TREND MICRO™ Securing Your Web World

NSS Labs 2010Q3 测评报告解读

Crane Shen
5th Nov 2010

NSS Labs

Agenda

1. 测评简介
2. 恶意软件防护评测
3. 漏洞防护评测
4. 性能影响
5. 总结

附录A：恶意软件防护测试环境与方法

附录B：关于NSS Labs

TREND MICRO

1. 测评简介

- 消费者周围充斥着太多声称可以保护他们免遭这些攻击的安全产品。当前存在超过 40 家防病毒厂商，消费者对如何选择很容易感到困惑
- 为帮助消费者就如何保护自身作出更好的、基于经验的决定，NSS Labs 进行了此次防恶意软件产品测试。
- 在整个测试过程中，完全按照现实世界中人们访问 Internet 的方式进行测试。整个产品测试报告详述了抵御以下威胁和感染源：
  - 从 Internet 上的 Web 站点下载的恶意软件
  - 客户端应用程序漏洞，如 Windows® Internet Explorer®、Mozilla® Firefox®、Apple® Quicktime® 和 Adobe® Acrobat®。

TREND MICRO

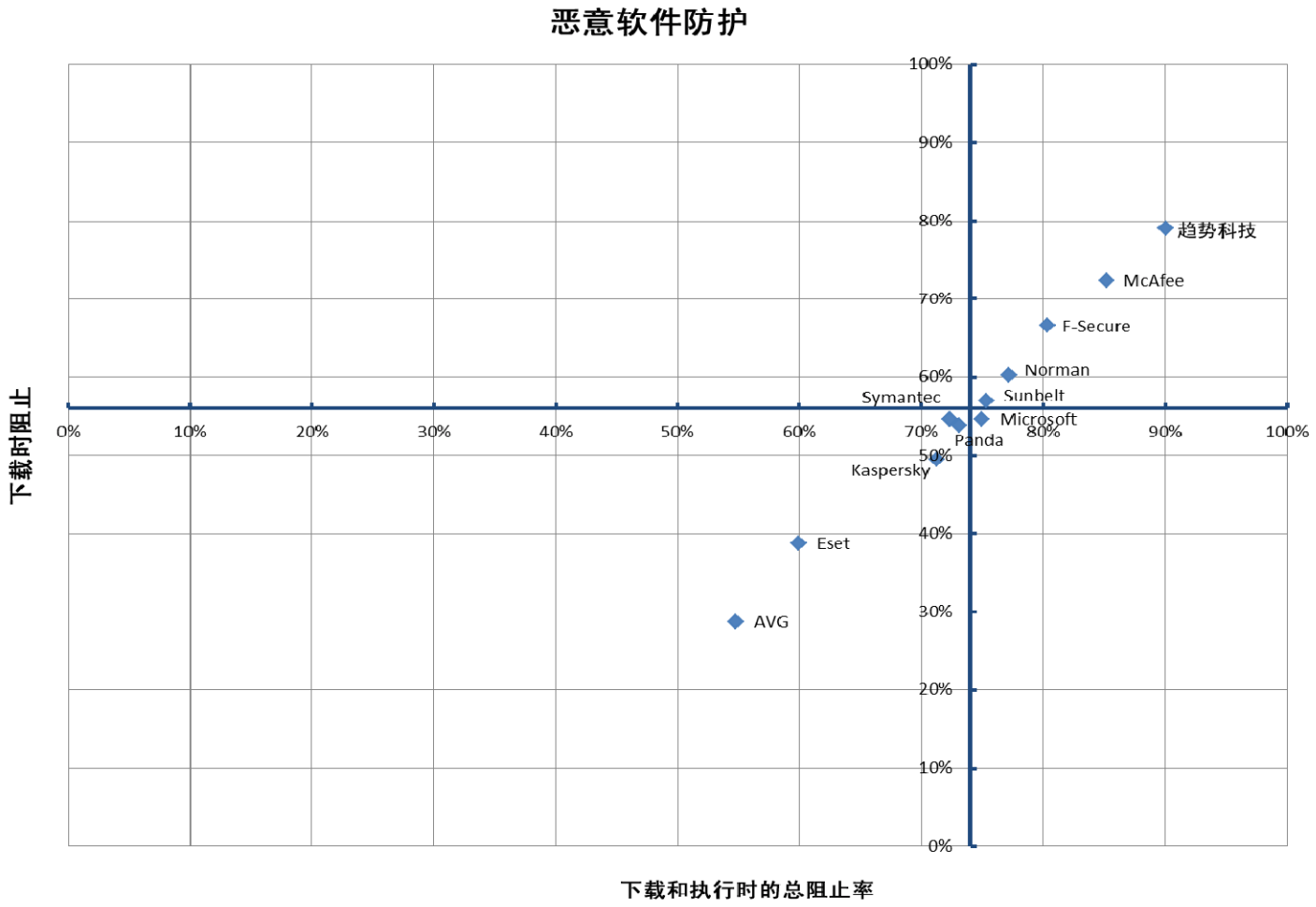
2. 恶意软件防护评测

- 基于社会工程学的恶意软件攻击欺骗用户下载并运行伪装成电影文件、代码和其他实用程序的恶意软件程序。这种基于 Web 的感染源占现今恶意软件总数的 50% 以上。由于犯罪活动越来越猖獗，检测和阻止这些威胁一直是一个巨大的挑战。防病毒研究人员平均每天检测到 50,000 种新的恶意程序，并且 2009 年和 2010 年的恶意软件增长统计数据表明有加速趋势

TREND MICRO

2.1主动防护和执行防护

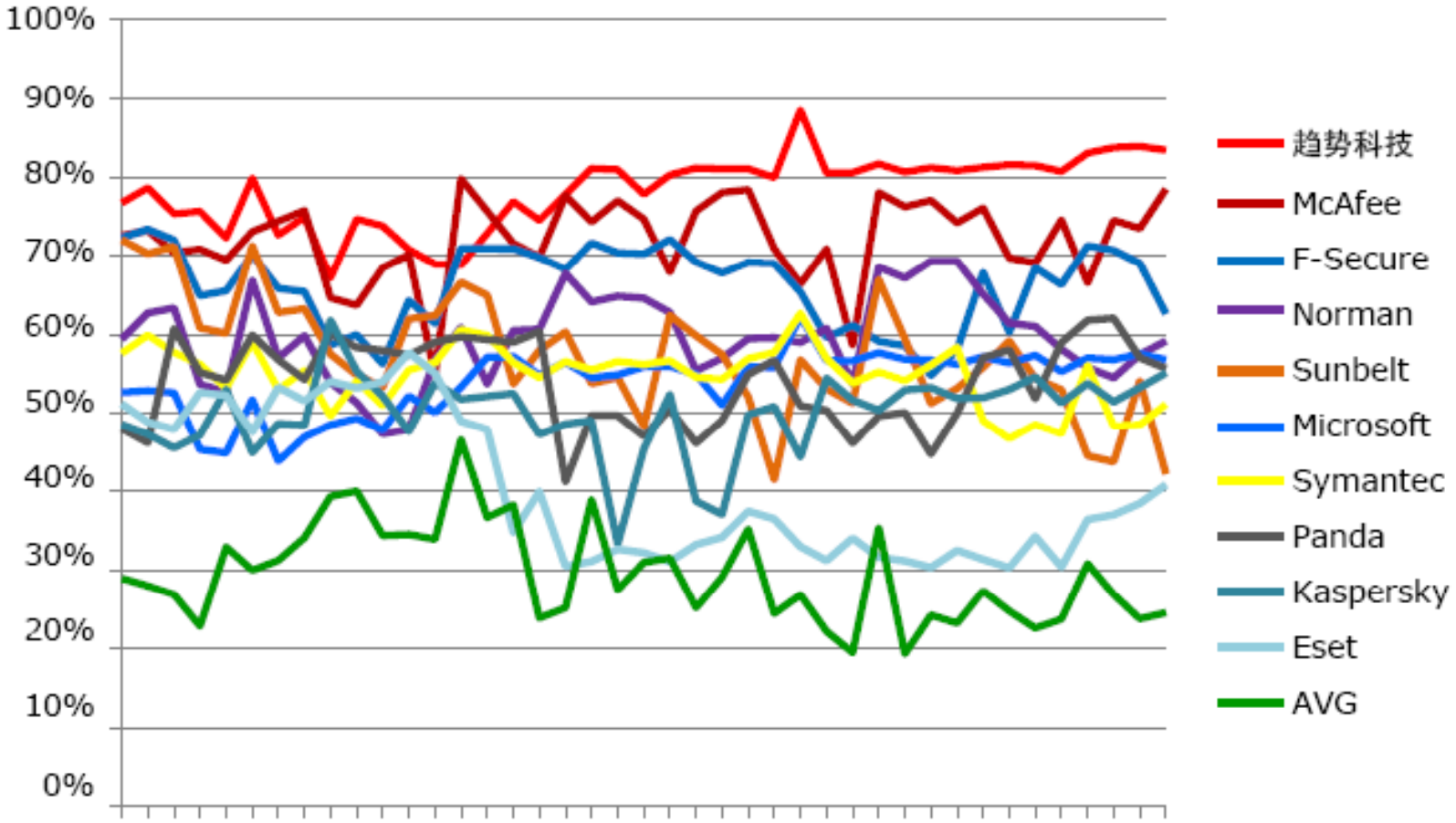
“下载时阻止”表示恶意软件被完全阻止在计算机之外。
对于通过这第一道防线的恶意软件，还评估了“执行时阻止”百分比。



2.2 延时阻止带有恶意软件的 URL

衡量阻止单个 **URL** 的能力仅代表一方面，在日常使用中，用户会访问大量变化迅速的站点。因此，在任意给定的时间，恶意 **URL** 集不断变化；持续阻止这些站点是衡量有效性的重要标准。**NSSL Labs** 每隔六个小时测试一组实时 **URL**。

下面的图中显示了在整个测试期间对阻止的重复评估：



2.3 下载和执行

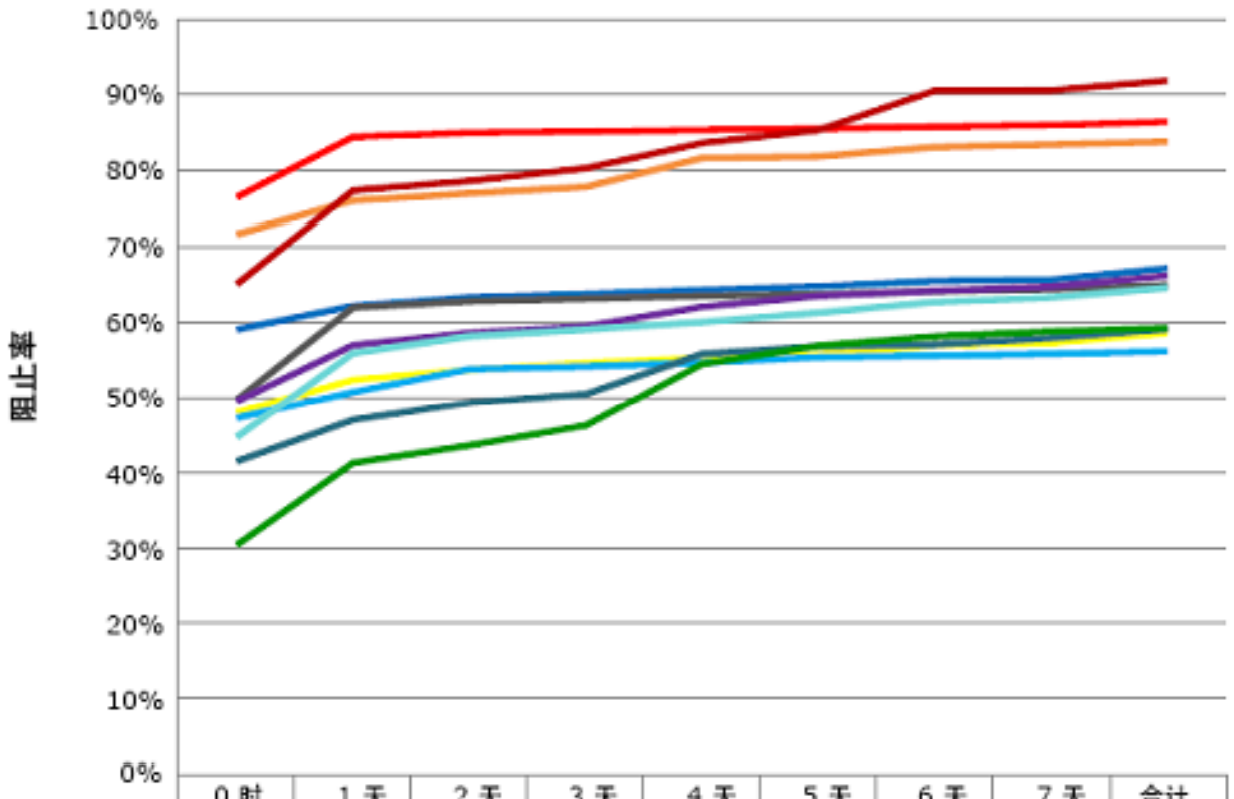
下面的表格提供了在2.1和2.2图表 中的详细结果，按照“总阻止率”对产品进行分类

产品	下载时 阻止率 (A+B)	执行时 阻止率的增 加值 (C)	总阻止率
趋势科技	79.0%	11.1%	90.1%
McAfee	72.4%	12.8%	85.2%
F-Secure	66.6%	13.8%	80.4%
Norman	60.3%	16.9%	77.2%
Sunbelt	57.0%	18.3%	75.3%
Microsoft	54.6%	20.3%	75.0%
Panda	53.8%	19.3%	73.1%
Symantec	54.6%	17.7%	72.3%
Kaspersky	49.5%	21.8%	71.3%
Eset	38.7%	21.3%	60.0%
AVG	28.7%	26.1%	54.8%

TREND MICRO

2.4 防护时间

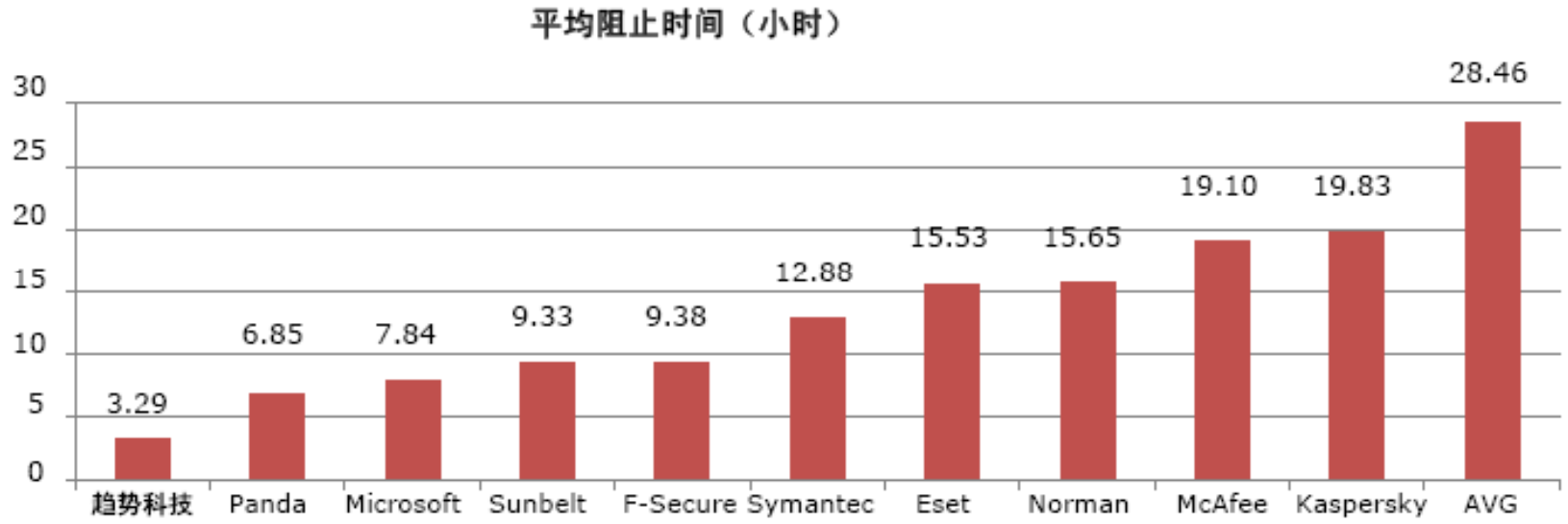
总体而言，零时防护率达到了总防护率的一半；
性能最差的产品 **(AVG)** 在零时的恶意软件捕获率停留在 **30%**
性能最好的产品（趋势科技）则停留在 **76.4%**。



	0 时	1 天	2 天	3 天	4 天	5 天	6 天	7 天	合计
趋势科技	76.4%	84.3%	84.8%	85.0%	85.2%	85.4%	85.7%	85.8%	86.3%
Sunbelt	71.7%	76.0%	76.9%	77.7%	81.6%	81.7%	83.0%	83.3%	83.7%
McAfee	65.1%	77.3%	78.5%	80.2%	83.5%	85.2%	90.4%	90.5%	91.7%
F-Secure	59.1%	62.2%	63.4%	63.8%	64.3%	64.8%	65.5%	65.7%	67.2%
Panda	49.7%	62.0%	62.8%	63.2%	63.5%	63.7%	64.2%	64.4%	65.0%
Norman	49.6%	57.0%	58.6%	59.5%	62.1%	63.5%	64.3%	64.8%	66.2%
Symantec	48.0%	52.4%	53.7%	54.6%	55.3%	55.8%	57.0%	57.3%	58.6%
Microsoft	47.3%	50.8%	53.8%	54.2%	54.7%	55.4%	55.6%	55.9%	56.2%
Eset	44.7%	56.0%	58.2%	59.1%	60.1%	61.3%	62.7%	63.4%	64.6%
Kaspersky	41.5%	47.1%	49.4%	50.5%	55.9%	56.9%	57.1%	58.0%	59.2%
AVG	30.5%	41.4%	43.7%	46.3%	54.5%	57.0%	58.2%	58.8%	59.4%

2.5 阻止恶意软件的平均响应时间

用户要等待多长时间，安全产品才能阻止恶意站点？



2.7 评分方法

“实时云端 (Live-in-the-Cloud)”测试框架

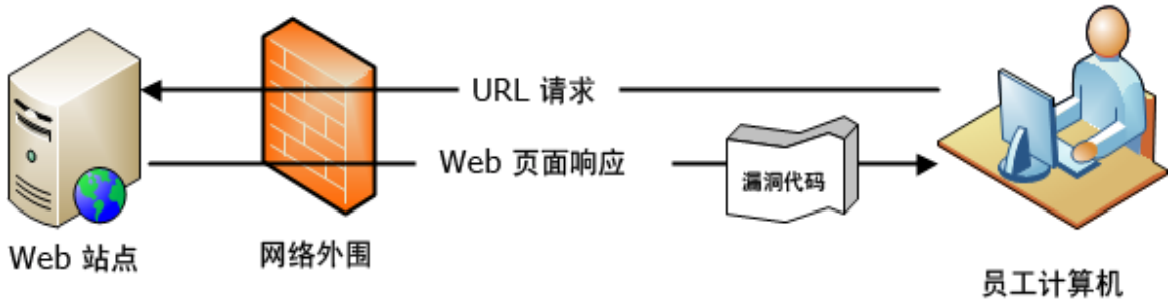
“实时测试”框架重点关注从庞大的全球智能网络中收集到的、当前活跃在 Internet 上的威胁。重复进行的测试在发现恶意软件的几分钟内将其引入到测试工具中，并每隔 6 小时重复测试，每次都添加新发现的恶意站点。从 2010 年 8 月 22 日到 2010 年 9 月 1 日的 11 天中，NSS Labs 的工程师们运行了包含 3,433 个独特恶意 URL 的 57,000 次测试。

预防阶段	阻止率
1. URL/文件访问（信誉）	A
2. 下载	B
3. 执行	C
总体防护	A+B+C = 100%（最大）

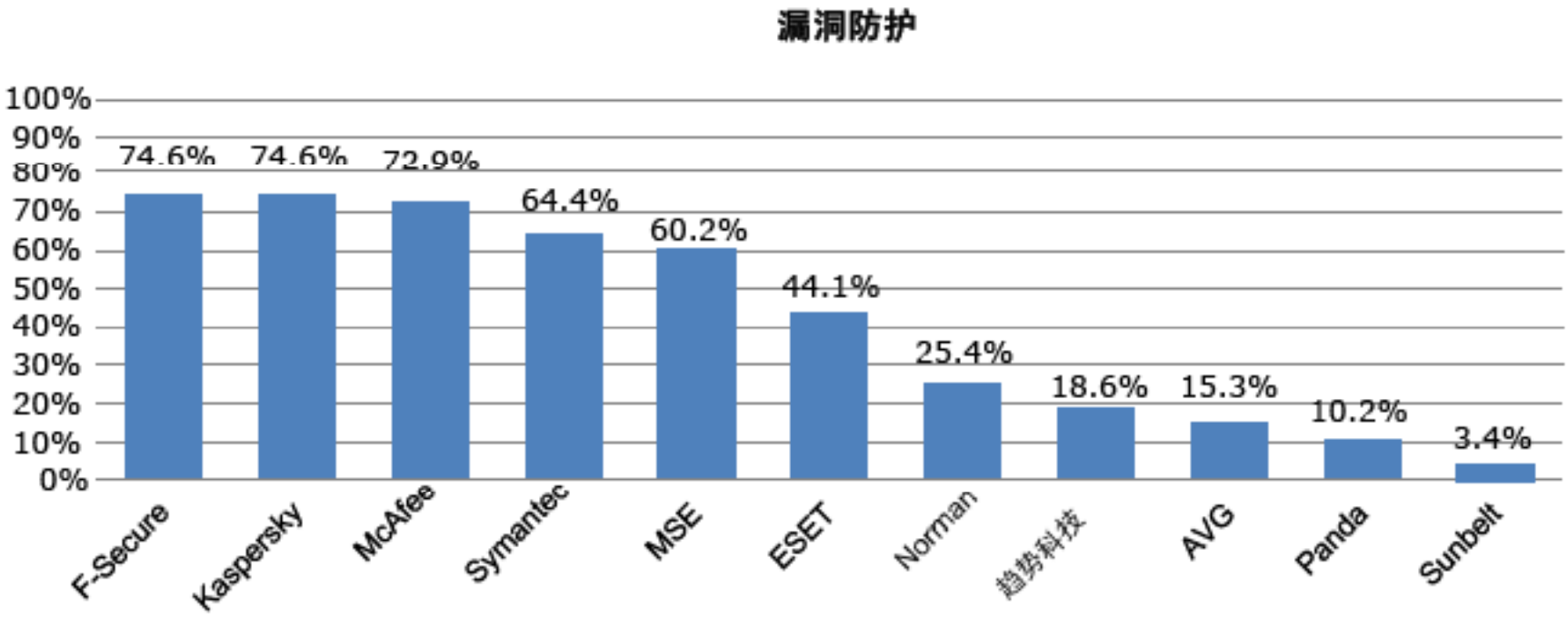
TREND MICRO

3. 漏洞防护

人们普遍持有这样一种观念 — 只要不访问 **Internet** 的“阴暗”部分，便不会处于遭受攻击的风险。这显而易见是错误的；无论最终用户访问哪里，他们都处于风险之中。即使像《华尔街日报》、《纽约时报》和 **MLB.com** 这样的站点都曾向其读者提供过恶意内容



3.1 漏洞防护测试结果与测试方法



这些测试是通过**Metasploit** 等最新的渗透测试工具在受控环境下执行的。这些测试用来评估产品的原始漏洞检测能力，而不管从何处发起攻击。
应当注意的是，某些厂商提供了信誉系统，可以阻止访问受感染的 **Web** 站点。尽管此技术可以防御某些特定的站点，但它无法防御原始类型(主动)的攻击，这种攻击可以通过数十亿不同的 **Internet** 地址进行投递。

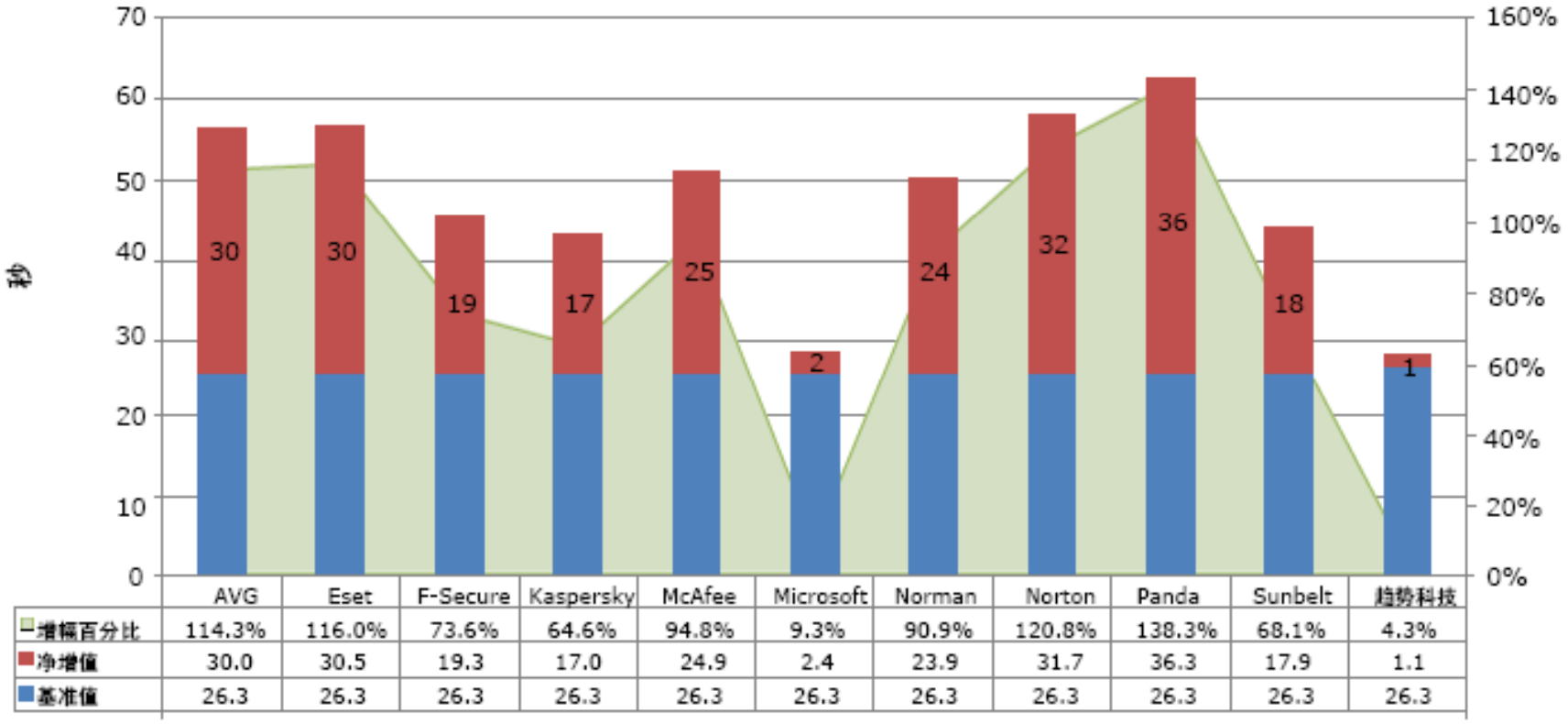
4. 性能影响

安全产品会降低系统的运行速度并耗费用于其它应用程序的内存，从而影响性能。这是一项必要的交换，一些安全产品对特定的应用程序影响较大，而对其他应用程序则影响较小。尽管比较有效的解决方案通常对系统的影响较大，但相反的观点并不一定成立，即不要认为对系统性能影响大，系统的安全性会更高。

对每个应用程序，我们执行了 **500** 次热启动以确保结果正确。相关的误差幅度为 **4.38%**，可信度为 **95%**。因此，如果我们的结果显示增加了 **1** 秒，则 **100** 次测试中有 **95** 次增加了一秒，结果介于 **0.9562** 秒到 **1.0438** 秒之间。

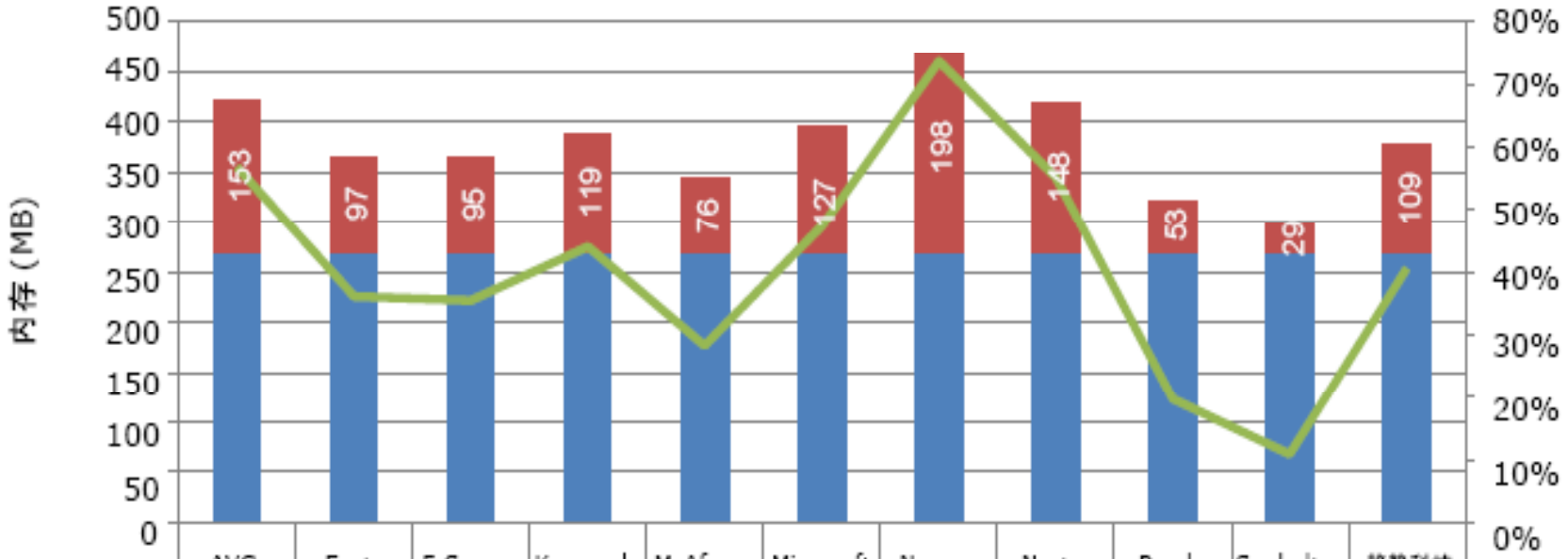
TREND MICRO

4.1 启动时间



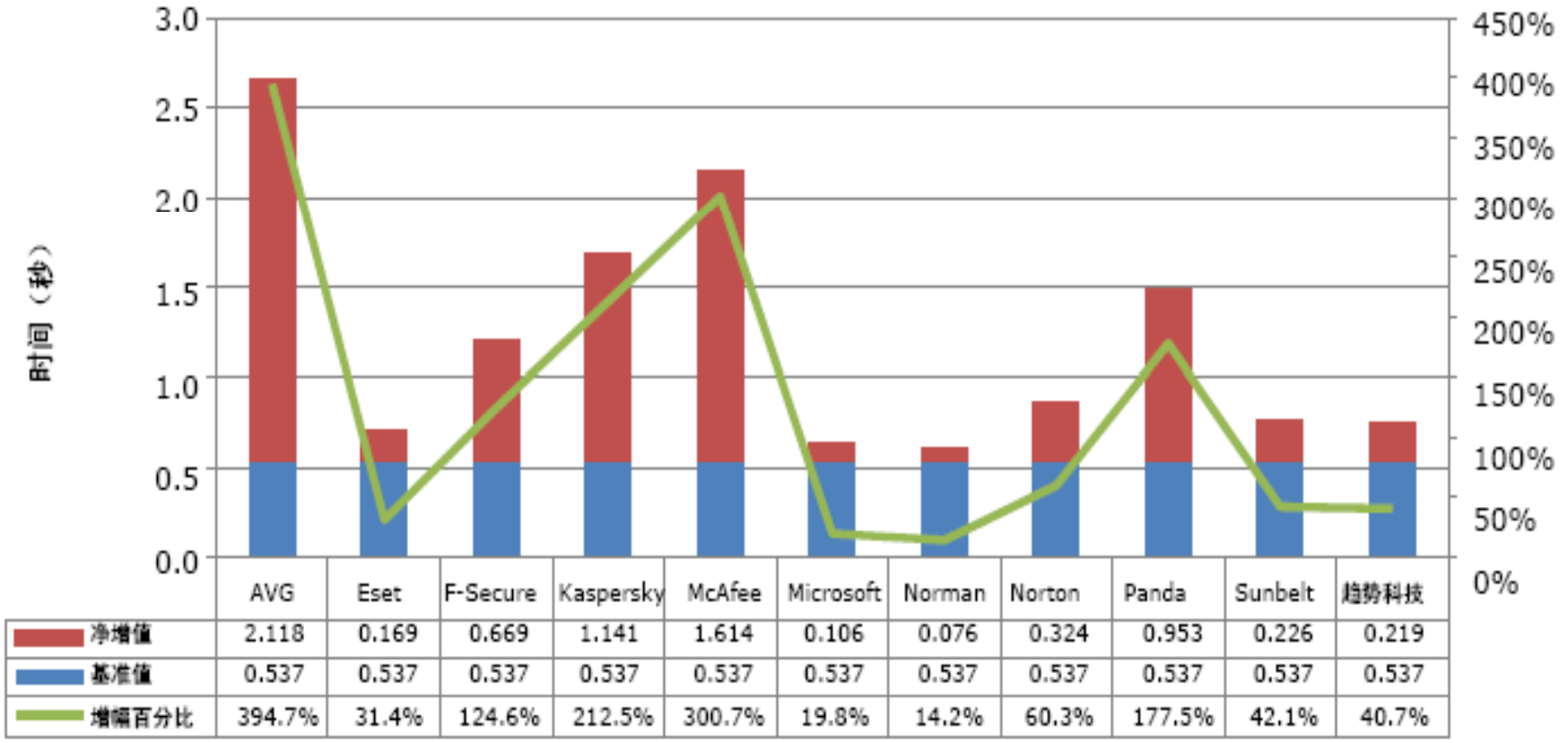
	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	趋势科技
增幅百分比	114.3%	116.0%	73.6%	64.6%	94.8%	9.3%	90.9%	120.8%	138.3%	68.1%	4.3%
净增值	30.0	30.5	19.3	17.0	24.9	2.4	23.9	31.7	36.3	17.9	1.1
基准值	26.3	26.3	26.3	26.3	26.3	26.3	26.3	26.3	26.3	26.3	26.3

4.2 空闲时的内存使用率



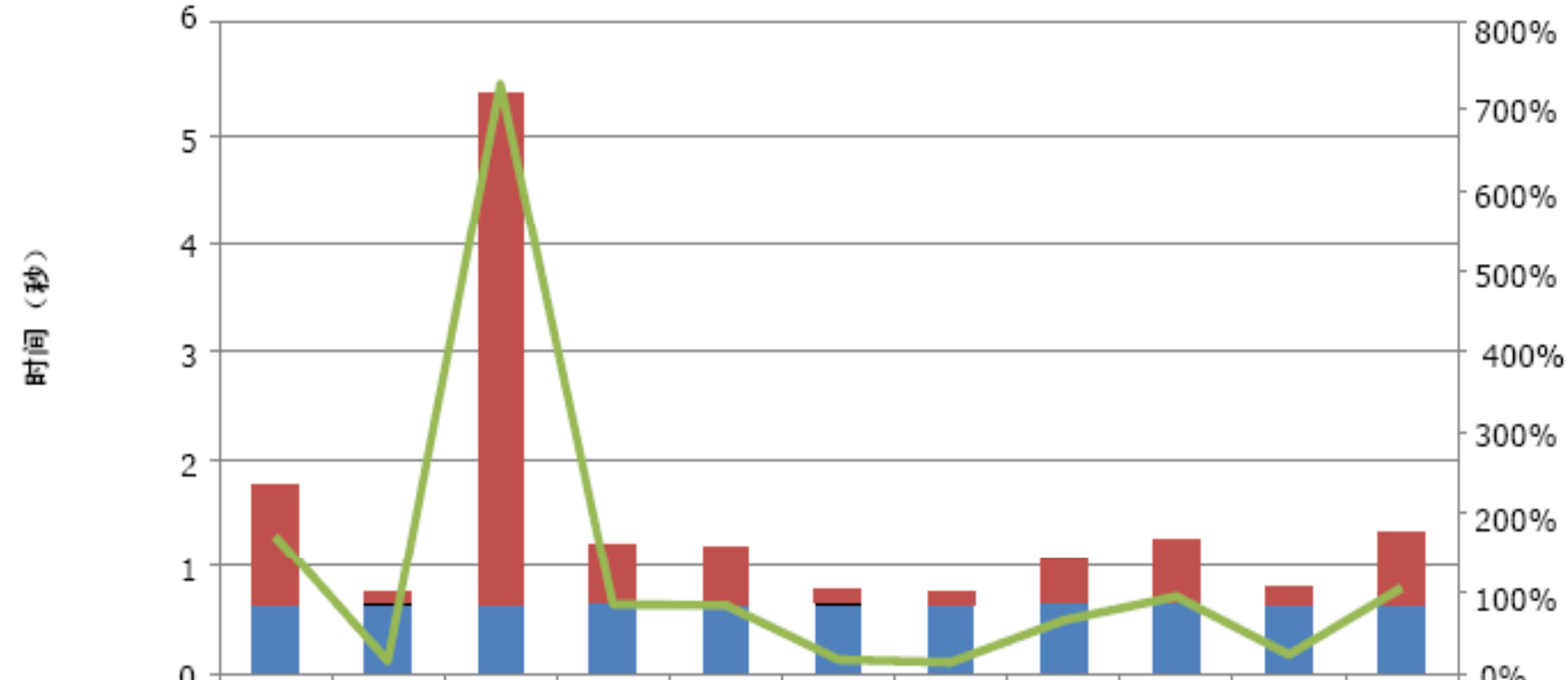
	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	趋势科技
净增值	153	97	95	119	76	127	198	148	53	29	109
基准值	269	269	269	269	269	269	269	269	269	269	269
增幅百分比	56.8%	36.1%	35.4%	44.1%	28.3%	47.3%	73.6%	55.2%	19.7%	10.9%	40.6%

4.3 OUTLOOK 2007



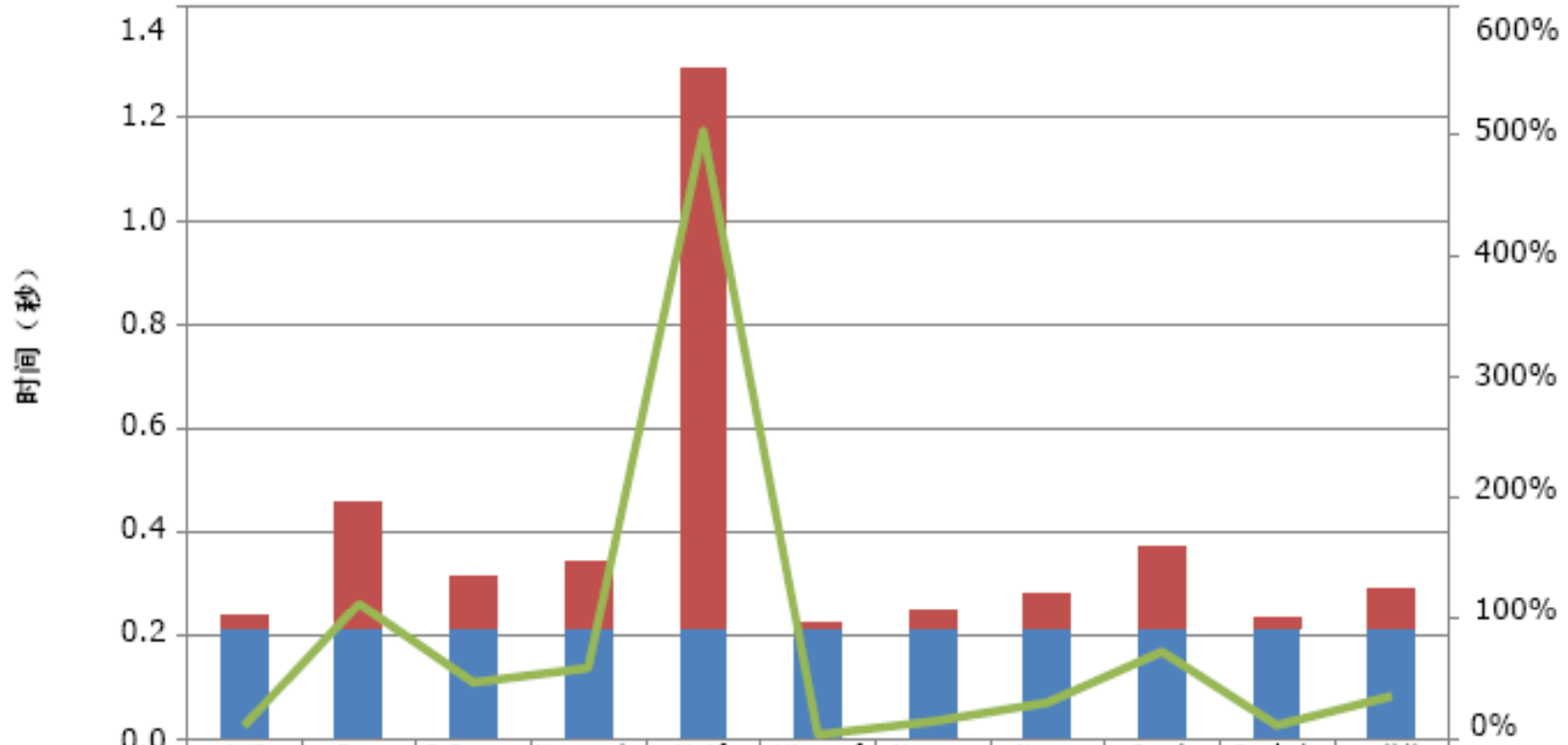
	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	趋势科技
净增值	2.118	0.169	0.669	1.141	1.614	0.106	0.076	0.324	0.953	0.226	0.219
基准值	0.537	0.537	0.537	0.537	0.537	0.537	0.537	0.537	0.537	0.537	0.537
增幅百分比	394.7%	31.4%	124.6%	212.5%	300.7%	19.8%	14.2%	60.3%	177.5%	42.1%	40.7%

4.4 INTERNET EXPLORER 8



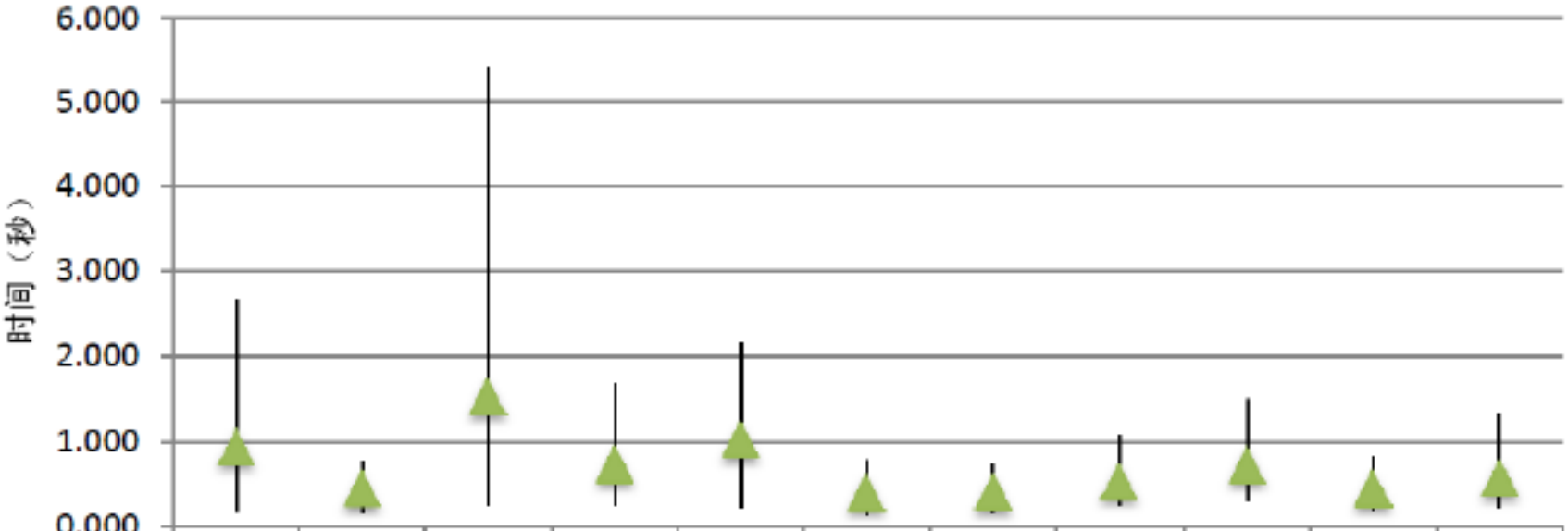
	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	趋势科技
净增值	1.117	0.100	4.758	0.553	0.549	0.114	0.091	0.426	0.616	0.151	0.687
基准值	0.650	0.650	0.650	0.650	0.650	0.650	0.650	0.650	0.650	0.650	0.650
增幅百分比	171.8%	15.5%	732.0%	85.0%	84.4%	17.5%	14.0%	65.5%	94.8%	23.3%	105.8%

4.5 WORD 2007



	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	趋势科技
净增值	0.023	0.240	0.099	0.125	1.079	0.007	0.031	0.064	0.154	0.024	0.075
基准值	0.215	0.215	0.215	0.215	0.215	0.215	0.215	0.215	0.215	0.215	0.215
增幅百分比	10.6%	111.6%	46.2%	58.4%	502.7%	3.4%	14.2%	29.8%	71.8%	11.2%	35.1%

4.6 启动应用程序的平均净增时间



	AVG	Eset	F-Secure	Kaspersky	McAfee	Microsoft	Norman	Norton	Panda	Sunbelt	趋势科技
高	2.655	0.750	5.408	1.677	2.151	0.764	0.741	1.076	1.490	0.801	1.337
低	0.172	0.161	0.253	0.248	0.219	0.171	0.188	0.249	0.291	0.198	0.206
▲平均值	0.933	0.441	1.525	0.728	1.019	0.396	0.402	0.523	0.720	0.436	0.559
增幅百分比	166.1%	26.0%	335.2%	107.6%	190.8%	13.1%	14.6%	49.3%	105.4%	24.4%	59.4%

热启动应用程序

5. 总结

产品	恶意软件阻止率	漏洞阻止率	性能影响
趋势科技	90.1%	19%	0.21
McAfee	85.2%	73%	0.67
F-Secure	80.4%	75%	1.17
Norman	77.2%	25%	0.05
Sunbelt	75.3%	3%	0.37
Microsoft	75.0%	60%	0.05
Panda	73.1%	10%	0.17
Symantec	72.3%	64%	0.09
Kaspersky	71.3%	75%	0.38
Eset	60.0%	44%	0.09
AVG	54.8%	15%	0.58

- ✓ 防护能力良莠不齐，有效率介于 **54%** 到 **90%** 之间，最高与最低之间相差 **36%**。
- ✓ 利用 **Web** 进行攻击的网络犯罪分子有 **10%** 到 **45%** 的机会绕过您的防病毒产品
- ✓ 利用漏洞进行攻击的网络犯罪分子有 **25%** 到 **97%** 的机会损害您的计算机

TREND MICRO

5. 总结---产品指导

- ✓ 趋势科技提供了最佳的 **Web** 恶意软件防护，并拥有极好的性能（即影响最小）。
- ✓ **McAfee** 和 **F-Secure** 也拥有较好的 **Web** 恶意软件防护能力。
- ✓ **F-Secure**、**Kaspersky** 和 **McAfee** 拥有最佳的漏洞防护能力。但是，**McAfee** 和 **F-Secure** 在性能影响方面表现最差。

评定	*产品（按字母顺序）*
推荐	F-Secure 趋势科技
中立	Kaspersky Microsoft Norman Panda Sunbelt Symantec
谨慎	AVG ESET

TREND MICRO

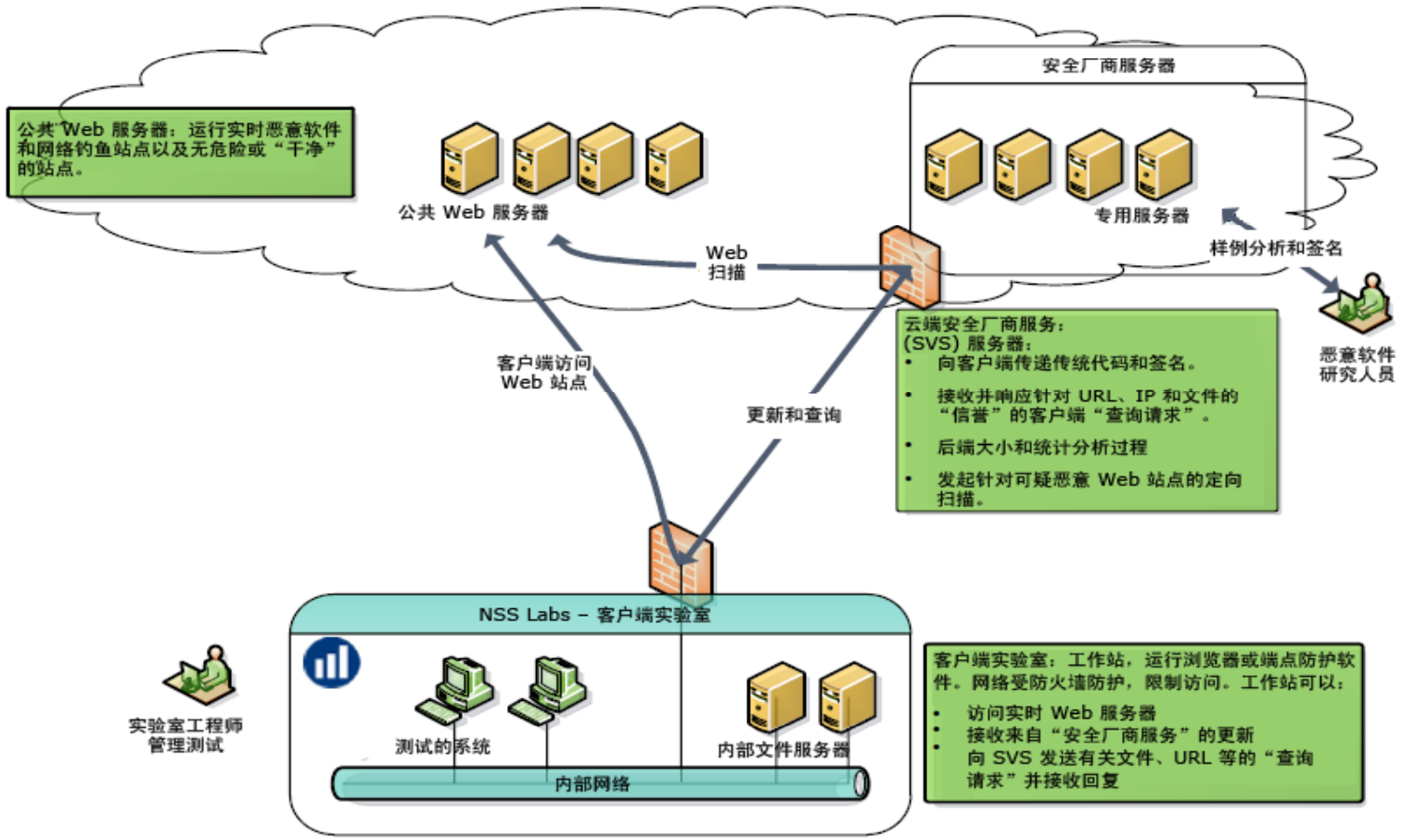
附录 A：恶意软件测试环境

“实时测试”工具和方法

所有产品均连接到真实 **Internet** 并且能够接收签名更新、软件更新和信誉更新或由厂商发布的其他信息。

测试阶段：

1. 信誉 - 允许用户访问站点
2. 下载 - 在下载期间阻止恶意内容
3. 执行 - 一旦有恶意内容保存在 **PC** 上，将阻止其运行



本测试以全天候方式 **(24x7)** 持续执行了 **9** 天，每隔 **6** 小时执行一次。发现新样例时，将其添加到测试中，之前发现的样例要重新测试。

附录 B：关于 NSS LABS, INC.

NSS Labs, Inc. 是全球领先的独立信息安全研究和评测机构。通过专业的分析，该机构可以在信息技术专业人士为其组织选择合适产品时向他们提供公正的参考数据。**NSS Labs** 于 **1991** 年发布第一个此类评测标准，从而开创了入侵检测和防御系统评测的历史，它还定期对防火墙、一体化威胁管理、恶意软件防护、加密、**Web** 应用防火墙和其他技术进行评估。该机构的真实评测方法是评估安全产品的网络威胁防护能力的唯一方法。

NSS Labs 评测被认为是行业内最具说服力的参考信息，能够得到它的推荐是许多安全企业梦寐以求的事情。该机构成立于 **1991** 年，目前在加利福尼亚州的卡尔斯巴德以及德克萨斯州的奥斯丁均设有分部。