全球特殊威胁分析与防护：
2013-2017 年预测及 2012 年厂商市场份额

非官方中文译本 · 安天实验室 译注

文档信息			
原文名称	Worldwide Specialized Threat Analysis and Protection: 2013 – 2017 Forecast and 2012 Vendor Shares		
原文作者	John Grady, Phil Hochmuth, Charles J. Kolodgy	**原文发布日期**	2013 年 8 月
作者简介	John Grady 是 IDC 安全产品部门的研究经理。在此期间，Grady 对网络安全市场进行深入研究，为客户提供准确的预测和有见地的分析。他的研究重点领域包括防火墙、VPN、入侵检测与防御、统一威胁管理技术。 http://www.idc.com/getdoc.jsp?containerId=PRF002808 Charles J. Kolodgy 是 IDC 安全产品部门的研究副总裁。在此期间，他执行主要研究项目，并并厂商和用户分析市场。 http://www.idc.com/getdoc.jsp?containerId=PRF000196		
原文发布单位	国际数据公司（International Data Corporation，IDC）		
原文出处	http://www.idc.com/getdoc.jsp?containerId=242346		
译者	Lily	**校对者**	Lily
免责声明	本译文为安天实验室针对网络资料翻译而成，并未取得原作者授权，仅供内部学习和交流使用，安天实验室不对任何可能因此导致的版权问题承担责任。		

IDC
Analyze the Future

市场分析

全球特殊威胁分析与防护：2013-2017 年预测及 2012 年厂商市场份额

John Grady，Phil Hochmuth，Charles J. Kolodgy

IDC 的观点

如今，网络犯罪已经从快速打砸抢战术演变到更精致的“长期持续性攻击”。犯罪组织，甚至政府，开发专门的恶意软件，针对特定目标，试图植入目标基础设施。这种恶意软件用于一系列未被发现的恶意活动，持续数月或数年，包括数据窃取、间谍活动、扰乱、破坏基础设施和进程。虽然方法不同，但是这些攻击的共性是：它们规避主流安全技术的检测，如反病毒软件、防火墙、内容检查网关。随着这些特殊威胁的出现，在过去几年中出现了新的安全技术，旨在检测、分析并防御这些威胁。IDC 将这个市场定义为特殊威胁分析与防护（STAP）。对当前特殊威胁全景和新市场的观察包括：

- STAP 技术可以二次防御强大的高级针对性攻击。通常情况下，大型企业部署 STAP 产品，以加强现有网络或端点安全产品。STAP 的早期应用者包括大型金融机构、政府机构、迫切需要保护数据的大型企业。
- 企业为 STAP 技术划拨了额外的预算，而不是将其他解决方案的预算转移到 STAP 技术。因为数据窃取、网络安全、黑客攻击、高级恶意软件仍然是企业高管和 IT 管理人员的头等大事，所以 IDC 认为这种趋势会持续下去。这一趋势可能有助于 STAP 厂商和其他高级恶意软件检测厂商在市场中的成长，而不会进入与更大、更成熟的安全厂商的直接竞争。
- IDC 预计，网络、终端、内容安全厂商最终会将 STAP 纳入现有解决方案，对现有产品进行补充。在企业中，对 STAP 解决方案的单独预算最终将与其他安全技术预算一起得到巩固，从而为现有安全厂商和 STAP 创业公司提供更大的竞争力。然而，很多现有安全企业直到最近才开始开发和提供 STAP 解决方案，并正在追平较小的 STAP 厂商（其中一些厂商已向客户提供产品超过 5 年了）。

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

Filing Information: August 2013, IDC #242346, Volume: 1
Security Products: Market Analysis

目录

表格目录

图形目录

关于该研究

本研究探讨了 2011-2017 年期间的特殊威胁分析和防护市场 ,并分析了收入趋势和市场增长预测。本文分析了 2011 年和 2012 年全球 STAP 市场规模，2012 年领军厂商的收入和市场份额；同时预测了 2013-2017 年的增长趋势。

方法论

请参见“更多信息”章节，以了解本研究所采用的预测和分析方法。

另外，请注意以下几点：

- 该预测分析了特殊威胁分析及防护产品的市场份额。
- 有关 IDC 定义和方法的更多信息，请参阅 *IDC's Worldwide Security Products Taxonomy, 2012 (IDC #235288, June 2012)*或 *IDC's Software Taxonomy, 2013 (IDC #241527, June 2013)*。
- 本研究在 2013 年年初进行。本研究中的一些信息均来自 2013 年 6 月 20 日的“Worldwide Security ApplianceTracker”，2013 年 5 月 2 日的“IDC's Software Market Forecaster database”。
- 本研究中呈现的数据代表了 IDC 基于各种数据来源的最佳估计，而不一定包括厂商的直接反馈。
- 由于采取四舍五入，本文中的数据可能不完全准确。

STAP 的定义

特殊威胁分析与防护（STAP）市场是一个竞争激烈的市场，从以下逻辑市场获得收入：网络、通讯、终端、安全和漏洞管理（取证）。该市场中的产品必须使用无特征技术（即沙箱、仿真、大数据分析、虚容器）来检测恶意活动。这些解决方案可以基于网络层、端点、或两者兼而有之，并扫描入站和出站的异常流量，包括僵尸网络和 C&C 流量。该市场还包括进行逆向工程和恶意软件取证分析的产品。

市场综述

应该如何防御从没见过的恶意软件呢？这就是企业现今努力解决的关键问题。从某种程度上说，这个问题一直存在于 IT 安全界。十年前，蠕虫或病毒爆发的第一批受害者基本上面临同样的问题：防御措施无法应对全新的威胁，使得资源处于危险中；直到能够检测到攻击并创建特征。与现在相比，当时有两个主要的不同点。首先，攻击往往更“吵闹”，因为其目的通常是扰乱运作，而且通常很清楚出现了攻击。其次，侥幸未被攻击的企业可以自我安慰：他们的外围防御和端点保护会接收更新的特征，以扫描新威胁、被感染的远程用户、过时的系统。不幸的是，今天的世界是完全不同的。

今天的威胁几乎都是全新的，以前从未见过。就其本质而言，零日漏洞利用这一优势。然而，攻击者真正的进步在于遵循同样的理念来开发恶意软件。越来越多地情况是，每次攻击都与之前的有所不同，这使得之前侥幸未受攻击的企业失去了优势。今天的恶意软件是针对性、多态和动态的。它可以通过网页、鱼叉式网络钓鱼电子邮件、或其他各种途径传播。当前攻击的最终目标通常是数据窃取，通常采用慢速攻击法，即攻击在很长一段时间里不会被发现。在 Shady RAT 攻击案例中，入侵在未被发现的情况下进行了若干年。台式机通常不是攻击的最终目标，而是作为攻击者提权和横向运动的入口点，以便攻击整个目标机构，而在整个过程中都不会被发现。当结合零日漏洞和零日恶意软件后，攻击者获得了应对传统防御的各种方法。

为了解决这个日益复杂的问题，一种新产品出现了，该产品充分利用各种技术来收集信息，包括行为、通信、活动、信誉等，以便及时发现看似无法察觉的问题。其中许多产品试图通过利用不同的核心技术来解决同样的问题（或同样问题的某些方面）：

- **虚拟沙箱/仿真和行为分析**越来越多地被部署，以检测高级恶意软件。特征方法无法检测到从未见过的文件，所以确定文件如何运行变得越来越重要。可以将可疑文件发送到镜像企业（或企业的某些部门）的虚拟环境，对活动进行分析，以确定注册表项是否被修改、进程是否被更改、或是否正在尝试与可疑的服务器进行通信。另外，也可以将该文件发送到类似的云环境。最后，可以对网络流量进行异常行为监视，如与 C&C 服务器、其他资源、或者正常活动范围之外的网络段进行通信。

- **虚容器/隔离**解决了从端点发起的高级攻击。遵循这一框架的解决方案基本上放弃阻止恶意软件攻破企业，但是会阻止恶意文件访问互联网连接或被感染机器的系统资源。特定的应用程序或任务

可以从机器的其余部分被虚拟分离开来，确保该恶意软件不能够扩散或“与攻击者通信”，将其危害性降至最低。

- **高级系统扫描**也专注于端点，而不是分离的资源。轻载代理检查系统行为，以识别恶意活动的迹象。这可以通过监控操作系统的注册表修改、有问题的进程、其他标志，或通过分析恶意活动的实际物理内存来完成。这些解决方案需要保持轻载，以免影响性能，并在设备上保持隐蔽，使攻击者相信他们没有被监控。

正如任何新兴市场一样，STAP 市场存在既有厂商商和小型新兴厂商。每一个厂商都有其不同的针对性攻击检测方案。

关键厂商

Blue Coat

Blue Coat 公司成立于 1996 年，当时名为 CacheFlow；公司专门从事网络安全、预防数据丢失和广域网优化解决方案。其前身是一家上市公司，Blue Coat 在 2011 年被私营股权投资公司 Thoma Bravo 收购。近日，Blue Coat 已完成了对 Crossbeam Systems 和 Solera Networks 的收购。在 Web 安全市场，Blue Coat 的主要产品是 ProxySG Web 代理和网关设备产品线、ProxyAV 反恶意软件检查设备，这两者都可以通过虚拟设备和云服务交付。高级威胁防御措施通过 WebPulse 交付，WebPulse 根据浏览历史、IP 地址和域名提供实时评价，还提供沙箱功能来检查特定的文件类型。WebPulse 服务向部署的 ProxySG / AV 网关提供已知威胁的情报；基于云的沙箱功能用于以下情况：客户需要分析未分类或未知 URL 或文件的行为。从收购的 Solera 产品的角度来看，Blue Coat 通过其 ThreatBLADES 产品系列提供 STAP 功能，其中包括 MalwareAnalysis BLADE（提供可疑文件爆轰/沙箱）、WebThreat BLADE（集成 WebPulse，来扫描网络上的命令/控制通信）、FileThreat BLADE（针对可疑代码的文件信誉和分析引擎）。ThreatBLADES 技术可以作为软件部署或部署于专门设备。

Bromium

Bromium 由 Gaurav Banga、Simon Crosby 和 Ian Pratt 创建于 2010 年，他们是公司高管和技术人员，具备 PC BIOS 系统、虚拟化、安全性等领域的背景知识。Bromium 已经从 Capital Partners、Intel Capital、Andreessen Horowitz 等公司筹集了超过 3,500 万美元的风险投资。Bromium 的核心 vSentry 产品为终端计算机提供了虚拟化沙箱环境，使用了公司称之为“Microvisor”的技术，当每个与恶意软件感染有关的进程（打开文件、网页、可执行文件等）被启动时，都会创建小型的硬件隔离虚拟环境。Microvisor 据称对终端用户

不可见，它在终端用户的每个任务中创建/撤销虚拟环境，封锁潜在的恶意软件、URL 或可能的其他攻击向量。类似于每天结束时擦除的虚拟桌面，vSentry 方法旨在擦除恶意软件导致的任何损害。Bromium 还提供了 LAVA（现场进攻可视化和分析），这是一个分析和取证工具，记录终端发现的恶意软件。该公司已与金融服务客户和其他数据敏感行业取得了一些成功；然而，Bromium 的终端软件要求高端硬件，如 64 位处理器和 4GB+内存，这限制了它在一些企业的广泛部署。通常情况下，Bromium 技术只部署于高价值或处于风险中的最终用户。

CounterTack

CounterTack 总部设在马萨诸塞州的沃尔瑟姆，成立于 2004 年，当时称为 NeuralIQ 公司，2011 年更改为现在的名称。这个私营公司由 Fairhaven Capital 以及私人投资者提供资金。CounterTack 的解决方案围绕其专利的深度系统检测（DSI）技术，可监控操作系统的活动，寻找异常行为（如注册表修改、进程交互和文件操作）。CounterTack 有两个产品系列：Scout 和 Sentinel。Scout 由隐形代理（Stealth Agent）和 Scout 服务器（Scout Server）组成。隐形代理部署于终点，不为操作系统所知，并允许内核级的活动捕获。Scout 服务器可以作为物理或虚拟服务器部署，支持 CounterTack 实时分析引擎。该引擎将受监控终端收集的所有行为联系起来，整合 SIEM 和 IPS 解决方案，以帮助阻止进一步入侵并进行修复。可以支持多达 200 个代理，因此该解决方案专为高价值的生产性资产所设计。CounterTack Sentinel 专供企业部署，其分析引擎能够充分利用大数据分析，以适应企业的数据收集需求。

Damballa

Damballa 成立于 2006 年，总部设在佐治亚州的亚特兰大市，是一家私营控股公司。Damballa 的旗舰 Failsafe 解决方案包括位于网络出口点的带外设备（通信分析器），这些设备监控入站和出站通信（包括代理和非代理），以识别恶意软件源头与外部 C&C 服务器之间的通信流量。这些传感器查看流量目的地的信誉、流量内容以及端点的通信行为，从而检测恶意活动。它们通过 Case Analyzer 管理控制台的中心辐射型架构连接，该控制台整合相关信息，提供风险分析，以帮助优化进一步行动和修复。此外，在云中进行文件审查，以提供更深入的现场分析。

FireEye

自 2004 年成立以来，FireEye 募集了超过 1 亿美元的风险基金，目前拥有超过 400 名员工。公司由 Ashar Aziz 成立，现任 CEO 是 Dave DeWalt，他是前迈克菲高管。FireEye 的 Web、电子邮件和网络文件 Malware Protection System 产品由多向量虚拟执行（MVX）引擎支撑，该引擎是一个高速沙箱或虚拟执行环境；能够打开，分析和检测恶意可执行文件、文件、URL 和其他可疑的有效载荷。多个 MVX 并行于内联设备，提供了高速分析，该分析能够仿真系统试图保护的各种环境（例如，基于 Windows 的台式机）。同时，它引入最终用户和网络之间的低延迟连接。类似地，相应的 Web 和电子邮件网关也部署到传统的内容安全网关（与传统 URL、垃圾邮件黑名单的定义不同，该网关通过 MVX 平台提供分析）。网关可以作为内联保护装置，或作为被动监控端口分析引擎部署。除了这些网关，文件分析设备能够抓取网络文件共享和其他存储资源，从而扫描、识别、隔离或消除可疑或危险的文件（可能存储于机器和网络内部）。恶意软件分析和取证工具也是该解决方案的一部分，能够通过 MVX 引擎分析取证环境中的可疑文件或有效载荷。FireEye 的网关、分析引擎、与其他内部产品共享基于云的服务，为部署于合作伙伴和服务供应商网络的产品提供管理平台。FireEye 也通过其内部研究实验室（基于云服务）共享情报。

HBGary

HBGary 由 Greg Hoglund 和 Penny Leavy 于 2003 年成立。2012 年，HBGary 被联邦政府技术承包公司 ManTech International 收购。HBGary 原本只专注于咨询，从 2006 年开始开发检测和防御高级威胁的软件。目前，HBGary 拥有员工 70 余人。该公司的旗舰技术是 Digital DNA，能够分析物理内存，以识别标志 rootkit 和零日恶意软件的恶意行为。Digital DNA 被整合到 HBGary 的两大平台产品：主动防御（Active Defense）和响应专家（Responder Pro）。主动防御是基于代理的解决方案，自动收集和分析整个企业的结果，对 Windows 终端进行威胁评估，从而确定攻击范围并进行修复。响应专家是一个取证工具，可供收集整个企业物理内存和虚拟内存信息的分析人员使用，能够使事件响应团队快速搜索结果，以确定攻击范围和响应方法，并创建合规性和 ediscovery 报告。

Invincea

Invincea（原名为 Secure Command）是 Anup Ghosh 于 2006 年在弗吉尼亚州费尔法克斯创建的，是一家专注 DARPA 的研发公司。2009 年，该公司通过风险投资将其技术推向市场，并更名为 Invincea。Invincea 产品是基于 Windows 的端点解决方案，能够创建围绕 7 大常见针对性应用程序的虚容

器：Web 浏览器；Java；电子邮件；微软 PowerPoint、Excel 和 Word； Adobe Acrobat。另外还有一个管理组件，可以在硬件、虚拟设备、云中运行，它关联威胁情报，并向其他安全解决方案提供反馈，如 Web 代理、IPS 和 SIEM 解决方案。该解决方案在虚容器中运行高风险的应用程序，同时通过系统注册表的更改请求、新的流程执行、系统写入、恶意软件 C&C 通信等检测恶意活动。如果检测到恶意活动，它就不再有效了，因为它与其他系统组件虚拟分离，这个环境可以被销毁。从最终用户的体验来看，该解决方案可以与现有应用程序无缝地协作。2013 年 6 月，Invincea 宣布与戴尔签订了代工（OEM）协议，据此，本产品的定制版本将作为标准商业图像的一部分进行预装，并具有前 12 个月的免费许可。12 个月之后，将会收取许可年费。Invincea 将有这些机器感染数据的独家访问权，包括零日漏洞攻击。

Norman ASA

Norman ASA 创建于 1984 年，是一家挪威 IT 安全公司。2013 年 1 月，该公司分解为两个独立机构：Norman Safeground（专注于中小型企业）和 Norman Shark（专注于企业）。旨在解决针对性威胁的 Norman 产品是 Norman Network Protection (NNP)和 Norman Malware Analyzer G2 (MAG2)。NNP 同时利用特征和轻载沙箱技术，来扫描网络出口点的内联或带外流量。MAG2 是混合沙箱技术，利用传统仿真技术和定制虚拟执行环境来分析恶意代码。根据特定的配置，单个 MAG2 设备上可以运行 20 至 40 个虚拟机。NNP 可以与 MAG2 整合，作为可疑文件的收集代理，该代理需要 MAG2 的额外分析，一旦分析结束，会向 NNP 反馈，帮助进行检测。Norman 还采用了开放的 API 架构，允许整合来自其它厂商的解决方案，向 MAG2 设备提供可疑文件。

Palo Alto Networks

Palo Alto Networks 由 Nir Zuk 创建于 2005 年，最有名的是其下一代防火墙平台，将市场推向应用感知和控制方向。2011 年末，它引入了 Wildfire，作为防火墙的免费插件，自动地向 Palo Alto Networks 提交未知文件进行分析；一旦分析完成，将返回包含完整细节的通知，例如恶意软件如何运作，目标是谁。2012 年 11 月，公司引入一项订阅服务，添加了自动记录和修复功能。在付费模式下，文件将被自动发送到 Palo Alto Networks 云进行虚拟执行，如果认为该文件是恶意的，该公司就会向所有 Wildfire 用户发送自定义特征，以防御新发现的恶意软件。2013 年 6 月初，公司增加了 WF-500 设备，使客户能够在私有、现场云环境中（而不是使用厂商的公共云）运行恶意软件。引擎允许恶意软件在分离环境中执行其有效载荷，同时观察 C&C 通信、异常 URL 和 DNS 模式。

Proofpoint

Proofpoint 成立于 2002 年，并于 2012 年 4 月成功上市，首次公开募股募得 8,000 万美元。该公司的重点是电子邮件安全，具备混合云和现场邮件安全解决方案，提供反垃圾邮件、反恶意软件和其他服务（如基于云的存储和归档信息检索）。除了这些解决方案，Proofpoint 提供了针对性攻击防御服务，这是其通信安全云服务的插件模块。针对性攻击防御（TAP）是基于数据的分析（发件人信息）、基于云的 URL 分析、沙箱技术的整合；能够隔离嵌入邮件的 URL，直到通过云服务确认该 URL 是安全的。该服务还结合了 IP 地址、发件人域名信誉等因素，以检测可疑的电子邮件，这将可能省略厂商的标准反垃圾邮件和恶意软件附件扫描服务。TAP 于 2012 年推出，此后迅速发展，目前拥有 100 多家客户。TAP 运行于云端，但与现场部署和基于云的部署兼容。它也与任何下游电子邮件安全系统兼容。

Sourcefire

Sourcefire 公司（总部设在马里兰州的哥伦比亚）成立于 2001 年，一直是入侵防御市场的一个关键厂商。2011 年，该公司收购了基于云的反病毒公司 Immunet，从而转向了新的方向。其技术为 Sourcefire 高级威胁防御措施（网络、终端、移动设备和虚拟环境）提供了大数据分析架构。这些解决方案提供了对现代威胁的可视性和控制：包括入口点、传播和感染后修复。高级恶意软件防御的部署选项包括内联网络保护（通过 FirePOWER 设备的软件许可插件），专用设备，以及 FireAMP 端点、移动和虚拟保护。Sourcefire 的大数据分析架构充分利用云计算，用 4 个不同引擎来分析文件：

- **单对单特征**使用基于特征的检测引擎，能够通过云来加速特征的创建和发布。
- **通用特征**使用基于特征的检测，能够检测目前多态恶意软件的差异。
- **机器学习**利用大数据分析和真实世界场景，将恶意文件分类、提取特征，并实时共享。
- **高级分析引擎**将前 3 个引擎的情报整合，以确保检测的准确性。

该解决方案允许连续分析、拦截恶意软件、追溯报告、修复；如果一个恶意文件最初被视为“良性”，在未来也可以被重新定义为“恶意”，并可以迅速修复。该解决方案部署于网络和端点，可以通过轨迹分析、设备流关联、威胁信标分析进行修复，这有助于快速确定网络上的哪些设备已经被感染、感染源、恶意文件的轨迹、爆发的可能性。

ThreatTrack Security

虽然 ThreatTrack Security 名称较新，但它在防御各种恶意软件方面有近 20 年的经验。ThreatTrack Security 最初被称为 Sunbelt Software，是 VIPRE AV 的母公司，于 2010 年成为 GFI Software 的安全业务机构，2 013 年 3 月被拆分为一个独立的机构。ThreatTrack Security 建立的目的是为所有企业提供安全产品。除了数以百万计地部署于客户和企业市场的传统反病毒产品，ThreatTrack 提供了一个恶意软件分析工具，称为 ThreatAnalyzer。ThreatAnalyzer 最初用于解构 VIPRE AV 发现的恶意软件。ThreatAnalyzer 使安全分析人员通过自动化的沙箱环境运行可疑文件。它可以确定文件的行为、对系统做出的改变、其产生的网络流量。ThreatAnalyzer 可以进行定制，能够镜像独特的系统配置，从而发现和清除针对性攻击。

Trend Micro

Trend Micro 2012 年报告收入超过 10 亿美元，拥有近 5000 名员工，是全球最大的专业安全厂商之一。最初专注于端点防护，最近几年重点已经转移到云、虚拟环境、针对性攻击。2012 年推出了 Deep Discovery，是该公司最新一代的攻击检测技术。它的目的是检测并缓解网络和企业的高级隐蔽攻击。趋势科技的两大主要产品是：

- **Deep Discovery Inspector** 是一个基于网络的设备系列（4 个物理，2 个虚拟），吞吐能力高达 1Gbps。该设备位于带外，监控网络流量，并通过使用多种检测技术，包括信誉分析、活动关联、以及虚拟分析（自定义沙箱）来识别恶意行为和标志着针对性威胁的通信。Deep Discovery Inspector 可以利用该公司的 Threat Connect 服务，提供威胁特征和修复的其他情报。此外，该解决方案可集成到多个 SIEM 解决方案中。

- **Deep Discovery Advisor** 是一个可选的自动沙箱分析工具，将高级恶意软件检测和威胁情报更新集成到其他趋势科技产品和第三方产品，例如电子邮件/Web 网关和端点解决方案。

  Deep Discovery 是趋势科技自定义防御（Custom Defense）解决方案的重要组成部分。自定义防御旨在整合跨客户信息，以加强攻击检测、沙箱分析和威胁情报共享，从而提高整个企业的防御和自动化攻击响应

水平。

其他厂商

除了上述关键厂商，下文列举了最近引入 STAP 产品、将 STAP 技术嵌入其他安全产品、或因其他原因没有包含于表 1 的厂商（请参阅 2012 年领军厂商的业绩）。

AhnLab

AhnLab 是一家韩国公司，2013 年初，该公司向北美市场推出了其恶意软件防御系统。该解决方案利用基于云的情报来进行特征、行为和动态内容分析。

Cognitive Security（思科）

Cognitive Security 是一家捷克安全厂商，成立于 2010 年，获得了不少于 100 万美元的资金，并于 2013 年 1 月被思科收购（收购金额未披露）。思科发挥自己的优势，通过收购 Cognitive Security 进入了 STAP 市场。Cognitive Security 很大程度上依赖于 NetFlow 的分析、20 世纪 90 年代思科创建的行业标准网络流量分析和监控协议。NetFlow 对网络设备收集的数据包进行统计抽样，以分析各种网络行为和流量模式。Cognitive Security 部署现场 NetFlow 采集器来分析可疑流量模式，以识别网络端点之间的异常通信。这些模式被用于检测高级恶意软件映射资源（试图在网络中横向运动）是否存在。Cognitive 技术用于网络行为异常检测（NBAD），还将流分析功能与人工智能、流量分析、高级异常检测、以及一系列其他高级算法相结合。思科计划继续将 Cognitive 技术作为独立设备和服务向客户供应，最终将该技术与其自身的安全设备和网络设备集成，从而利用思科在交换机和路由器上收集和处理 NetFlow 数据的能力。

Cylance

Cylance 由前迈克菲总裁高管 Stuart McClure 和 Ryan Perme 创建，提供高级取证收集产品，称为 CylanceCOLLECT。此外，PrivateDETECT 是一个免费软件，向当前测试版补充了云端点解决方案。其他利用基于云的大数据分析的产品也在计划中。该公司目前正在从事称为“Presponse”的访问：即渗透测试、威胁评估、事件响应。

Check Point Software

Check Point Software 很早就是网络防火墙市场的领军者，它在 2013 RSA 大会上宣布了其产品 Threat Emulation Software Blade。该解决方案在网关上（通常是防火墙）进行初步扫描，然后向云或专用威胁仿真器发送任何可疑文件，其中文件可以在虚拟沙箱中运行。之后，通过 ThreatCloud 情报服务与所有的客户端共享信息。

Fortinet

2012 年末，该 UTM 厂商将其操作系统更新至 FortiOS 5，并添加了防御针对性威胁的关键功能。On-box 功能包括高级行为分析、仿真、C&C 监控制、紧凑型模式识别语言（CPRL，它基本上允许一个特征应用到多达 50,000 个恶意软件）。此外，公司还提供 FortiGuard 服务，针对运行于云和僵尸网络黑名单数据库中的更高级沙箱。

Mandiant

Mandiant 由 Kevin Mandia 在 2004 年创建于弗吉尼亚州的亚历山德里亚。虽然主要是一个服务机构，Mandiant 已经为客户内部安全操作和事故响应团队开发了专利产品。Mandiant 平台使用基于设备的管理控制台和轻载端点代理，提供威胁信标（IOC）扫描整个企业的高级攻击的迹象。与现有的 SIEM、日志管理、网络安全解决方案双向整合，使 Mandiant 解决方案能够迅速使用这些产品产生的警报，以确定受感染机器并进行修复。为此，Mandiant 目前向 HP ArcSight、Palo Alto Networks 和 FireEye 提供了认证集成。

McAfee（Intel）

2012 年，英特尔子公司收购了名不见经传的虚拟沙箱厂商 ValidEdge，并在 2013 年 RSA 大会上宣布了这一收购。作为其 Comprehensive Malware Protection 架构的一部分，迈克菲将 ValidEdge 的沙箱技术与 GTI、网关反恶意软件、传统反病毒方案进行整合，并通过 ePO 提供态势感知，以协助快速修复。

RSA（EMC）

RSA 于 2006 年被 EMC 收购，它是身份和访问管理、安全和漏洞管理市场的领军者。RSA 的高级威胁管理解决方案建立在 RSA Security Analytics（最主要是 NetWitness Spectrum）和 RSA （ECAT）Enterprise Compromise Assessment Tool 的基础之上。NetWitness Spectrum 分析通过网络的可执行文件。它可以帮助识别可疑文件、确定文件正在试图做什么、文件在网络上什么地方出现过。2012 年 9 月，RSA ECAT 被 Silicium Security 收购，作为端

点组件。它利用无特征行为检测模型揭示复杂的恶意软件。ECAT 和 NetWitness Spectrum 的结合使得企业能够利用端点和基于网络的监控、取证和分析。

Websense

Websense 成立于 1998 年，是目前市场上最悠久的内容和威胁分析公司之一。虽然成熟的产品导致其增长缓慢，该公司 2012 年的收入仍然超过 2.6 亿美元。Websense 最近被 Vista Equity Partners 以近 10 亿美元的价格私人收购，因此成为一家私营公司。除了传统的 Web、信息、DLP 安全网关、以及产品的 SaaS（软件即服务）版本，该公司的 STAP 产品是 ThreatScope 基于云的沙箱和可疑内容分析环境。通过这项服务，Websense 用户将可疑或未知文件类型发送至威胁范围沙箱环境，在模拟的实时 PC 环境中进行分析。对日志中的活动进行分析，并与其他已知威胁情报因素进行关联。与感染和感染后进程有关的分析包括注册表、内存、文件系统和网络通信事件细节。

2012 年领军厂商的业绩

2012 年，FireEye 是 STAP 市场的领军厂商，拥有 38.8%的市场份额；Blue Coat 以 2,890 万美元占 14.3%的市场份额；Damballa 是唯一的其他供应商，至少占 10%的市场份额（10.1%）。趋势科技和 Invincea 杀进了前 5 名。

表 1 提供了 2012 年全球 STAP 市场的收入和份额。

表 1：2012 年厂商 STAP 收入

	收入（百万美元）	份额（%）
FireEye	78.3	38.8
Blue Coat	28.9	14.3
Damballa	20.4	10.1
Trend Micro	11.4	5.6
Invincea	9.8	4.9
Solera	9.5	4.7
Norman	4.5	2.2
ThreatTrack	4.2	2.1
HBGary	3.2	1.6
Sourcefire	2.8	1.4
CounterTack	1.8	0.9
Palo Alto Networks	1.7	0.8
Proofpoint	1.3	0.7
其他	23.8	11.8
总额	201.5	100

来源：IDC，2013 年 7 月

未来展望

预测与假设

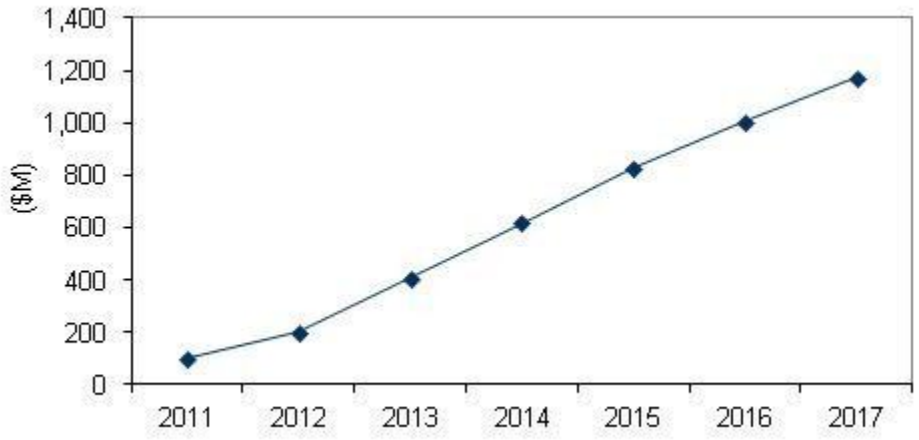
全球 STAP 市场的复合年增长率为 42.2%，到 2017 年将达 12 亿美元。表 2 显示了 IDC 对 2011 年和 2012 年 STAP 市场规模的分析、2013 年至 2017 年的预期收益；而图 1 是 2011 年至 2017 年的图形表示。

表 2：2011 年至 2017 年全球 STAP 收入（百万美元）

	2011	2012	2013	2014	2015	2016	2017	2012–2017 复合年均增长率(%)
STAP	100.6	201.5	406.2	616.9	827.4	1,002.4	1,172.6	42.2

来源：IDC，2013 年 7 月

图 1：2011 年至 2017 年全球 STAP 收入



来源：IDC，2013 年 7 月

假设

表 3 和表 4 分别列出了全球 STAP 市场的前 3 位假设及关键预测。

表 3： 2013 至 2017 年全球 STAP 市场的前 3 位假设

市场力量	IDC 的假设	意义	可能影响当前预测的假设变化	评论
消费化	自带设备(BYOD)趋势继续影响 2012 年的 IT 规划,一些企业举白旗投降,而另一些则加大了安全和控制投入。随着 IT 机构努力跟上移动设备和 Web 服务的创新步伐,个人用户将继续想方设法提高自己的工作效率。一些前瞻性企业正在采取新政策,使用户在选择智能手机和平板电脑方面有更大的自主权(例如,同时采取新的软件来保护这些设备上的企业数据的完整性)。	消费化是 IT 支出的驱动因素,因为个人用户采取新设备和服务的速度比集中式的 IT 机构更快。它甚至创建了间接的消费循环,因为一些企业投资软件来保护企业数据或保护网络。不利的一面是,如果企业在控制员工生产力方面投入过多,会影响其他 IT 项目的资源。	如果企业开始撤销消费化战略,减轻威胁就会变得比较容易,这可能降低市场的增长。	IDC 认为消费化带来的好处大于潜在的问题。

市场力量	IDC 的假设	意义	可能影响当前预测的假设变化	评论
经济	2013 年的全球经济将会不平衡，有些地区比 2012 年的增长势头更强劲，而其他地区很难恢复势头。全球国内生产总值（GDP）将增长 2.5％左右，比 2012 年略有走低，大部分增长来自新兴市场。美国经济依然脆弱，即使企业投资一直保持相对稳定，但是自动减赤在短期内还是降低了政府支出。2013 年，美国 GDP 预计增长 1.9%，低于 2012 年 2.2%的增长率。西欧仍将是全球经济的主要阻力，而欧元区将会连续两年出现 GDP 负增长。日本已采取严厉措施打击通货紧缩，这可能在 2013 年末出现温和的改善，但对中国出口的放缓将继续拖累经济增长。中国是主要的变数，2013 年上半年的增长率弱于预期。政府可能会在下半年制定刺激措施，它有充足的财政储备，但短期政策是不确定的。中国经济增长疲软可能对其他经济体产生负面影响，特别是亚洲。	经济不景气影响了企业和消费者信心、信贷供应和私人投资、以及内部资金。全球经济衰退将导致企业推迟 IT 更新和一些新项目;而上升的经济则相反。一场危机（可能由欧洲事件或美国政治变数触发）会导致类似于 2008 年金融危机级别的影响。	如果全球经济陷入衰退，企业可能会减少支出，削减安全预算。	高级威胁防御是许多大型的战略重点，IDC 认为任何宏观经济软化都不会对市场经济增长产生很大的影响。但是，根据低迷的范围，也会出现影响。

市场力量	IDC 的假设	意义	可能影响当前预测的假设变化	评论
云	云是一种新的计算范式，将塑造未来几十年的IT支出(IDC 称之为“动态 IT”）的逻辑演变。它需要通过互联网虚拟资源的共享访问。IDC 估计，未来几年内，云计算服务指出将继续以两位数的速度增长，逐渐占全部IT支出的较大比重。到 2013 年年底，几乎 10%的软件支出和15%的基础设施支出（服务器和存储)将转移到云。	云服务的主要优势应该是： IT 企业能够将 IT 资源从维护转移至新措施。这反过来又可能带来新的业务收入和竞争力，为中小企业市场和新兴市场的 IT 厂商创造新的机会。这些益处可能会被自相蚕食抵消一些，从而导致缩短的服务、价格模型破坏、硬件商品化；但强劲的经济会使大多数企业将资源转移到新的 IT 发展和应用领域。我们认为采用云是IT支出的驱动因素，尽管存在自相蚕食效应。	如果云技术在这个市场上越来越普遍，它会在一定程度上降低成本和减缓增长。	IDC 预计，短期内会出现云增长，但更普遍的是现场解决方案。

来源：IDC，2013 年 7 月

表 4： 2013 年至 2017 年 STAP 市场的关键预测

市场力量	IDC 的假设	影响	加速器/抑制器/中性	假设的可能性
宏观经济				
经济	2013 年的全球经济将会不平衡，有些地区比 2012 年的增长势头更强劲，而其他地区很难恢复势头。全球国内生产总值（GDP）将增长 2.5％左右，比 2012 年略有走低，大部分增长来自新兴市场。美国经济依然脆弱，即使企业投资一直保持相对稳定，但是自动减赤在短期内还是降低了政府支出。2013 年，美国 GDP 预计增长 1.9%，低于 2012 年 2.2%的增长率。西欧仍将是全球经济的主要阻力，而欧元区将会连续两年出现 GDP 负增长。日本已采取严厉措施打击通货紧缩，这可能在 2013 年末出现温和的改善，但对中国出口的放缓将继续拖累经济增长。中国是主要的变数，2013 年上半年的增长率弱于预期。政府可能会在下半年制定刺激措施，它有充足的财政储备，但短期政策是不确定的。中国经济增长疲软可能对其他经济体产生负面影响，特别是亚洲。	**适中**：经济不景气影响了企业和消费者信心、信贷供应和私人投资、以及内部资金。全球经济衰退将导致企业推迟 IT 更新和一些新项目;而上升的经济则相反。一场危机（可能由欧洲事件或美国政治变数触发）会导致类似于 2008 年金融危机级别的影响。	↔	★★★☆☆

市场力量	IDC 的假设	影响	加速器/抑制器/中性	假设的可能性
财政刺激因素	到 2013 年目前为止，刺激措施也是供不应求。欧洲专注于财政紧缩措施以降低债务水平，而美国面临政府开支的强制“削减”。在中国，针对第一季度低于预期的增长，政府有希望制定新一轮经济刺激措施，但是仍未实现。尽管如此，如果 2013 年下半年 GDP 放缓更加严重，中国仍然拥有充足的储备来制定经济刺激计划。到目前为止，日本实施了最积极的财政政策：政府放松货币政策以应对通货紧缩。	**适中：**金融危机后的刺激和救助措施在成熟经济体中已经减弱；如果欧洲出现另一个低迷，则制定新一轮刺激政策将更加困难。面临着政府支出下降和紧张的政治局势，美国没有心思制定额外的刺激措施。我们认为，GDP 预测已解释了最有可能的政府行为，包括中国 2013 年下半年的任何温和的刺激措施。	↔	★★★★☆

市场力量	IDC 的假设	影响	加速器/抑制器/中性	假设的可能性
危机持续时间/潜在的复发	2012 年，由于债务危机（金融危机的后果）继续威胁欧洲单一货币，欧洲的许多国家进入二次衰退。仍然有许多可能会影响脆弱市场的风险因素；过去 18 个月中 ,新危机的可能性已大幅波动，但从来没有完全消退。即使下降情况可以避免（政治僵局引发的欧元区或美国经济衰退得到瓦解）,金融危机复苏的强劲势头仍无法挽回企业和消费者的信心。中国 2013 年上半年明显的增长放缓使得其更重视下降风险。虽然我们的预测中没有二次全球经济衰退，但诸多因素有可能引发短期内的低迷。	**适中：**全球经济衰退的长期持续导致对 IT 产品和服务需求的衰退，但经济衰退的严重程度使得购买者异常谨慎。如果企业认为风险正在消退，他们可能愿意投资更长期的项目。然而，如果他们认为长期的经济增长疲软取代了危机，则不会这样做。更糟的是，中国、欧洲或美国事件触发的“危机模式”可能使全球经济暴跌到起点。复发的风险一直存在，企业信心在一定程度上仍将受到抑制。	↓	★★★☆☆

市场力量	IDC 的假设	影响	加速器/抑制器/中性	假设的可能性
政策	更大的变数在于政府的不作为而不是作为。美国的政治僵局仍然是一个威胁，已经导致了所谓的强制削减；而欧洲各国政府继续抵制压力，以改变紧缩措施。欧洲的一线希望是：欧债危机已引起政府规定的一些放松，以刺激私营机构，而这可能在长期内推动生产力。在日本，最近的货币放松政策可能在未来 18-24 个月内有助于解决通货紧缩。	**适中。**欧洲政府的规定放松可能直接和间接地驱动 IT 支出。日本还制定了有助于稳定内需和应对通货紧缩影响的政策。美国困于政治冲突僵局，短期内无法制定任何显著的新政策。	↔	★★★★☆

市场力量	IDC 的假设	影响	加速器/抑制器/中性	假设的可能性
全球大趋势				
云	云是一种新的计算范式，将塑造未来几十年的IT支出(IDC 称之为“动态 IT”）的逻辑演变。它需要通过互联网虚拟资源的共享访问。IDC 估计，未来几年内，云计算服务指出将继续以两位数的速度增长，逐渐占全部IT支出的较大比重。到 2013 年年底，几乎 10%的软件支出和15%的基础设施支出（服务器和存储)将转移到云。	**高：**云服务的主要优势应该是： IT 企业能够将 IT 资源从维护转移至新措施。这反过来又可能带来新的业务收入和竞争力，为中小企业市场和新兴市场的IT 厂商创造新的机会。这些益处可能会被自相蚕食抵消一些，从而导致缩短的服务、价格模型破坏、硬件商品化；但强劲的经济会使大多数企业将资源转移到新的 IT 发展和应用领域。我们认为采用云是 IT 支出的驱动因素，尽管存在自相蚕食效应。	↑	★★★★☆

市场力量	IDC 的假设	影响	加速器/抑制器/中性	假设的可能性
融合	融合是一个出现于各个层面的复杂现象 :电话网络、互联网、通信和 IT 技术、消费者和企业技术，甚至数据中心的存储、路由和处理。在这些领域中，也许最首要的是语音、视频和数据通信的融合。这种融合是一种永久性的现象 ,会在未来 10 年不断发展。其中一项措施是 ,IDC 在 2012 年底记录了 19 亿互联网用户和 30 亿电话网络用户。其重叠将是非常显著的。	**低。**融合将推动新的有竞争力的动力，向用户提供新的应用程序和功能，应变法律和监管制度。这也将推动 ICT 支出的增加。	↑	★★★★☆
消费化	自带设备(BYOD)趋势继续影响 2012 年的 IT 规划 ,一些企业举白旗投降，而另一些则加大了安全和控制投入。随着 IT 机构努力跟上移动设备和 Web 服务的创新步伐，个人用户将继续想方设法提高自己的工作效率。一些前瞻性企业正在采取新政策，使用户在选择智能手机和平板电脑方面有更大的自主权（例如，同时采取新的软件来保护这些设备上的企业数据的完整性）。	**高：**消费化是 IT 支出的驱动因素，因为个人用户采取新设备和服务的速度比集中式的 IT 机构更快。它甚至创建了间接的消费循环，因为一些企业投资软件来保护企业数据或保护网络。不利的一面是，如果企业在控制员工生产力方面投入过多，会影响其他 IT 项目的资源。	↑	★★★★☆

市场力量	IDC 的假设	影响	加速器/抑制器/中性	假设的可能性
软件产业转变	软件业仍在经历重大转变，从基本架构（面向服务的体系架构，SOA）和软件的写入方式（复合应用程序）到软件交付方式（软件即服务）和资助方式（基于广告）。特别是，在 2013 年及未来几年，定价和交付模式的破坏将是显著的。这种转变需要 10 年的时间才能完成，但完成后，会使得软件功能的交付更快更动态。	**低。**新的软件创建和交付模式应增加交付和向 ICT 系统整合新软件功能的能力。即使降低了成本，这应该能增加整体开支。	↔	★★★★☆
数字市场	新的数字市场的影响可见于软件即服务，互联网与企业搜索等功能的整合，“云计算”理念，微软、谷歌和其他厂商的广告收入竞争。数字市场将影响内容交付、商业、数据中心的架构、广告、市场营销、电信和社交。它也可能加速新兴地区（即出现越来越多的网民）ICT 的消费。	**高。**寻找软件即服务模式的快速发展、复合应用程序和直接竞争产品（如社交网络应用平台）的更多发展。另外，寻找新兴地区互联网广告收入的快速增长。	↑	★★★★☆

市场力量	IDC 的假设	影响	加速器/抑制器/中性	假设的可能性
嵌入式计算、物联网	这个术语指的是网络中的客户端设备、最终用户或最终设备的普及。这些其他设备从智能手机、连网娱乐设备到汽车、自动化系统、智能电表、恒温器、医疗电子、工业控制器，更不用说 RFID 标签和传感器。通信客户端设备的普及速度将会是 PC 的 5-10 倍。设备既融合（智能手机具有更多功能）又发散（一次性设备，如 RFID 读取器和特定行业设备）。	**高。**向网络中增加数十亿设备将带动更多企业系统部署、管理和使用这些设备。它也会将大量流量从网络外部中心转移到网络边界内部，这将影响到计算和通信架构。	↑	★★★★☆
绿色 IT	绿色IT是指一系列旨在最大限度地减少电力成本、碳排放、危险废物的技术和做法。绿色 IT 的主要影响是基于低功耗的技术选择、更加注重资产处置、以及厂商选择的变化。根据国家的不同，自愿坚持绿色 IT 原则可以成为法律。寻求 IT 以外领域的可持续性会为IT厂商带来机会。然而，疲弱的经济在短期内使得厂商对绿色 IT 的关注降低，因为厂商无力资助新项目。	**高。**采用绿色 IT 产品和做法应该加大对新 IT 产品和服务的需求。然而，在经济疲软使其，启动新项目，用短期成本获取长期收益是比较困难的。	↔	★★★★☆

市场力量	IDC 的假设	影响	加速器/抑制器/中性	假设的可能性
劳动力供给				
IT 人才	现在，全球 IT 就业人数超过 3,500 万 将继续以 1.3 倍的速度增长。在 IT 行业中，支出以 1.1 倍、设备以超过 2 倍、创造的信息以 5 倍、客户之间的网络交互以 8 倍的速度增长。IDC 认为，这是一个长期的结构性约束。近几年的经济放缓收紧了这一约束。	**低。**像网络安全和外包一样，可用性和人才技术水平对市场产生各种直接影响。可用性可能会影响某些市场或采用率，比如 SOA 的发展；但在一般情况下，还会有其他的、更直接的控制因素。从长远来看，增长缓慢的劳动力资源的优化论证了云计算。	↔	★★★★★
资金				
风险投资	尽管经济的不确定性，过去 12 个月的风险投资相对稳定。目前，资金仍然充足，并于 2012 年成功筹集新一轮资金，这受到成功退出战略的回归趋势的激励。目前，风险投资尚不阻碍创新或 IT 投资。	**高。**ICT 创新（将影响预测）似乎没有资金限制。	↔	★★★☆☆

市场力量	IDC 的假设	影响	加速器/抑制器/中性	假设的可能性
股市	2012 年的股市不稳定，反映了持续的经济不确定性和可见性缺乏。但下半年的激增是一个显著的经济顺风车。考虑到同期不温不火的经济增长状态，2012 年下半年的股市涨幅引发了非理性繁荣和投机的担忧。投资者投注在这样的场景上：全球经济在短期内回稳，长期内回复稳健增长。但是，鉴于去年的结果，经济下降比上行的可能性更大。	**适中。**不断上涨的股票价格增加了企业的信心；价格下跌可以驱动较低的经济预期。	↑	★★☆☆☆

市场力量	IDC 的假设	影响	加速器/抑制器/中性	假设的可能性
市场特点				
硬件	2012 年，对 IT 设备的资本支出相对稳定，尽管一些市场表现差于预期。存储、智能手机和平板电脑的需求趋势持续强劲；而网络投资也一直保持稳定。由于企业信息的下降和平板电脑导致的自相蚕食 ,PC 市场经历了艰难的 2012 年；但 Windows 8 和新型因素将有助于推动 2013 年的稳定。2012 年的服务器销售收入也有所下降，但是由于企业持续投资虚拟化部署，第 4 季度出现了改善趋势。与往常一样，如果企业采取应急计划和裁员，资本支出很容易受到经济前景恶化的影响。	**高。**硬件支出约占总 IT 支出的 40%，推动了软件和服务方面的支出。	↔	★★★★☆

市场力量	IDC 的假设	影响	加速器/抑制器/中性	假设的可能性
软件	在过去两年，软件支出强劲反弹，很大程度上符合 2012 年的预期。有证据表明，软件支出正在成为劳动力成本的替代。在过去 6 个月内，硬件增长逐渐软化，势头再次转移到软件投资上。即使在欧洲，很多国家的软件支出超出了2012年上半年的预期。企业似乎愿意继续进行软件投资，甚至在寻求削减其他领域的投资。	**适中。**软件支出约占总 IT 支出的 20%，可以带动硬件、IT 和服务支出。	↑	★★★★☆
服务	2012 年的服务市场是稳定的，甚至不引人注意；自 2010 年以来硬件和软件部署的缓慢下降导致了服务市场的逐步提高。欧洲政府的紧缩方案包括一些主要 IT 服务合同的中止，然而，也有迹象表明金融服务行业基于项目的支出较为疲软。在另一方面，新兴经济体的需求仍然强劲，预计 2013 年的整体增长仍会稳步提高（假设宏观经济增长不出现大崩溃）。云导致的自相蚕食对整体经济增长的拖累，然而，按历史标准来看，复苏周期依然疲软。	**适中。**IT 服务支出会影响整体解决方案的采用率，以及转移到云计算的比率。IT 服务约占 IT 支出的 40%。	↔	★★★★☆

市场力量	IDC 的假设	影响	加速器/抑制器/中性	假设的可能性
电信	电信业的规模和效用使其未受突如其来的经济波动的影响，或者至少具备显著的惯性。过去 24 个月，由于智能手机的采用和相关移动数据费用，服务供应供商的收入有所回升。移动数据收入将继续推动 2013 年的增长，预计 2013 年整体的电信服务收入将会增加 4%。	**低。**IT 行业已经将电信业支出纳入其内部预测；关键是融合的步伐。移动服务将继续推动移动设备和软件，反之亦然。	↔	★★★★☆

标准：★☆☆☆☆很低；★★☆☆☆低；★★★☆☆适中；★★★★☆高；★★★★★很高

来源：IDC，2013 年 7 月

基本指导

毫无疑问，今天，大多数企业关心的问题是针对性恶意软件和高级威胁。STAP 解决方案的早期采用一直非常快，IDC 预计该市场将继续以更快的速度增长。尽管如此，还有一些需要改进的地方，企业部署之前必须考虑一些因素。

给用户的建议

解决高级威胁并没有什么灵丹妙药。在考虑解决办法时，重要的是要围绕保护数据和关键资产，并限制恢复时间和数据丢失。最安全的做法是假设会发生攻击，并确定如何将损失降到最低。与安全一样，最好的防御是多层次的，而这个市场也没什么不同。最好的解决办法是结合各种技术，如防止恶意软件进入网络，监控横向运动的内部流量、C&C 通信的出站流量、数据泄露，利用强大的取证功能进行迅速修复。然而，结合各种技术并进行部署将是非常昂贵的，所以对现有的基础设施进行彻底评估是必要的，以确定哪些技术最有效地保护资源和限制信息泄露。

企业不能够将 STAP 作为目前部署的安全技术的直接替代。相反，应将 STAP 视为分层安全方法的演变，或“皮带与吊带式 2.0”。目前的 STAP 缺乏 IPS、防火墙、Web/电子邮件网关和端点保护套件的许多基本功能；这些产品仍然在 IT 安全方面发挥着重要作用，并不能用 STAP 网关或端点软件解决方案替代。鉴于合规性理由（或好或坏），许多传统的安全措施将继续强制部署。然而，STAP 可以在短期和中期内帮助减少感染率和安全事故。

给厂商的建议

如前所述，充分解决当今高级威胁的部署方案并非一个简单的任务。目前的解决方案仍有许多限制需要加以解决，例如有限的环境支持、网络之外的远程和移动用户、缺乏自动化、可扩展性。此外，攻击者已经开发了能够识别虚拟环境的恶意软件，可以采用先进的休眠技术和其他功能来应对 STAP 产品。能够提供上述问题的解决方案、显示出强劲伙伴关系的厂商将会获得最佳优势。如果只考虑当今解决方案的复杂性和资源密集性，这些技术仍然是企业关注的主要问题。然而，这些问题影响到所有企业，考虑到 SMB（中小型企业）市场范围，有能力打造更轻载、成本更低、更自动化的解决方案的厂商会获得巨大的优势。较小的厂商将需要继续创新，以避免更大的终端到终端解决方案厂商用其现有产品的集成功能主导市场（这已经发生了）。

因为客户群将越来越多地要求在传统方案基础上增加 STAP 技术，没有开发自己的 STAP 技术的现有安全厂商应该与具有互补产品的创业公司合作、或与较小的厂商进行 OEM 合作。随着整体市场更趋向动态、无特征攻击检测技术，无视 STAP 功能、不投资于合作伙伴或内部开发的厂商将被抛在后面。

与此同时，所谓的“最好”的 STAP 厂商必须为其技术的最终“功能化”做准备；尖端的、单一用途的安全产品在市场上的活跃期有限。历史表明，独立的解决方案，例如反间谍软件、VPN、加密和 DLP，最终会被纳入多功能产品或解决方案，这是因为最终用户被迫合并支出和减少费用。由于规模较大的竞争对手能够提供同类产品，使用 STAP 创业公司必须准备存活于更大的安全生态系统，或接受被收购等命运。

更多信息

相关研究

- Worldwide Security 2013 Top 10 Predictions (IDC #239424, February 2013)
- Cisco Gets Cognitive for, and About, Advanced Threat Protection (IDC#lcUS23944713, February 2013)
- Worldwide IT Security Products 2012–2016 Forecast and 2011 Vendor Shares: Comprehensive Security Product Review (IDC #237934, November 2012)
- Sourcefire Not Sitting Pat — Expands Advanced Malware Solution (IDClcUS23787712, November 2012)

方法论

本 IDC 市场规模和预测以套装软件和设备收入的方式呈现。IDC 使用术语“套装软件”来区分现成商用软件和定制软件；并不意味着该软件必须薄膜包装或通过物理媒介提供。套装软件是任何类型的现成商用程序或代码集，可用于出售、出租、租赁或服务。套装软件收入通常包括初始和持续使用授权许可费用。作为许可合同的一部分，这些费用可能包括与许可费用结构密不可分的产品支持和/或其他服务访问，或者这种支持可以单独定价。升级可以包括在持续授权许可费用中，也可以单独定价。IDC 将上述这些算作套装软件收入。设备被定义为硬件、操作环境、应用软件的组合，并形成单独的产品。

套装软件收入不包括独立于（或分拆于）授权许可的培训、咨询和系统集成费用，但包括包含在服务（通过不同的服务定价方案提供软件功能）中的产品隐含价值。总产品收入进一步分配给市场、地理区域以及运行环境。

市场预测和分析方法结合了来自 5 个不同但相互关联的来源的信息，如下所示：

- **报告/观察到的趋势和金融活动。**本研究结合了 2012 年到 2013 年 4 月底的报道/观察到的趋势和金融活动，包括在北美证券交易所交易的上市公司的报告收入数据（在几乎所有情况下 CY 1Q12-4Q12）。
- **IDC 的软件统计采访。**IDC 采访了所有重要的市场参与者，以确定产品收入、收入统计资料、定价以及其他相关信息。
- **产品简报，新闻稿及其他公开资料。**世界各地的 IDC 的软件分析员每年与数百个软件厂商召开会议。这些简报提供了一个机会来审

查当前和未来的业务和产品策略、收入、出货、客户群、目标市场、其他重点产品和有竞争力的信息。

- **厂商财务报表及相关申报文件。**虽然很多软件厂商为私人所有，并限制财务信息的披露，但是上市公司的信息为评估私营公司非正规市场预期提供了基准。IDC 还通过深入分析关系创建了与私营公司有关的详细信息，并具备一个庞大的 IT 行业财务及企业的资料库。我们还了解全球 1000 多家厂商的详细产品收入。
- **IDC 需求方研究。**这包括与软件解决方案用户每年数千个采访，并提供了强大的评估竞争绩效和市场动态。IDC 的用户策略数据库提供可信的行业趋势和发展信息。与科技买家的直接对话微调查结果提供了宝贵的补充。

最后，这项研究中呈现的数据代表 IDC 的最佳估计，其来源包括厂商报告和观察到的活动、我们认为真实的数据建模。

本研究中的数据纳入 IDC 的软件市场预测数据库，并不断更新软家具厂商收入的信息。出于这个原因，当将本研究中的数据与其他研究中的软件收入比较时，读者应注意该研究中的“截止”日期。

摘要

该 IDC 研究调查了特殊威胁分析与防护（STAP）市场。它提供了 2011 年的市场规模、2012 年的厂商份额、2013-2017 年的预测。

“随着攻击变得更有针对性和持续性，恶意软件更加复杂和专业化，防御这些高级威胁的解决方案市场已经出现”，IDC 安全产品项目研究经理 John Grady 说。“IDC 认为，基于特征的技术无法充分应对目前的攻击。结合启发式、行为仿真、沙箱技术的智能解决方案对于防止感染及减少风险是必要的。”

版权声明