病毒、变种病毒、未知病毒能力上远远超过 trend *广告软件查杀只有 95.14% * Trend 内部使用多个引擎, 杀毒速度慢。企业管理能力弱。					
Sophos 比较于 Symantec	*Sophos 在杀病毒、新病毒、变种、未知病毒、以及新病毒响应时间上都超过 symantec					

SOPHOS

	*symantec 杀毒能力弱， 响应速度慢， 是业界公认的。
Sophos 相较于 Rising	*Rising 作为不错的国内杀毒，在反病毒各方面与国外一流产品的差距还是很大的。 大部分指标都是一般水平 * 简单的杀毒软件，作为企业版，管理能力弱
总结	*防病毒产品最重要和基本的能力是查毒，即病毒、广告软件、间谍软件、新病毒、未知病毒、变种病毒的检测能力。在这方面，Sophos 为 3 个++，都远超过其它竞争对手。 *Sophos 产品的所有方面都是业界+（好）以上水平，没有 0（一般），-（差），--（最差），而其他几家都有或多或少的 0，-， --

数据来源，请参考：http://www.virusbtn.com/news/2008/03_13a.xml

三、 企业反病毒详细对比

等级表			
类别	McAfee Total Protection for Enterprise	Sophos Endpoint Security and Console 7.0	Symantec Endpoint Protection 11.0
安装及部署	▲▲	▲▲▲▲	▲▲▲
可用性及管理	▲▲▲	▲▲▲▲	▲▲▲
可视性	▲▲▲▲	▲▲▲▲	▲▲▲▲
有效性（基本）	▲▲▲▲	▲▲▲▲	▲▲▲
有效性（zero-day）	▲▲▲	▲▲▲▲▲	▲▲▲
性能	▲▲▲	▲▲▲▲	▲▲▲
总体	▲▲▲	▲▲▲▲	▲▲▲
快速总结	McAfee Total Protection for Enterprise在Active Directory同步及固定报表引擎方面提供一些新功能，但仍然很复杂，并且zero-day保护性差。	Sophos Endpoint Security and Control 是一款设计很好的产品，对那些寻求一种高集成度 endpoint 安全套件的企业来说，这是很好的选择，它可以有效防护 zero-day 威胁。	Symantec Endpoint Protection 11.0 具有比以前版本更好的管理及集成功能，但我们发现其缺乏 zero-day 或基于行为的探测功能，用户也会发现从以前版本升级到新版本非常困难。
关键字：▲ 差，▲▲ 清楚 ▲▲▲ 一般 ▲▲▲▲ 好 ▲▲▲▲▲ 优秀			

四、 为什么选择 Sophos

公司实力	20 多年病毒防御经验
	全球 1 亿多客户的选择
	全球销量前三的安全软件公司

强大	专注于企业、教育、政府客户，不向个人用户零售	
杀毒能力强劲	单引擎提供防御病毒、广告软件、间谍软件、未知病毒、HIPS、应用程序控制	
	2008 年最新 AV-test 测试中，唯一一家在病毒、广告软件、间谍软件、未知病毒、变种病毒、新病毒各方面都获得”++”顶级鉴定的安全软件	
	扫描速度快	
	全盘扫描时，不影响用户正常工作	
	专利缓存决策技术：用户重复扫描硬盘时，只扫描必要文件，速度非常快	
	完美防御最新的 U 盘病毒等恶性病毒	
安全防护功能完整	应用程序控制： 监控或阻止客户端使用 QQ、Skype、eDonkey、游戏等数百种应用	
	设备控制： 监控或阻止客户端使用软盘、U 盘、光驱、蓝牙、wifi 等移动设备，避免机密数据流失	
	HIPS 运行时行为分析： 实时检测可疑行为及缓冲区溢出，阻断可以进程或仅报告给管理员。	
集成的网络准入控制(NAC)	监测并评估客户端安全水平（windows 补丁，杀毒软件状态，个人防火墙状态），不符合要求者，隔离处理。	
	支持应用代理和 Web 代理，支持 DHCP 隔离	
	纯软件产品，安装简单，不需要改动任何已有网络硬件。	
	提供整个网络安全漏洞报告	
强大的集中控管	一个管理窗口下，同时管理监控多达数十万客户端	
	支持 Windows、MAC、Linux 的同时监控	
	支持总部—分公司---客户端级联环境，内外网隔离环境	
	管理面板实时显示各客户端的状态：是否染毒，病毒名称，病毒样本更新情况，防火墙状态，是否在使用受控应用程序和受控设备，策略是否一致，其他错误和提示信息	
	管理中心可以远程控制客户端：下发最新策略，更新样本库，全盘扫描，清除已发现病毒等	
	支持客户端分组，可以以组的方式，控制组内所有客户端	
	提供灵活的报告，分析某时间段、某些客户端的染毒情况，支持导出为 pdf,html,xls 等格式	
简单，易用	支持 Active directory 自动部署，客户端不用做任何事	
	管理中心生成企业定制的安装包，客户端只需获得安全包，点击“下一步”或“确定”，无需其它任何配置， 即可部署完以上所有功能。	
	企业只需要一个外网连接：管理中心从 sophos 网站更新、生成最新引擎、样本，各客户端从管理中心更新或从级联的管理中心更新	
	支持主备升级源，笔记本等移动用户在公司从管理中心下载，在家从 sophos 网站下载，自动切换。	
全线安全产品	Endpoint Security and Control	传统的杀毒软件---防御病毒攻击
		应用程序控制 --- 监控和阻止影响工作效率的应用程序
		设备控制 ---监控和阻止移动设备使用，避免核心数据流失
		网络准入控制 NAC --- 隔离隐患计算机，防患于未然
	邮件安全网关 --- 反垃圾邮件，邮件病毒，及邮件内容控制，提升员工工作效率	
	网页安全网关 --- 过滤员工上网内容，防御内嵌病毒、广告软件，提升员工工作效率。	
NAC Advanced --- 相比于 ESC 里集成的 NAC，支持更多检查及更多强制		

附：管理中心控制台抓图

