cisco

2015
年度安全报告

执行摘要

虽然当今威胁形势瞬息万变，但也有一些方面是始终不变的。

网络攻击者持续不断地改良或开发新方法，以求逃避侦查并隐藏恶意活动。另一方面，防御者（即安全团队）必须持续不断地改进防御措施，以便保护组织和用户免受日趋复杂的攻击活动侵害。

处于这场对抗中心的，正是用户。但是现在，用户似乎已不单纯是攻击的目标，还有可能成为攻击的帮凶。

*思科 2015 年度安全报告*汇集了思科® 安全研究部门和思科内部其他安全专家的研究、见解及预测，对攻击者与防御者之间的拉锯战，以及用户如何逐渐成为安全链中的薄弱环节做出剖析。

网络安全是一个具有广泛性和复杂性的课题，对全球范围的用户、公司、政府和其他实体都有深远的影响。*思科 2015 年度安全报告*的内容分为四个方面。这四个部分以及各部分所讨论的问题初看起来可能毫无联系，但是如果进行更深入的审视，则会发现它们之间的关联。

*思科 2015 年度安全报告*的四个主题：

1. 威胁情报
2. 思科安全功能基准研究
3. 地缘政治趋势和行业趋势
4. 改变看待网络安全的视角 – 从用户转移到企业高层

1. 威胁情报

此部分概括介绍思科最新的威胁研究，包括有关漏洞攻击包、垃圾邮件、威胁和漏洞，以及恶意广告趋势的最新信息。此部分还审视了网络攻击者开始越来越多地依赖用户帮助其发起攻击的趋势。为了对 2014 年观察到的各种趋势做出分析，思科安全研究部门使用了全球遥感勘测数据集。这份报告中提供的威胁情报是思科全体顶级安全专家的工作结晶。

2. 安全功能基准研究

为了评估在组织中担任安全职务的安全专业人员的安全意识，思科对首席信息安全官 (CISO) 和安全运营 (SecOps) 经理就安全资源和安全规程进行了调查，调查对象来自九个国家/地区不同规模的组织。这次调查的结果仅在*思科 2015 年度安全报告中*提供。

3. 地缘政治趋势和行业趋势

此部分包含由思科安全专家、地缘政治专家和政策专家发现的现有和新兴地缘政治趋势，需要组织（尤其是跨国公司）予以关注。此部分的焦点是：网络犯罪如何在监管力度薄弱的地区疯狂肆虐。其他内容还包括全球各地有关数据主权、数据本地化、加密和数据兼容性等问题的最新发展。

4. 改变看待网络安全的视角 – 从用户转移到企业高层

思科安全专家建议，如果组织希望真正实现安全性，就应立即采用不同以往的方式思考网络安全方法。所应采用的战略包括：采用更加完善的安全控制措施来抵御攻击前、攻击中和攻击后的所有威胁；确保安全问题成为公司董事级人员关注的话题；以及实施思科安全宣言。思科安全宣言是一套安全准则，可以帮助组织获得更加动态的安全方法，而且拥有比网络攻击者更高的适应能力和创新水平。

*思科 2015 年度安全报告*中各个安全主题之间的联系在于：攻击者已经变得更擅长利用安全漏洞来藏匿和隐蔽他们的恶意行为。用户和安全团队都与安全问题息息相关。虽然许多防御者自认为其安全流程已实现优化，而且其安全工具十分有效。但实际上，他们的安全就绪程度很有可能仍待提高。同时，地缘政治形势（从立法到安全威胁）的变化可能会直接影响到企业运营以及组织的安全措施。鉴于以上所有考虑事项，所有规模的组织现在都必须了解到：安全是每个人的问题，侵害不可避免，现在是采用新安全方法的时候了！

关键发现

以下为思科 2015 年度安全报告*的关键发现*。

攻击者已经变得更擅长利用安全漏洞来藏匿和隐蔽他们的恶意行为。

- 2014 年，有 1% 的高危常见漏洞和攻击 (CVE) 警报被频繁利用。也就是说，企业必须优先考虑并迅速修补这 1% 的漏洞。但要解决这些漏洞，只有领先的安全技术还不够，还必须拥有卓越的流程。
- 自 2013 年 Blackhole 漏洞攻击包退出后，尚无其他漏洞攻击包取得类似成功。但这可能是漏洞攻击包作者不再像以前那样觊觎榜首地位所致。
- Java 漏洞数下降了 34%，原因是 Java 的安全性得到了提升，以及网络攻击者转而拥抱其他新的攻击媒介。
- Flash 恶意软件现在能够与 JavaScript 交互，以帮助掩盖恶意活动，使其更难被检测和分析。
- 从 2014 年 1 月至 2014 年 11 月，垃圾邮件的数量增加了 250%。
- Snowshoe 垃圾邮件攻击方式（从一大批 IP 地址发送小批量的垃圾邮件，以规避检测）是一种新兴的威胁。

用户和 IT 团队在无意之中已成为安全问题的一部分。

- 网络攻击者依赖于用户安装恶意软件或帮助其利用安全漏洞。
- Heartbleed 高危安全漏洞使得 OpenSSL 处于不设防状态。然而，却有 56% 的 OpenSSL 版本超过 50 个月未更新，因而仍十分脆弱。
- 用户在使用互联网时的粗心行为加上网络攻击者富有针对性的恶意活动，使得许多行业极易遭遇网络恶意软件侵扰。据思科安全研究部门称，2014 年，制药和化工行业上升为遭遇网络恶意软件风险最高的行业。
- 恶意软件制作者开始将网络浏览器的加载项用作分发恶意软件和不必要应用的媒介。事实证明，这种散播恶意软件的方法卓有成效，原因是许多用户不假思索地信任加载项，或简单地将它们看作是良性的。

***思科安全功能基准研究*报告显示企业对自身安全状况的看法存在分歧。**

- 59% 的首席信息安全官认为其安全流程是最优的，相比之下，只有 46% 的安全运营经理持此看法。
- 约 75% 的首席信息安全官认为其安全工具非常或极为有效，其余 25% 认为安全工具效果有限。
- 在拥有先进安全措施的企业受访者中，91% 的受访者极为赞同企业高管将安全摆在高优先级位置的做法。
- 但使用标准工具，如修补程序和配置，来帮助阻止安全漏洞的受访者不足 50%。
- 大中型组织的安全状况可能优于本次调研的其他规模的组织。

目录

执行摘要 2

关键发现 4

攻击者对防御者：旷日持久的拉锯战 6

1. 威胁情报 7

网络漏洞：对漏洞攻击包制作者来说，保持头把交椅可能并不是好事 7

威胁和漏洞：使用 Java 作为攻击媒介的案例有所减少 8

揭秘漏洞考古学：过时软件的危险性，以及为什么修补并不是唯一的解决方案 12

行业风险报告：网络攻击者有针对性的攻击和用户的粗心行为对处于高风险行业中的公司构成了极大的威胁 13

垃圾邮件最新动态：垃圾邮件发送者采取“Snowshoe”（雪鞋）策略 18

来自浏览器加载项的恶意广告：轻微影响每位用户，却能疯狂敛财 21

2. 思科安全功能基准研究 24

思科安全功能：组织的达标情况如何？ 24

3. 地缘政治趋势和行业趋势 38

网络犯罪在监管力度薄弱的地区疯狂肆虐 38

关于数据主权、数据本地化和加密的复杂难题 39

数据隐私的兼容性 40

4. 改变看待网络安全的视角 – 从用户转移到企业高层 42

安全访问：掌握网络中用户的身份、接入时间和接入方式 42

网络安全的未来取决于企业高层今日的参与 44

思科安全宣言：实现现实世界安全的基本准则 45

关于思科 46

附录 47

尾注 52

攻击者对防御者：旷日持久的拉锯战

安全专业人员与网络攻击者之间正在进行一场拉锯战，双方都希望以智取胜。

在安全性方面，组织似乎都开始采用更完善的工具来阻止各种攻击并减轻攻击的影响，以求取得更好的效果。他们已经认识到稳固的安全保护对开展业务必不可少，而且对其安全流程的优化状态充满自信。技术供应商也更注重寻找和修复其产品中的漏洞，以减少犯罪分子利用漏洞发动攻击的机会。

但与此同时，网络攻击者也变得越来越狡猾。他们不仅在攻击方式上花样翻新，而且千方百计地设法逃避检测：

- 他们每时每刻都在改变战术和工具，有的在遭到拦截之前就从网络上消失，有的迅速变换手段以图成功入侵。
- 他们利用成百上千的 IP 地址精心策划垃圾邮件攻击，企图绕过基于 IP 的反垃圾邮件产品的检测。
- 他们还设计出寄身于用户信赖或认为无害的工具上的恶意软件，此类恶意软件会永久感染用户设备，并隐藏在不易察觉之处。
- 如果供应商修复了某产品的漏洞，他们会在其他产品中寻找新的弱点。
- 他们会设法在作为目标的组织内隐藏或伪装身份，有时甚至不惜花费数周甚至数月时间，只为在基础设施和用户数据库内制造多个立足点。他们会耐心等待一切准备妥当后才开始进行其核心活动。

据新的*思科安全功能基准研究*（参见第 24 页）显示，安全专业人员对这场较量持乐观态度，称他们已准备充分，能够成功抵御网络攻击者。但是，网络攻击者窃取信息、诈骗金钱，或出于政治目的破坏网络的现象仍屡见不鲜。最终，安全攻防只是一场数字游戏：面对数十亿封垃圾邮件，即使组织成功拦截了其中的 99.99%，但仍会有漏网之鱼。没有任何方法能确保 100% 有效。

一旦此类邮件或攻击成功触及到用户，这些用户就会成为网络中的薄弱点。如今的企业更善于借助解决方案来拦截网络攻击、恶意软件和垃圾邮件，因此恶意攻击者可能会转而采取诱骗用户上当的策略，例如向用户发送虚假的密码重置请求。

用户逐渐成为安全链中最薄弱的环节，企业在实施安全技术和安全策略时需要作出选择：随着开发人员努力使应用和软件更加直观、更加易用，组织是否会敞开可被网络攻击者利用的新漏洞？ 企业是应该假定用户不可信任或难以驯化，而绕过用户直接实施影响用户工作方式的更严格的安全控制措施？ 还是应该花时间教导用户为何要实施安全控制措施，并明确解释用户如何在帮助组织打造支持业务的动态安全环境方面扮演着至关重要的角色？

思科安全宣言（参见第 45 页）建议选择后者。技术解决方案很少能让用户作为积极的参与者来承担安全责任， 反而会迫使用户不得不处处使用妨碍其日常工作的安全工具。这就为企业留下了安全隐患。安全不再是网络*是否*会遭到入侵的问题。所有网络都*必会*在某个时刻遭到入侵。问题在于，组织到时应怎么办？ 如果安全人员认识到网络必会遭到入侵，他们是否会采取不同的安全策略？

*思科 2015 年度安全报告*展示了思科安全研究团队的最新研究成果。思科安全研究团队审视了安全行业在帮助组织和用户抵御攻击方面所取得的进步，以及网络攻击者试图攻破这些防线所采用的技术和策略。本报告还着重讲述了*思科安全功能基准研究*的主要研究成果。该研究对企业的安全状况以及企业对自身的攻击抵御能力的看法进行了考查。此外，本报告还探讨了地缘政治趋势、数据本地化的全球发展、更完善的安全访问控制措施的价值、以基于角色的访问为基础的分段，以及将网络安全提升为董事会议题的重要性。

1. 威胁情报

思科安全研究团队以全球遥感勘测数据集为基础，总结并分析出本报告中提出的安全见解。思科安全专家持续研究并分析恶意软件流量等已发现的威胁，可以洞察未来可能发生的网络犯罪行为，并协助检测威胁。

网络漏洞：对漏洞攻击包制作者来说，保持头把交椅可能并不是好事

在商业领域，公司都全力以赴地力争成为行业领导者。不过对于从事所谓“影子经济”的漏洞攻击包制作者来说，却不是这样。思科安全研究部门指出，在漏洞攻击包排行榜保持第四或第五的位置，成功的可能性更大。

*思科 2014 年中安全报告*中提到，自 2013 年年底开始，漏洞攻击包领域便没有明确的领导者。[1]当时，政府当局逮捕了涉嫌制作和分发 Blackhole（一款使用广泛且维护良好的高效漏洞攻击包）的黑客 Paunch。思科安全研究部门认为，目前之所以没有占绝对主导地位的漏洞攻击包，主要是因为尚未有真正的技术领导者从这场竞争中脱颖而出。另一项明显趋势是：自 Paunch 和 Blackhole 遭到查禁后，更多的漏洞攻击包使用者似乎开始注重寻找和使用具有公认的先进检测逃避能力的攻击包。

思科安全专家称，2014 年观察到的最常“兴风作浪”的漏洞攻击包是 Angler、Sweet Orange 和 Goon。在所有漏洞攻击包中，Angler 是 2014 年最常被检测到的攻击包，而且由于某些未知原因，它在八月下旬活动最为频繁。思科安全研究部门认为，Angler 之所以受到欢迎，是因为其制作者实现了无需下载 Windows 可执行文件就能传播恶意软件。

思科研究人员表示，Angler 之所以值得警惕，是因为该漏洞攻击包利用了 Flash、Java 和 Microsoft Internet Explorer (IE) 乃至 Silverlight 中的漏洞。该攻击包一经触发，就会将恶意软件负载直接写入内存里的某一进程中，如 iexplore.exe，而不是写入磁盘。Angler 传输的负载看起来就像加密数据的二进制对象，因而系统更难识别和阻止它。

有关 Angler 以及攻击者如何利用恶意广告向用户发送漏洞攻击包的更多信息，请参阅思科安全博客文章：“Angling for Silverlight Exploits”（Silverlight 漏洞钓鱼术）。

Sweet Orange 漏洞攻击包也十分活跃；其组件、端口和负载 URL 不断变化，这使得 Sweet Orange 能够保持有效和避开检测。思科安全研究部门认为，这一策略使得 Sweet Orange 成为“最有可能取得成功”的漏洞攻击包。Sweet Orange 会向未安装修补程序的最终用户系统分发一系列恶意软件，并利用 Adobe Flash Player、IE 和 Java 中的漏洞发动攻击。使用 Sweet Orange 的网络攻击者常用的攻击策略是：依靠恶意广告将用户重定向到挂有该漏洞攻击包的网站（包括合法网站）。在该过程中，用户通常会被重定向至少两次。运行过时版本内容管理系统 (CMS)（如 WordPress 和 Joomla）的受害网站也是已知的适合挂载 Sweet Orange 漏洞攻击包的场所。[2]

思科安全研究部门认为 Goon 漏洞攻击包的“成功之处”在于其可靠性，也可能正是这一原因导致其在 2014 年低调、持久地流行；与其他漏洞攻击包相比，它还因“最有组织”而独树一帜。Goon 于 2013 年首次被安全研究人员发现，又称为“Goon/Infinity 漏洞攻击包”。它是一个恶意软件传播框架，能够利用 Windows 和 Mac 平台上的浏览器在 Flash、Java 或 Silverlight 组件方面的薄弱之处生成漏洞。[3]

图 1. 漏洞攻击包发展趋势：2014 年 1 月至 11 月检测到的有效点击数

来源：思科安全研究部门

在 Blackhole 漏洞攻击包被终结后的几个月里，虽然检测到的漏洞攻击包总数减少了 87%，但思科安全研究部门检测到的攻击包数量却在 2014 年夏季出现了反弹（见图 1）。在 8 月份的最后两个星期里，他们发现 Angler 漏洞攻击包领域的攻击包数量出现显著增加。但到 11 月时，已知漏洞攻击包被检测到的总次数再度出现下降，其中，Angler 和 Goon/Infinity 仍最为活跃。2014 年 5 月至 11 月间，检测到的漏洞攻击包数量整体平均减少了 88%。

威胁和漏洞：使用 Java 作为攻击媒介的案例有所减少

近年来，在最普遍和最严重的漏洞排行榜中，Java 不期然地成为主角。但思科安全研究部门称，在网络攻击者搜寻最快速、最简单和最不易被检测到的利用软件漏洞发起攻击的途径中，Java 似乎受到冷落。

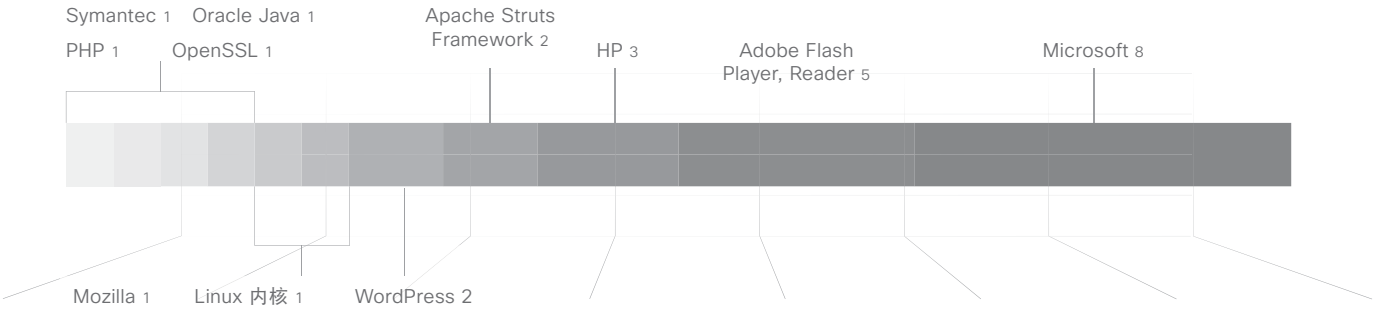
有关企业如何抵御 Fiesta 漏洞攻击包的信息，请阅读思科安全博客文章：“Fiesta Exploit Pack Is No Party for Drive-By Victims”（Fiesta 漏洞包并非万能）。该攻击包通过 Silverlight 之类的攻击媒介和利用动态 DNS 域 (DDNS) 作为攻击登录页面来传播恶意软件。

Nuclear 漏洞攻击包能够评估用户系统以确定薄弱之处并传输相应的恶意软件类型，有关该攻击包及其能力的信息，请参阅思科安全博客文章：“Evolution of the Nuclear Exploit Kit”（Nuclear 漏洞攻击包的进化）。

从 2014 年 1 月 1 日起至 2014 年 11 月 30 日止，在供应商和产品相关漏洞警报排行榜的前 25 个席位中，Java 只占一席（参见第 10 页上的表 1 - 通用安全漏洞评分系统 [CVSS]）。2013 年，思科安全研究部门跟踪到 54 个危急的新 Java 漏洞；2014 年，这一数量减少为仅 19 个。尽管如此，攻击今天仍然存在的这些陈旧漏洞仍十分盛行和有效，网络攻击者应该不会忽视这一点。

美国国家漏洞数据库 (NVD) 的数据也反映了这一下降趋势：2013 年，NVD 报告的 Java 漏洞数为 309 个，而 2014 年，新的 Java 漏洞数为 253 个。（思科安全研究部门跟踪的是在 CVSS 系统中得分较高的重大漏洞，因此数量较少，而 NVD 包含了所有报告的漏洞。）图 2 概括了 2014 年最主要的供应商和产品漏洞。

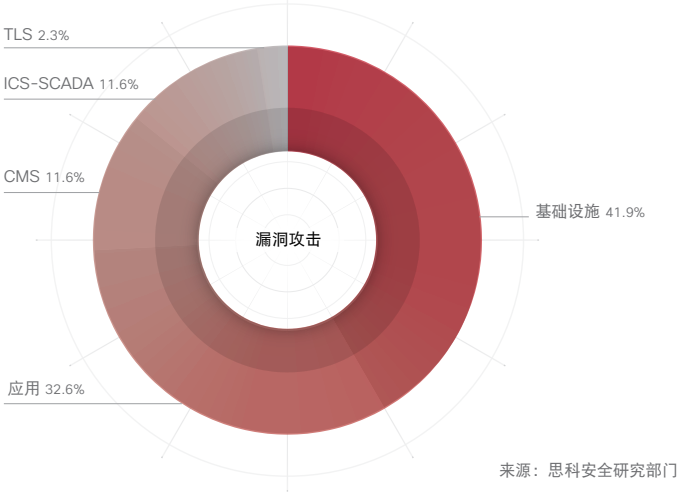
图 2. 按供应商和产品划分的最易受攻击的漏洞



来源：思科安全研究部门

分享报告

图 3. 最易遭受攻击的产品类别



来源：思科安全研究部门

与 Adobe Flash Player、Microsoft IE 等相关的客户端漏洞和以服务器为目标的漏洞（如 Apache Struts Framework 和开源网络框架中的漏洞）在排名中超越了 Java。网络攻击者在攻击期间倾向于通过“占领”网络基础设施来拓展其攻击范围和能力，Apache Struts Framework 受到的攻击越来越多就是一个例证。

Apache Struts Framework 因广受欢迎而成为逻辑上的攻击起点。

图 3 展示了 2014 年经常遭受攻击的产品类别。

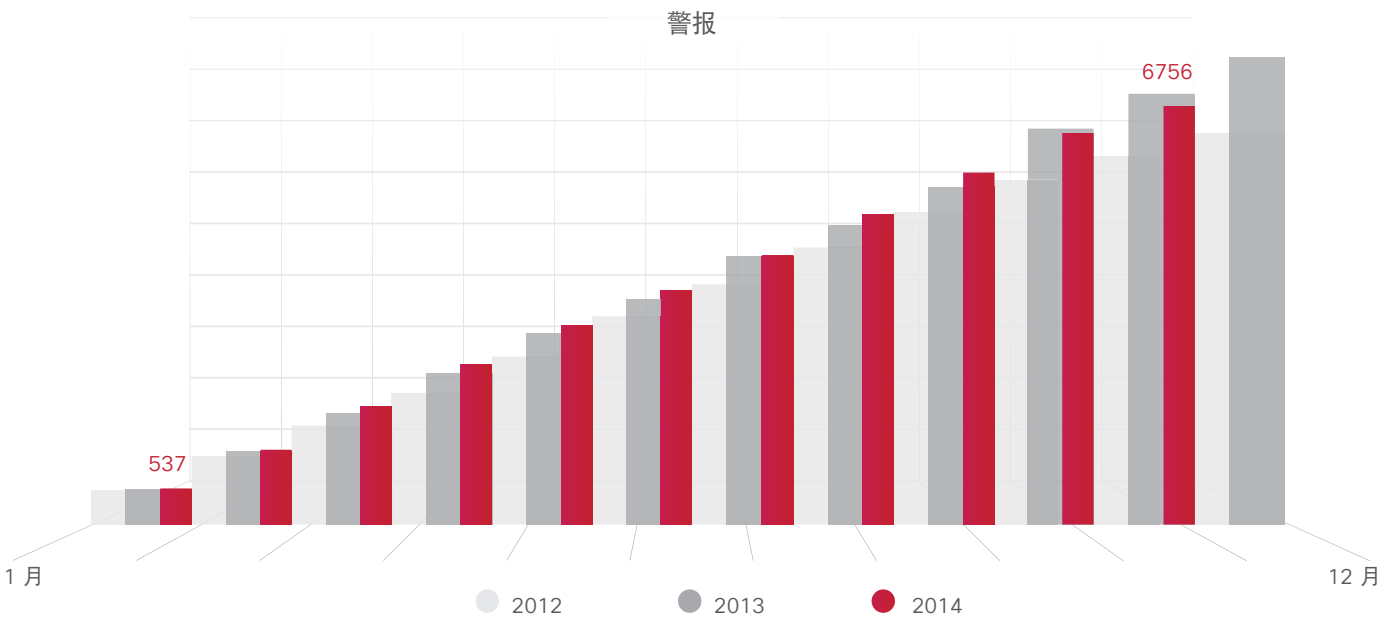
从思科安全研究部门提供的数据来看，2014 年应用和基础设施遭受的攻击最频繁。内容管理系统 (CMS) 也是首选目标；网络攻击者依靠运行过时版本 CMS 的网站来实施攻击

年度累计警报数量出现下降

2014 年报告以及思科安全研究部门编制的累计新增和更新的产品漏洞年度警报总数似乎呈现下降趋势（见图 4）。截至 2014 年 11 月，警报总数较 2013 年下降了 1.8 个百分点。这一比例虽小，但却是近年来警报数量首次较前一年出现下降。

出现下降最可能的原因是供应商越来越重视软件的测试和开发。开发生命周期的完善似乎可以减少犯罪分子能够轻易利用的漏洞的数量。

图 4. 年度累计警报总数



来源：思科安全研究部门

分享报告

表 1. 最常被利用的漏洞

通用安全漏洞评分系统 (CVSS)

IntelliShield ID	标题	紧急	信誉	严重性	基本	临时
33695	OpenSSL TLS/DTLS 心跳信息泄露漏洞				5.0	5.0
35880	GNU Bash 环境变量内容处理任意代码执行漏洞				10.0	7.4
35879	GNU Bash 环境变量函数定义处理任意代码执行漏洞				10.0	7.4
36121	Drupal Core SQL 注入漏洞				7.5	6.2
32718	Adobe Flash Player 远程代码执行漏洞				9.3	7.7
33961	Microsoft Internet Explorer 已删除内存对象代码执行漏洞				9.3	7.7
28462	Oracle Java SE 安全规避任意代码执行漏洞				9.3	7.7
30128	多家供应商产品的 Struts 2 行为：参数处理命令行注入漏洞				10.0	8.3

来源：思科安全研究部门

新警报与更新警报

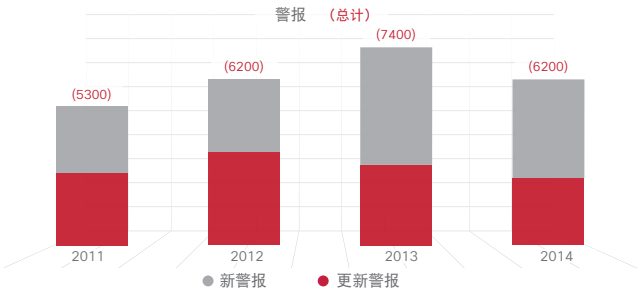
2013 年和 2014 年的新警报数量表明，所报告的新漏洞数仍比往年要多，这意味着供应商、开发人员和安全研究人员在其产品中发现、修复和报告了更多的新漏洞。2014 年的新警报总数和年度总数与 2013 年持平甚至略有下降，如图 5 所示。

图 1 显示了根据通用安全漏洞评分系统 (CVSS)，一些最常被攻击者利用的漏洞。美国国家标准与技术研究所(NIST)的美国国家漏洞数据库 (NVD) 为传达IT漏洞的特点和影响提供了一个框架，并为 CVSS 提供了支持。CVSS 表中的“紧迫性”表示这些漏洞频繁被利用，其分数与表示活跃利用的“临时”分数相对应。通过扫描被利用产品列表中列出的产品，企业可以确定其中的哪些产品正在使用中，需要进行监控和修补。

图 6 展示了 CVSS 得分最高的供应商和产品。思科通过 CVSS 分数证明了概念验证攻击代码的存在；但该代码并不公开可用。

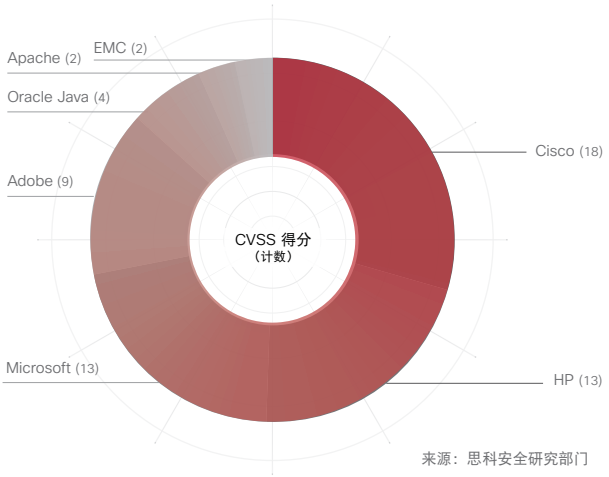
注：表 1 中的漏洞是那些在观测期间显露初步攻击迹象的漏洞。其中的大部分漏洞尚未成为“主流”，这意味着它们还未渗入待售的漏洞攻击包。

图 5. 新警报和更新警报的对比



来源：思科安全研究部门

图 6. CVSS 得分最高的供应商和产品



来源：思科安全研究部门

分享报告

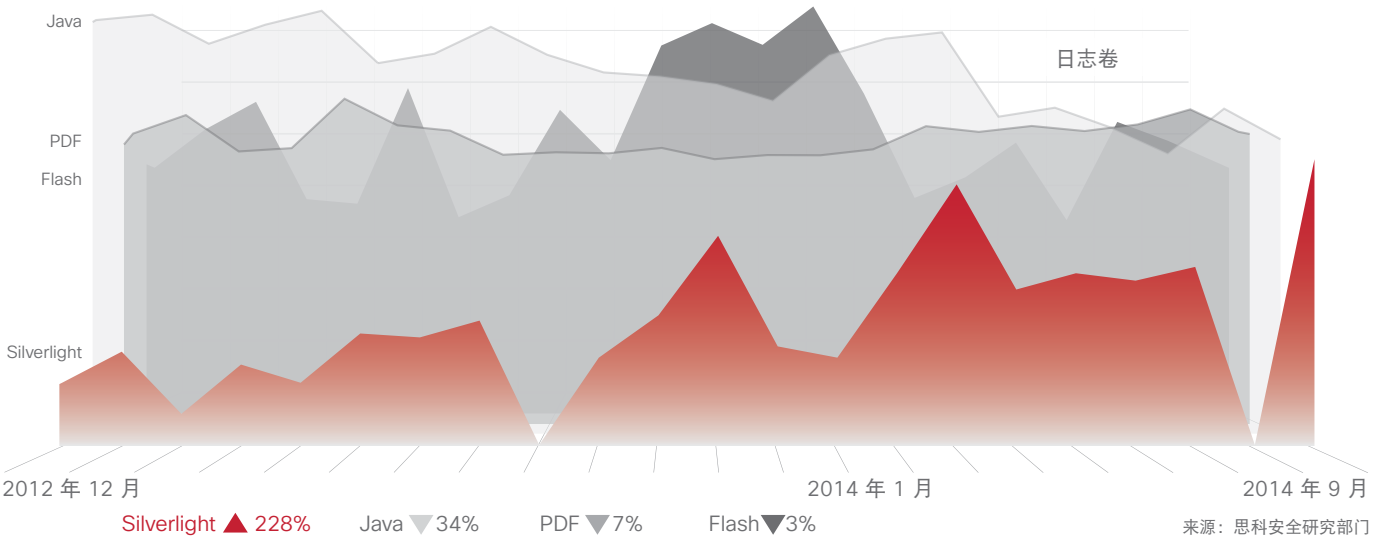
分析：网络攻击者放弃 Java 漏洞的可能原因

思科安全研究部门认为Java漏洞的减少可能与以下事实有关：2014年没有新的 Java 零日漏洞披露，也没有可供网络攻击者利用的Java零日漏洞。现代版本的Java会自动安装修补程序，而更易遭受攻击的旧版本 Java 运行时环境在默认情况下会被浏览器供应商阻止。苹果公司甚至采取了进一步的措施：禁用易受攻击的旧版本Java，并通过自动更新功能来为其安装修补程序。此外，美国 计算机应急准备小组(US-CERT)已于2013年1月提出建议：计算机用户应确保Java安全，或禁用、删除 Java。

Java 的最新版本 Java 8 较以前的版本拥有更强大的控制功能。攻击者想要利用它将会更难，因为它现在需要人工干预，比如代码签名和要求用户启用 Java 的用户对话框。网络罪犯分子业已发现更易利用的目标，并已将注意力转移到非Java媒介上，以提高投资回报。例如，许多用户未定期更新AdobeFlash和PDF阅读器或浏览器，这使得犯罪分子能够发现一系列可利用的新旧漏洞。根据*思科2014年年中安全报告*，包括Microsoft Silverlight漏洞在内的漏洞数量正在增加。[4]

图7显示Java作为首要攻击媒介的地位在一年多的时间里一直处于稳步下降的态势。利用 Flash 发动攻击一直不太规律，且这种情况于2014 年1月达到高峰。利用PDF发动击的情况一直比较稳定，因为有许多恶意行为者似乎对利用PDF附件通过电子邮件发动具有高度针对性的攻击情有独钟。与其他形式的攻击相比，Silverlight型攻击的数量仍然很少，但呈上升趋势（尤其是自8月以来）。

图 7. 攻击媒介数量趋势对比



Flash 与 JavaScript：联手攻击更高效?

2014 年，思科安全研究部门发现攻击者越来越多地开始使用与 JavaScript 交互的 Flash 恶意软件。这一攻击形式由两种不同的文件共同完成：一种是 Flash 文件，另一种是 JavaScript 文件。对于利用两种不同的文件和格式发动的攻击，安全设备将更难识别和阻止，也更难借助逆向工程工具对其展开分析。这种方法可帮助网络攻击者发动更高效的攻击。例如，如果攻击的第一阶段完全在 JavaScript 中进行，那么第二阶段（即负载传输）只能在该 JavaScript 成功执行后才能进行。这样一来，就只有能够运行该恶意文件的用户才能收到负载。

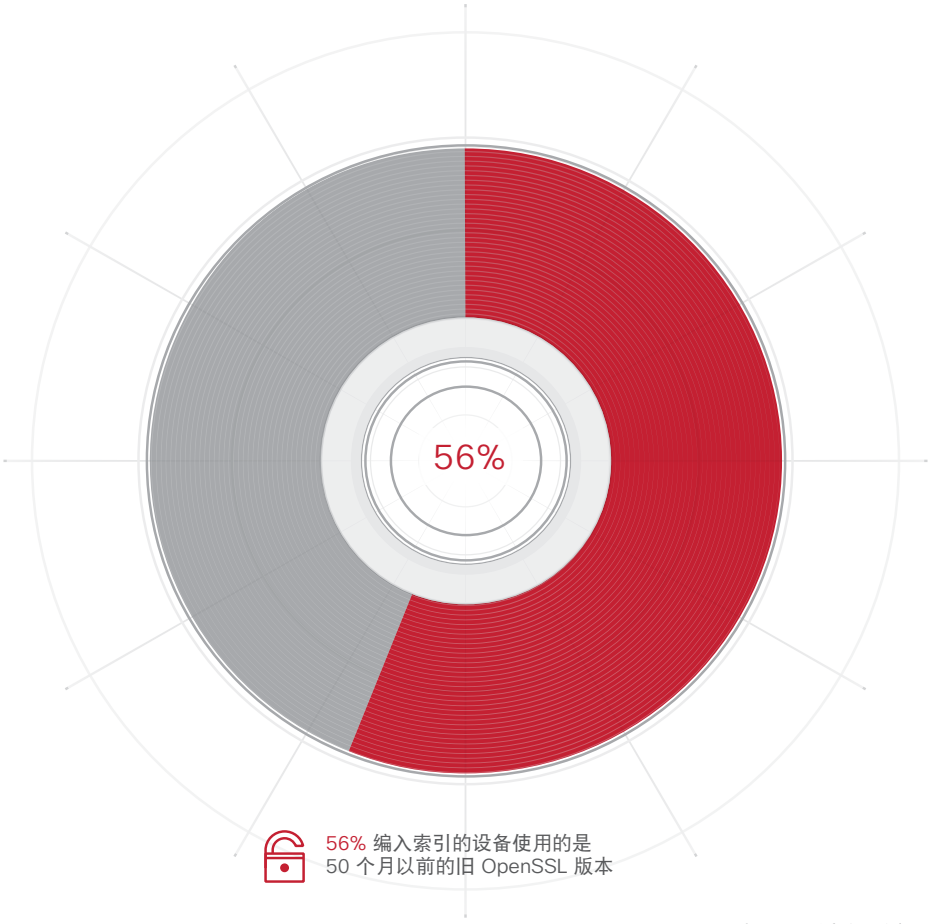
分享报告

揭秘漏洞考古学：过时软件的危险性，以及为什么修补并不是唯一的解决方案

正如关于漏洞的讨论（见第 8 页）解释的那样，网络攻击者在决定其攻击如何以及会在何处取得成功时，会采取最简单的可行路径。他们会选择拥有更多攻击面机会的产品；这些机会通常源自用户使用未经修补或过时的软件。例如，设备修补仍然是一大难题，因为仍有许多系统易受 SSL Poodle 攻击。[5]基于所观测到的趋势，思科安全研究部门认为，包含漏洞的过时版本软件的激增仍将会导致十分严重的安全问题。

思科安全研究部门借助扫描引擎检查了连接到互联网并使用了 OpenSSL 的设备。该小组发现，56% 的受访设备使用的是 50 个月之前的 OpenSSL 版本。这意味着，尽管安全厂商努力引起大家对 Heartbleed[6]（于 2014 年发现的传输层安全 [TLS] 处理漏洞）的注意，且将软件升级到最新的 OpenSSL 版本来避免此类安全漏洞已迫在眉睫，但许多组织却未能做到这一点。图 8 显示了 OpenSSL 版本的滞后程度。

图 8. OpenSSL 版本滞后程度



来源：思科安全研究部门

分享报告

可能的解决方案：自动更新和安装修补程序

更加有效地使用自动更新也许可以解决过时软件的问题。思科安全研究部门检查了在线连接并使用了 Chrome 或 IE 浏览器的设备的数据。该数据显示，64% 的 Chrome 请求源自该浏览器的最新版本。至于 IE 用户，则只有 10% 的请求来自最新版本。

思科安全研究部门认为，Chrome 的自动更新系统或许能更有效地确保尽可能多的用户拥有最新的软件版本。（还有一种可能是 Chrome 用户较 IE 用户更精通技术，因而更倾向于升级浏览器和安装更新。）

结合 Java 漏洞数下降和攻击次数减少这一趋势，该研究结果明确指出，能够自动安装更新的软件在创建更安全的安全框架方面似乎具有某种优势。为了克服手动更新过程最终导致的不可避免的危害，组织不妨暂且接受自动更新所造成的偶然故障和不兼容情况。

行业风险报告：网络攻击者有针对性的攻击和用户的粗心行为对处于高风险行业中的公司构成了极大的威胁

2014 年，制药和化工行业已成为头号易遭受网络恶意软件侵扰的高风险行业。上半年，媒体和出版行业占据着头把交椅，但到 11 月份，其行业地位已退居第二。排名前五位的其它行业分别是制造业、交通运输业、航运、航空。所有这些行业在 2014 年上半年均位列前五名。

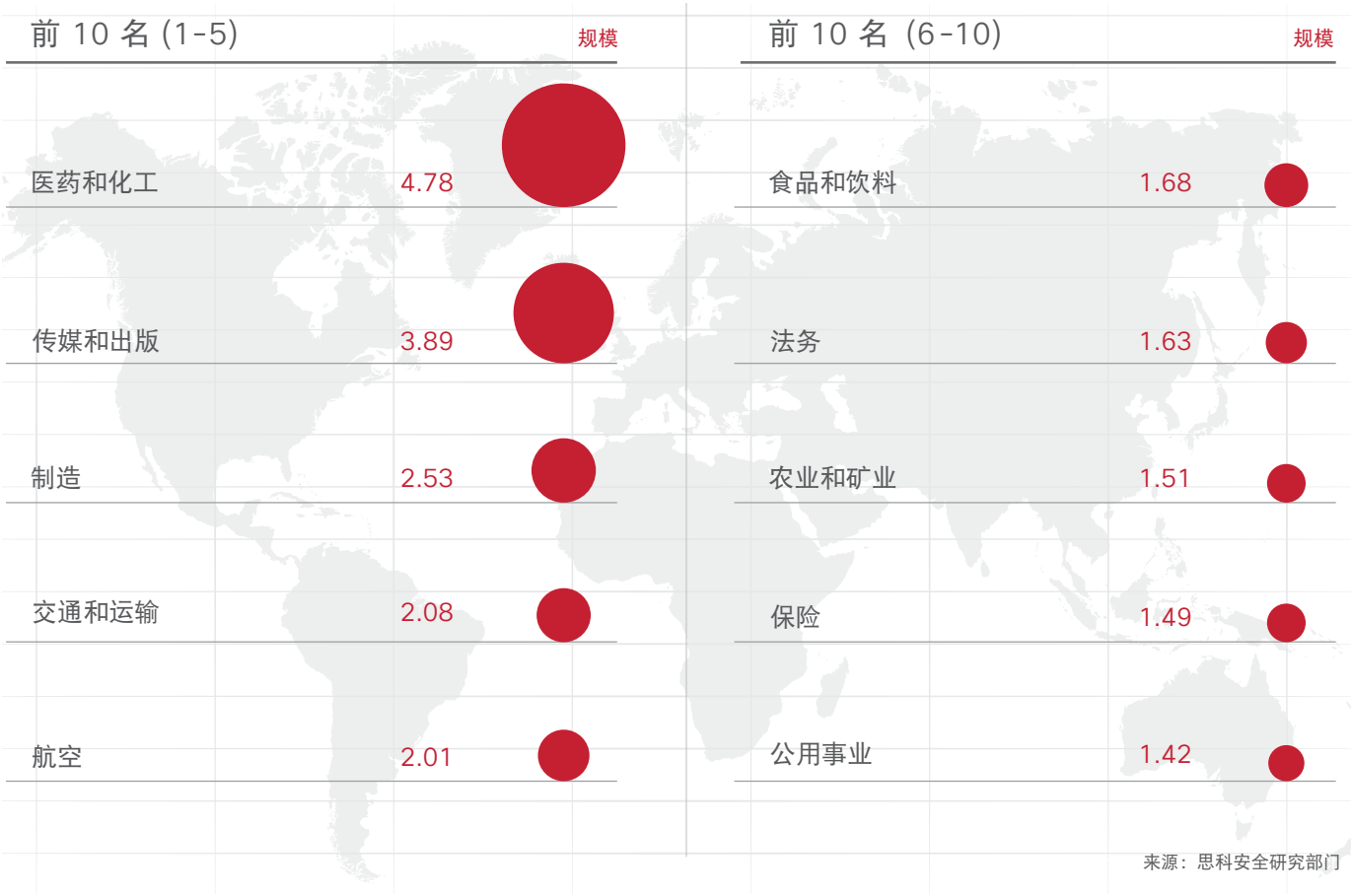
虽然零售行业近期遭受的攻击颇为令人注目，但该行业在这份名单上的排名却并不靠前，原因在于：该排名统计的是恶意软件遭遇率，而非实际的攻击次数。

为确定特定行业的恶意软件遭遇率，思科安全研究人员对使用思科云网络安全的所有企业的遭遇率中间值和特定行业内使用该服务的所有企业的遭遇率中间值进行了比较（图 9）。如果某个行业的遭遇率高于 1%，则表明其面临的网络恶意软件遭遇率的风险高于正常值，如果比率低于 1%，则表明其面临的风险较低。例如，如果一家企业的遭遇率高达 1.7%，则表明其面临的风险高出中间值 70%。相反，如果一家企业的遭遇率为 0.7%，则表明其面临的风险低于中间值 30%。

遭遇与危害

“遭遇”是阻止恶意软件的实例。不同于“危害”，用户在遭遇期间因没有下载二进制文件不会被感染。

图 9. 行业网络恶意软件遭遇率风险，
所有区域（2014 年 1 月 1 日 - 2014 年 11 月 15 日）



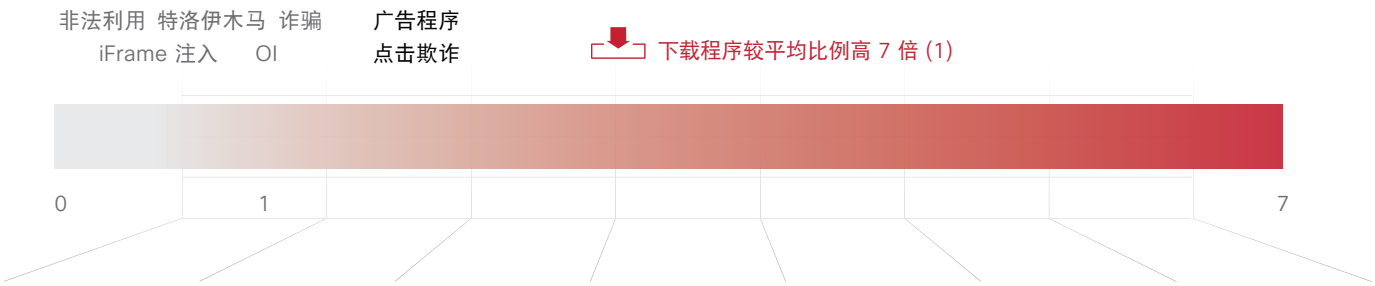
思科安全研究部门审查了八种类型的攻击方式（图 10），以确定导致行业恶意软件遭遇率风险升高的主要原因在于网络攻击者采取有针对性的攻击方法还是人员使用网络的方式。他们发现了一个“完美风暴”- 有针对性的攻击方法和粗心的用户在线行为都会影响该风险级别。

为确定高风险和低风险的行业用户行为之间是否真的存在差别，思科安全研究部门审查了用户在浏览互联网时经常会遇到的四种类型的非针对性攻击方式：广告软件、点击诈骗、诈骗和 iframe 注入。此外，该团队还研究了网络攻击者在有针对性的攻击活动中经常采用的四类更先进的攻击方式：漏洞、特洛伊木马、OI（检测恶意软件）和下载程序。

注：思科安全研究部门将这八种攻击方式归类为启发式桶。

分享报告

图 10. 网络恶意软件攻击方式：四个风险最高和四个风险最低的行业的对比



来源：思科安全研究部门

思科安全研究部门基于思科云网络安全数据取出排名前四位和后四位的最易遭受恶意软件侵扰的行业，然后利用每种攻击类型的事件数生成了排名前四位和后四位的行业的平均遭遇率。图 10 所示的对比结果是以最高平均比率除以最低平均比率得出的。比率为 1 表明最具针对性的群体与最不具针对性的群体之间所观察到的活动模式相同。

该数据显示，最高危行业遭遇先进下载器攻击方式的频率较排名靠后的四个高危行业高七倍。就是否会发生面向高危行业的有针对性的攻击方式而言，这一结果符合人们的预期。

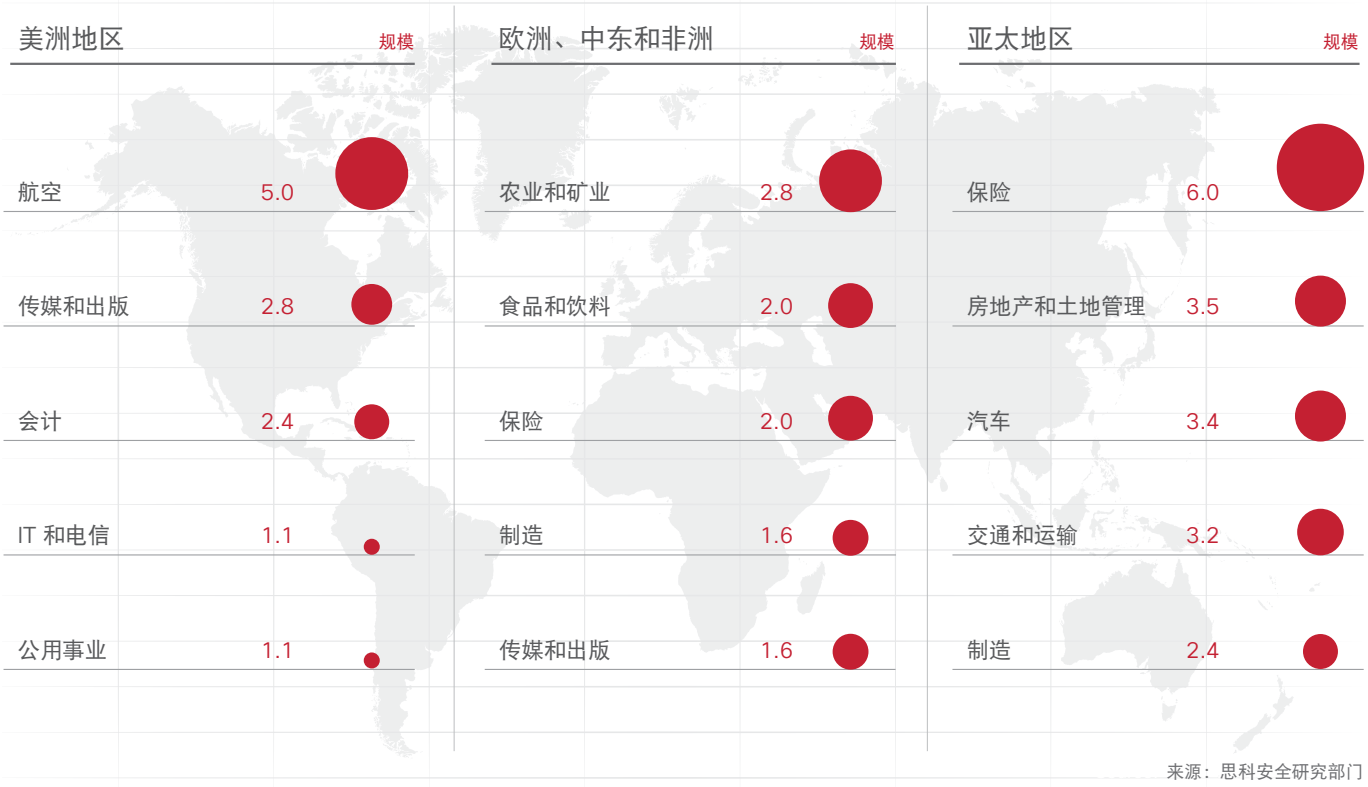
与针对性较少和风险较低的行业相比，针对性较多和风险较高的行业遭遇点击欺诈和广告软件的几率也较高。这表明，与只是被恶意行为者当做目标的情况相比，这种差别可能更为复杂。此外，用户行为也可能与恶意软件遭遇率的增加有关，可能的原因是：用户使用互联网的方式和浏览习惯的差异会导致高风险行业更频繁地遭遇网络恶意软件攻击。此外，在某些行业中鼓励使用新媒体，而且这也是提升竞争力和创新力所必需的，而与其他行业的用户（比如在政府部门，用户使用互联网时可能会受到更多限制，且/或严格受控）相比，这些行业的用户则可能更易遭遇网络恶意软件的攻击。

例如，据思科安全研究报告显示，由于媒体和出版行业的用户通常是对互联网的依赖性很强的用户，他们遭遇网络攻击的风险往往要高于其他行业的用户。

注：2014 年，媒体和出版行业遭遇网络恶意软件攻击的比率远远高于思科安全研究部门之前观测到的正常值（思科安全研究部门自 2008 年即开始编制这一数据）。导致这一数据增长的另一个可能原因是用户在合法网站上遭遇恶意广告的几率增加。

分享报告

图 11. 跨 AMER、APJC 和 EMEA 的最易遭受恶意软件攻击的行业



来源：思科安全研究部门

按地区划分的恶意软件遭遇率

下面是按区域划分的高风险行业的网络恶意软件遭遇率风险数据。这三个区域定义如下：

- 北美洲、中美洲和拉丁美洲 (AMER)
- 亚太地区、中国、日本和印度 (APJC)
- 非洲、欧洲和中东地区 (EMEA)

思科安全研究部门在检视了世界各地风险最高的局部行业（图 11 中所列的行业）后发现：

- 与所有三个区域所观测的 12 个行业相比，在 APJC 地区，保险业用户遭遇恶意软件的几率为平均水平的六倍。（平均基准：1.5）
- 在 AMER 地区，航空业用户遭遇恶意软件的几率为五倍。
- 在 APJC 地区，房地产和土地管理业的用户及汽车行业的用户，遭遇恶意软件的几率为 3.5 倍。
- 在 APJC 地区，交通运输和航运业的用户遭遇恶意软件的几率为 3.25 倍。

思科安全研究部门认为，网络攻击者挑选在 APJC 地区从事汽车、保险、房地产和土地管理、交通运输和航运业相关工作的用户作为攻击目标的原因在于：该地区土地和住房价格疯涨、近期发生过自然灾害，且出口和制造业活动非常频繁。AMER 地区航空业用户遭受攻击的主要目标可能在于：盗窃客户数据、知识产权（包括来自民族国家的攻击）和货运数据。

分享报告

散播恶意软件的攻击方式（按地区划分）

图 12a 到图 12c（按地区划分）显示的是网络攻击者在散播恶意软件时最常使用的技术手段。根据 Cisco Cloud Web Security 数据，这些图表中的发现结果主要基于阻止 Web 恶意软件发生（即遭遇恶意软件）的位置，以及 Web 中的威胁类型。

2014 年间，美洲地区的用户主要遭受的是恶意脚本攻击；这种攻击所占比例远高于排在第二位的 iframe 注入。在亚太地区，网络攻击者过去一年里非常依赖于使用诈骗、恶意脚本和基于网络的漏洞，对所有垂直行业中的用户发动攻击。而在欧洲、中东和非洲地区，基于网络的漏洞攻击尤为普遍。

请参阅思科安全博客文章：“Threat Spotlight: Group 72”（威胁聚焦：72 团），以了解对于网络威胁者团队针对制造业、工业、航空航天、国防和媒体领域拥有高价值知识产权的知名组织发起的攻击活动，思科安全研究部门在帮助甄别和阻击方面所发挥的作用。

有关 72 团实施网络间谍活动所采用的远程管理工具 (RAT) 的详细信息，请参阅博客文章：“Threat Spotlight: Group 72, Opening the ZxShell”（威胁聚焦：72 团，打开 ZxShell）。

图 12a. 美洲地区的攻击方式分布

攻击方式	所占比例
脚本	24.93%
iFrame 注入	17.43%
漏洞	13.63%
OI（检测恶意软件）	10.35%
特洛伊木马	10.06%

来源：思科安全研究部门

图 12b. 亚太地区的攻击方式分布

攻击方式	所占比例
诈骗	25.26%
脚本	25.04%
iFrame 注入	18.68%
OI（检测恶意软件）	9.93%
漏洞	6.72%

来源：思科安全研究部门

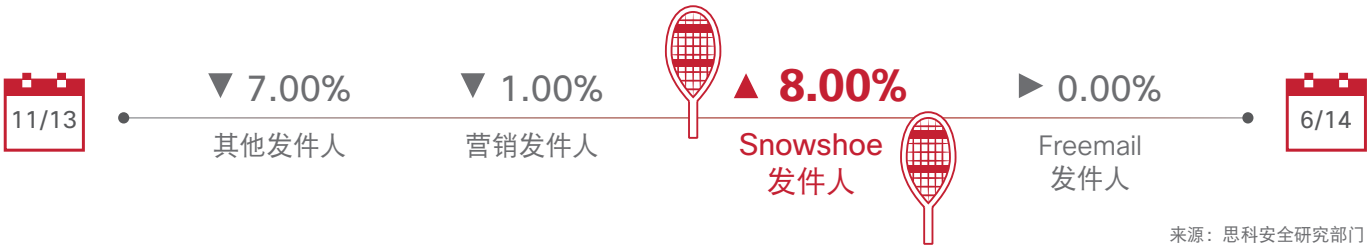
图 12c. 欧洲、中东和非洲地区的攻击方式分布

攻击方式	所占比例
iFrame 注入	51.48%
脚本	15.17%
非法利用	8.64%
诈骗	7.31%
OI（检测恶意软件）	4.16%

来源：思科安全研究部门

分享报告

图 13. 来自 Snowshoe 发送者的垃圾邮件增多



来源：思科安全研究部门

垃圾邮件最新动态：垃圾邮件发送者采取“Snowshoe”（雪鞋）策略

垃圾邮件手段虽已为人所熟知但用户仍深受其害，因而网络钓鱼攻击仍然奏效，常被网络攻击者用作传播恶意软件和窃取凭据的工具。攻击者已意识到，在浏览器和电子邮件层面向用户发动攻击往往比攻陷服务器容易，因此，垃圾邮件发送者会继续翻新花样。

垃圾邮件捕获率超过 99% 的反垃圾邮件系统并不少见。大多数顶级的反垃圾邮件系统的捕获率都能超过 99.9%。在这种环境下，垃圾邮件发送者会想尽办法来尝试逃避垃圾邮件过滤器检测。为确保垃圾邮件抵达目标受众，垃圾邮件发送者越来越多地采用此类策略来逃避基于 IP 的反垃圾邮件信誉技术的检测。

言归正传，说说 Snowshoe 垃圾邮件：雪鞋这个比喻很恰当，因为人们穿着雪鞋可以在厚厚的积雪上行走，而这是因为雪鞋与地面之间的接触面积更大，可以更好地分担人的体重，从而防止穿着者的脚下沉。Snowshoe 垃圾邮件是来路不明的批量邮件，通过大量的 IP 地址发送，而每一 IP 地址只发送少量邮件，因而可以避免垃圾邮件“陷入”某些反垃圾邮件系统之中。图 13 突出显示了 2013 年至 2014 年 Snowshoe 垃圾邮件的增长。

在思科安全研究部门观测到的最近一次 Snowshoe 垃圾邮件攻击活动中，垃圾邮件发送者采用了“闪电战”战术。整个垃圾邮件攻击活动只持续了三个小时，但却一度占据了全球垃圾邮件流量的 10%（图 14）。

有关 Snowshoe 垃圾邮件的更多信息，请参阅思科安全博客文章：“Snowshoe Spam Attack Comes and Goes in a Flurry”（Snowshoe 垃圾邮件攻击：来无影，去无踪）。

思科研究人员检查发现，Snowshoe 垃圾邮件有一些标准特征。举例来说，这些垃圾邮件的主题行存在拼写错误，比如“inovice 2921411.pdf”，且包含一个随机生成的编号。附件通常为 PDF 文件，里面包含用于攻击 Adobe Reader 漏洞的特洛伊木马。

图 14. Snowshoe 垃圾邮件攻击事件

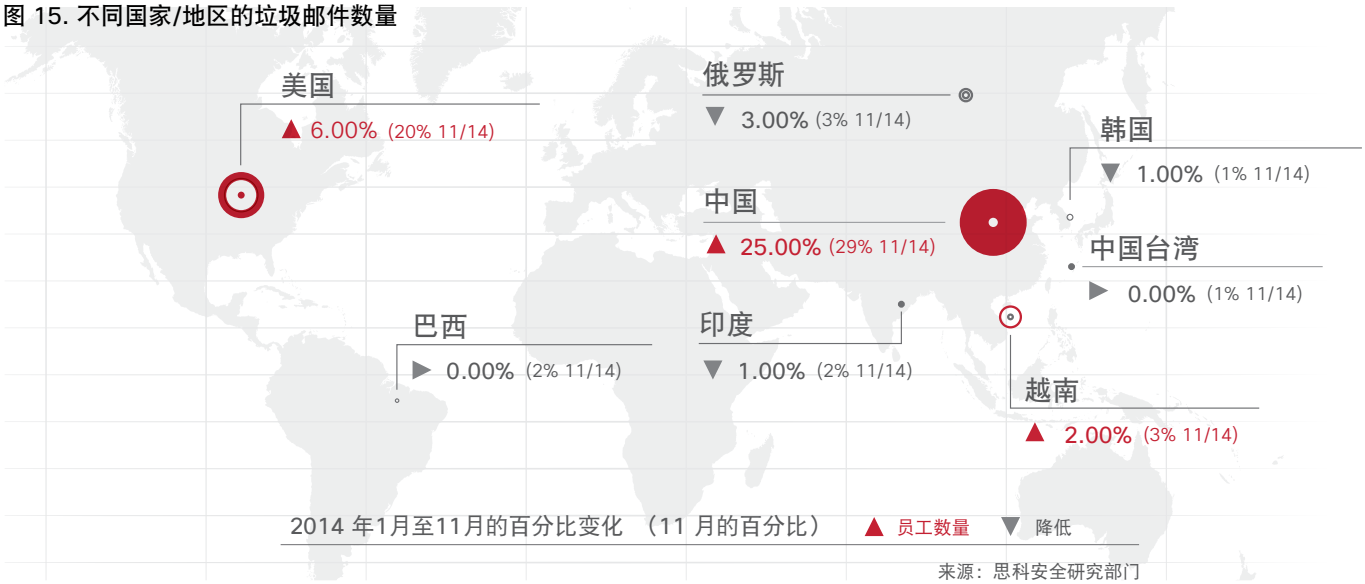
来源：思科安全研究部门

要应对 Snowshoe 垃圾邮件的攻击，安全专业人员不能再简单地依靠基于信誉的解决方案，因为如果攻击来自僵尸网络，相同的邮件可能源自成百上千的网络位置。检查垃圾邮件的其他特征，比如邮件服务器的健康状况，可使检测更加精确。例如，在思科安全研究部门观测的攻击活动中，许多 IP 地址缺少匹配的正向和逆向域名系统 (DNS)，而这通常可视为判定邮件服务器不合法的明显指标。

此外，许多此类 IP 地址缺少 Snowshoe 垃圾邮件攻击活动开始前的电子邮件发送记录，这进一步表明网络攻击者是利用被侵害机器建立了一个基础设施以发动 Snowshoe 垃圾邮件攻击。

分享报告

图 15. 不同国家/地区的垃圾邮件数量



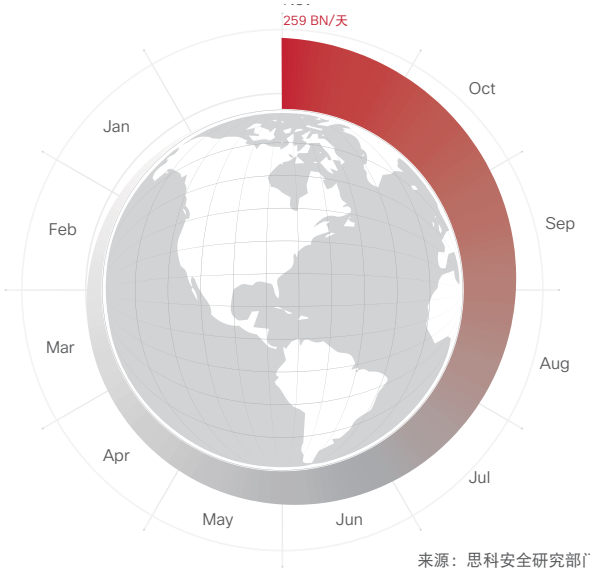
来源：思科安全研究部门

垃圾邮件发送者花样翻新，蒙骗消费者

全球垃圾邮件数量呈上升趋势，这表明垃圾邮件对网络攻击者来说仍是一种获利丰厚的攻击手段（图 16）。网络攻击者一直在不断改进邮件内容，以便让垃圾邮件更能够欺骗收件人点击危险链接。他们通常会使用社交工程策略。

在 2014 年，虽然美国的垃圾邮件数量总体有所减少，但其他国家/地区的垃圾邮件数量有所增加（图 15）。思科安全研究部门指出，这种趋势表明许多恶意攻击者可能正在转移活动重心。其他国家/地区垃圾邮件数量上升也可能表明，其他区域产生的垃圾邮件量正在接近美国，因为美国一直是全球垃圾邮件的最大源头。最终，美国在 2014 年的垃圾邮件数量还是呈上升之势。

图 16. 2014 年全球垃圾邮件数量增加



来源：思科安全研究部门

多年来，网络攻击者将鱼叉式网络钓鱼邮件应用得越发地得心应手，即使是经验丰富的最终用户也很难辨别其真假。此类邮件经过精心设计，以具体个人为目标，通过伪装，看似发自常向用户发送邮件的知名厂商或服务提供商，如送货服务、在线购物网站、音乐和娱乐提供商等。这种邮件带有值得信赖的名称和标志，即使是伪造的，也比传统的兜售药品或手表的垃圾邮件高一个档次。如果邮件恰好包含收件人熟悉的操作请求，比如关于近期订单的通知或快递跟踪编号，用户很可能会上当去点击邮件中包含的链接。

思科安全研究部门近来发现一小批自称发自苹果公司的鱼叉式网络钓鱼邮件，这些邮件声称收件人下载了一款流行的移动 iOS 设备游戏。邮件主题行包含一个随机生成的收据编号，这又是一处看似真实的伪装，因为合法邮件通常会包含这样的编号。邮件中的链接提示收件人如果尚未下载游戏，应登录并更改密码，而该链接会将用户重定向到某个已知的钓鱼网站。

分享报告

垃圾邮件发送者变换邮件形态以逃避检测

当垃圾邮件发送者找到一个能够得手的模式，即能够诱使用户点击垃圾邮件中的链接，或购买假冒产品，他们就会调整邮件，保持邮件的基本结构不变。但邮件会有足够的差异来逃避垃圾邮件过滤器的检测，至少能短期奏效。在表 2 中，思科研究人员统计了在一个采样周期内，垃圾邮件发送者为逃避遭持续遏制而试图改变邮件内容的次数。该表列出了需要思科邮件安全设备 (ESA) 变更规则的威胁。

表 2. 威胁爆发警报：最持久的垃圾邮件和钓鱼威胁

IntelliShield ID	标题	版本	紧迫性	可信性	严重性
24986	Threat Outbreak Alert: Fake FedEx Shipment Notification	95			
31819	Threat Outbreak Alert: Fake Fax Message Delivery Email	88			
30527	Threat Outbreak Alert: Malicious Personal Pictures Attachment	81			
36121	Threat Outbreak Alert: Fake Electronic Payment Canceled	80			
23517	Threat Outbreak Alert: Fake Product Order Email Message	79			
23517	Threat Outbreak Alert: Fake Invoice Statement Attachment	78			
27077	Threat Outbreak Alert: Fake Money Transfer Notification	78			
26690	Threat Outbreak Alert: Fake Bank Payment Transfer Notification	78			

来源：思科安全研究部门

分享报告

来自浏览器加载项的恶意广告：轻微影响每位用户，却能疯狂敛财

近来，思科安全研究部门对一种基于网络的威胁进行了深入分析，这种威胁使用来自网络浏览器加载项的恶意广告作为散播恶意软件和不需要的应用的媒介。该部门发现，这种威胁具有与僵尸网络的行为极为类似的特征。思科安全研究部门通过研究分析 70 家公司中超过 80 万名用户从 2014 年 1 月 1 日至 2014 年 11 月 30 日的活动，测算出这种威胁的总体规模，并确认了其意图和结构。

分析结果表明，此类浏览器插件远比预期的范围广泛，且恶意软件制作者将高度复杂的专业代码与精心策划的商业模式加以结合，以确保其恶意软件能够长期获利。换句话说，完全控制目标主机不是成功获利的必要条件。这导致越来越多的恶意软件故意设计成下述模式：只对受波及的主机产生轻微影响，并且经过优化能够通过大量感染系统而长期获利。

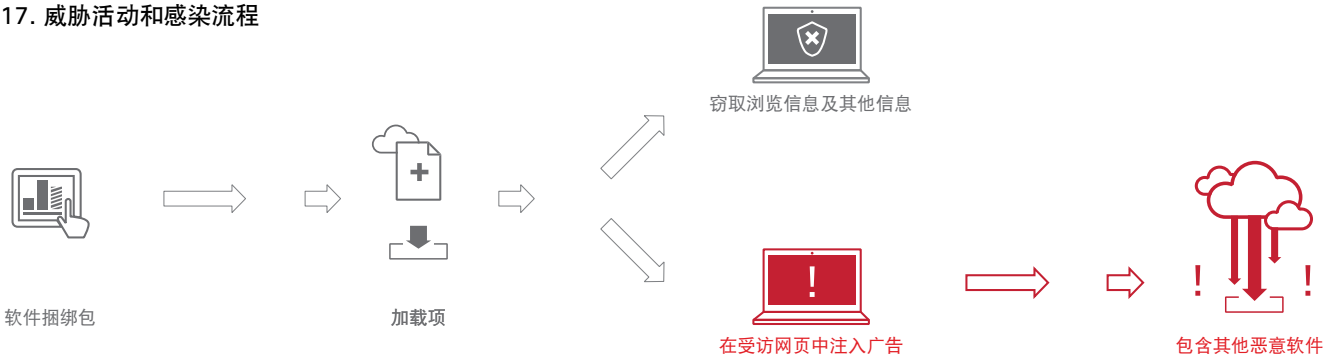
这种方式通过在目标用户设备上安装捆绑软件（通过其他软件包或产品分发的软件，通常不需用户明确同意）的方式使用户感染此类恶意浏览器加载项。用户可能以为从不受信任的来源下载的应用（如 PDF 工具或视频播放器）没有问题，而随意安装此类应用。但这些应用有可能“捆绑”了不需要的软件或恶意的软件。这种散播恶意软件的方式遵循按安装量收费 (PPI) 的获利模式：原始应用中捆绑的软件每被安装一次，发布者就得到相应的付款。

许多用户不假思索地信任加载项，或简单地将其视为良性的，这就为恶意攻击者能通过这种方式成功散播恶意软件创造了条件。这种散播恶意软件的方式减轻了网络攻击者对其他技术（如漏洞攻击包等可能更易被检测到的技术）的依赖。（请参阅第 7 页的“网络漏洞：对漏洞攻击包制作者来说，保持头把交椅可能并不是好事”。）

思科安全研究部门观察到，通过此类浏览器加载项生成的网络流量有具体特征，可藉由以下两个明确定义的模式来加以识别。查询字符串通常包含编码数据，其中含有遭窃信息，如加载项的名称和用户之前访问过的 URL（包括内部网络链接）。

在分析过程中，思科安全研究部门发现了4000多种不同的加载项名称，如 PassShow、Bettersurf、Bettermarkit 和关联 SHA (bee4b83970ffa8346f0e791be92555702154348c14bd8a1048abaf5b3ca049e35167317272539fa0dece3ac1a6010c7a936be8cbf70c09e547e0973ef21718e5)。每次安装可能会使用多个加载项名称，因而要跟踪恶意软件极为困难（图 17）。

图 17. 威胁活动和感染流程



来源：思科安全研究部门

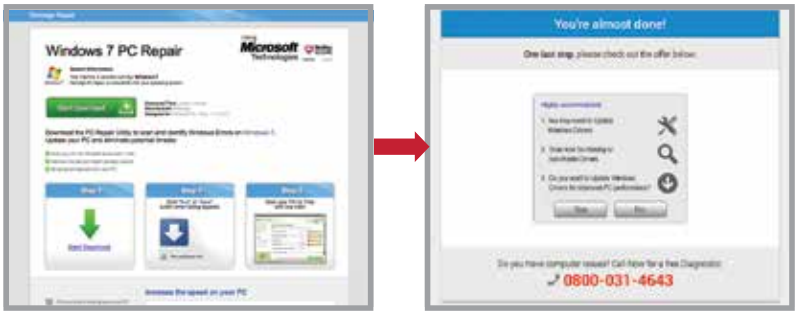
分享报告

恶意软件检测操作系统的类型，然后利用相应的漏洞

思科安全研究人员发现，他们所分析的恶意加载项会根据用户的“指纹”在浏览器上显示某种特定类型的广告。向 Linux 用户注入的广告通常是关于在线游戏网站。安装 Microsoft IE 的用户则被重定向到某些会诱导用户下载软件的广告，这些软件看似合法，实则存在恶意。

Linux

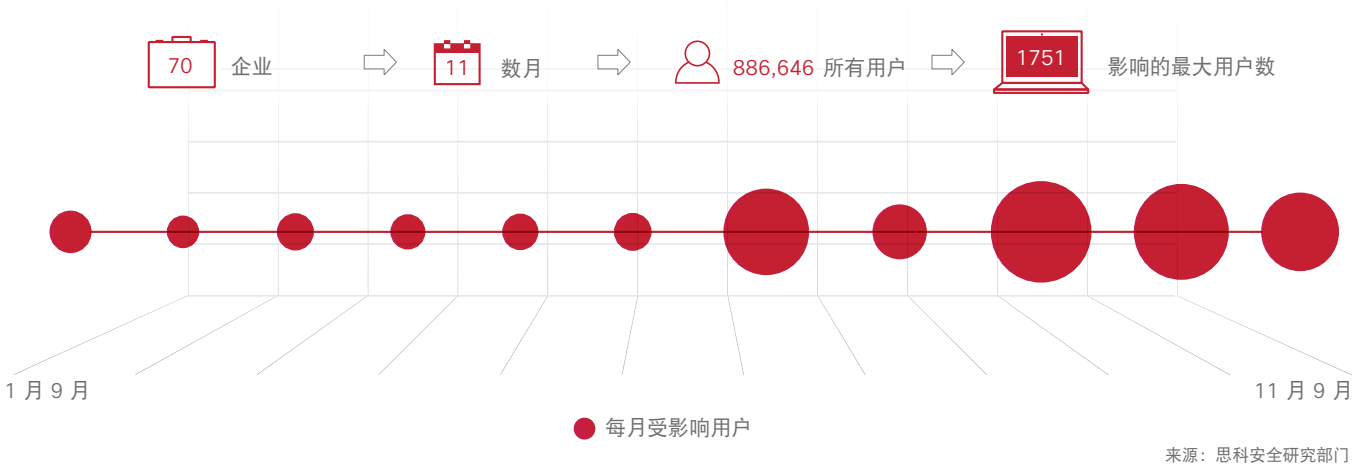
Microsoft IE



根据对 70 家公司 11 个月的用户活动所做的分析，受此类威胁影响的用户数呈上升趋势。1 月份有 711 名用户受到影响，而在下半年受影响的用户超过 1000 名，9 月份达到峰值 1751（图 18）。9 月份和 10 月份数量出现高峰的原因之一可能是人们结束暑期度假返回工作岗位后在线活动增加。

通过研究，思科安全专家发现网络攻击者往往会利用多台不同的服务器来支持其恶意软件攻击。这可能意味着某一个擅于分组活动的网络犯罪组织是造成此类威胁的罪魁祸首，或者某个“技术提供商”将其产品销售给了多个组织。无论哪种情况，恶意软件传播者似乎都在试图建立一个颇具规模的僵尸网络。

图 18. 每月受感染的用户数 2014 年 1 月至 11 月



来源：思科安全研究部门

分享报告

思科安全研究部门还发现，有 500 多个不同的域名与此类威胁有关；其中 24 个的 Alexa 排名在 100 万以内。也有许多域名排名相对较高（图 19）。这意味着这些域名比较受欢迎，但用户访问这些域名会非常危险，因为它们可能会给用户的网络带来安全风险。

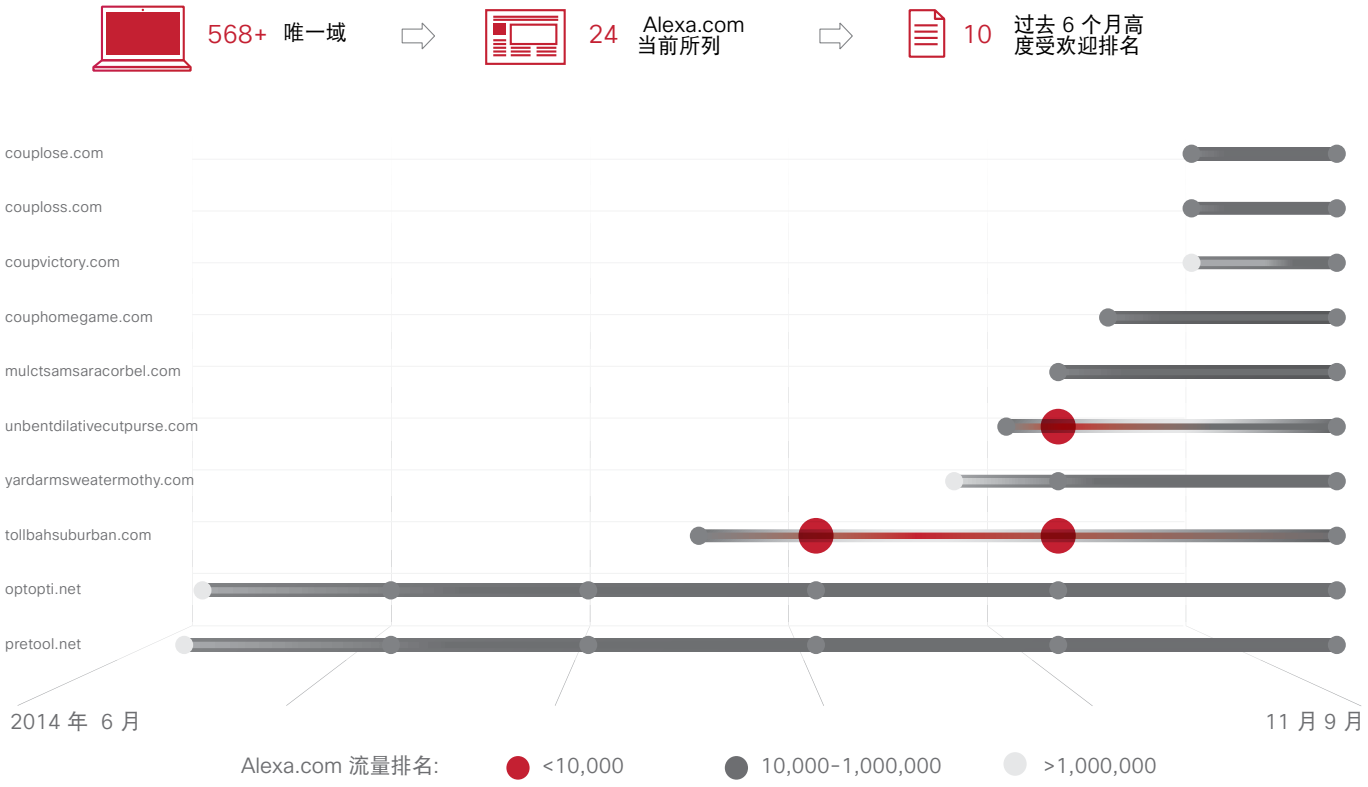
其中的某些域名已经活跃了一年多，但大多数的生命周期短得多 - 很多仅有几个星期（图 19）。所有的域名都有一个共同特征：普及的速度非常快。

防范与补救措施

要避免被浏览器加载项方案感染，或解决已有的感染，用户应采取以下措施：

- 从受信任的来源下载应用
- 以捆绑包方式安装时，不要勾选不需要的软件
- 使用威胁分析、沙盒技术和网络安全技术帮助防范和检测此类威胁
- 如果可能，手动卸载加载项；也可以使用反间谍软件工具清除不需要的程序

图 19. 通过浏览器加载项方案传播恶意广告所用的、在 Alexa 上有排名的流行域名



来源：思科安全研究部门

分享报告

2. 思科安全功能基准研究

为了评估在组织中担任安全职务的安全专业人员的安全意识，思科对首席信息安全官和安全运营经理就安全资源和安全规程进行了调查，调查对象来自多个国家/地区不同规模的组织。于 2014 年 10 月完成的*思科安全功能基准研究*，提供了有关安全运营完善度和当前采取的安全措施的见解。

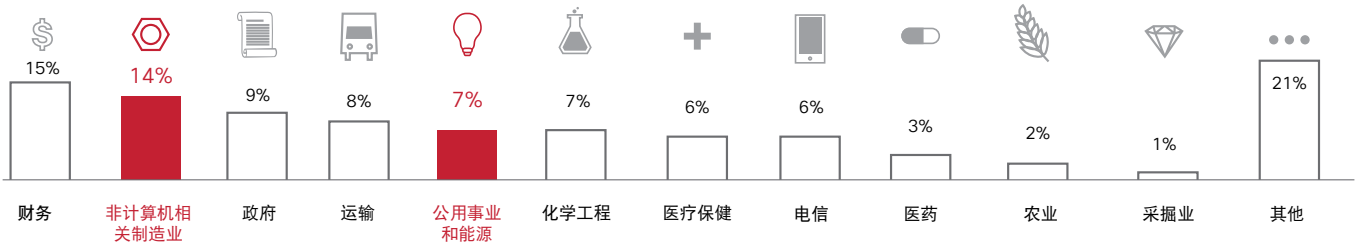
思科安全功能：组织的达标情况如何?

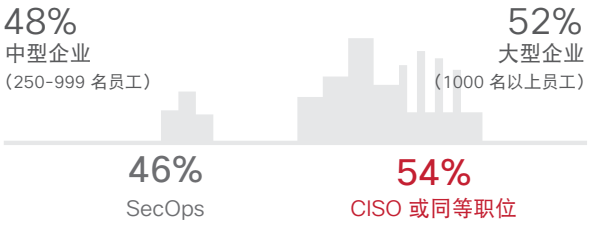
企业安全专业人员如何看待其组织应对安全漏洞的能力? 根据最新的思科安全功能基准研究，答案取决于该人员在组织内担任的角色和组织所在的行业。

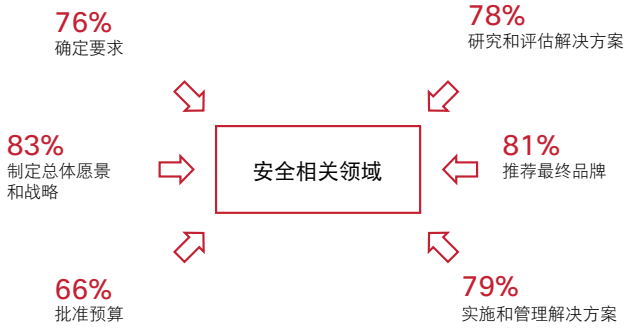
图 20 按行业和组织规模显示了专业人员的回答。来自非计算机相关制造业和公用事业/能源业的受访者报告了最高级别的安全投入和知识水平。

N（受访者人数） = 1738

图 20. 受访者背景和安全漏洞应对能力







来源：*思科安全功能基准研究*

分享报告

该研究对首席信息安全官和安全运营经理就以下方面进行了调查：所在公司投入到网络安全的资源；安全运营、策略和规程；以及公司网络安全运营的完善度。调查的结果令人欣慰：大多数安全专业人员认为他们在有效维护安全方面已拥有了相应的工具和流程。不过，对于目前的安全状况，首席信息安全官明显要比负责安全运营的同事乐观得多。例如，62% 的首席信息安全官非常赞同其组织中的安全流程清晰明确且已被充分理解；相比之下，仅有 48% 的安全运营经理持此看法。首席信息安全官对其安全流程也更满意。59% 的首席信息安全官非常赞同其安全流程已优化，现在侧重于流程改进；相比之下，只有 46% 的安全运营经理持此看法。

为什么自信度会存在这样的差距？ 可能是因为以下事实：首席信息安全官通常更远离日常安全活动，而安全运营人员往往深入参与到解决大大小小的安全事件当中。超大型组织的首席信息安全官可能并不了解通常每天会有上千台机器感染了恶意软件，而安全运营经理为了减轻感染而投入的时间要多得多，因此对组织安全的看法并不那么乐观。

此外，首席信息安全官可能正在制定诸如阻止访问社交媒体等策略，造成安全防御更严密、更坚不可摧的假象。然而，一旦完全关闭了这些渠道，安全团队将对仍徘徊在其网络四周的威胁缺乏了解或经验。

另一个自信度方面的差距体现在受访者对其组织安全策略自信度的回答。首席信息安全官和安全运营经理都对其策略高度自信（见图 21），但对其确定感染范围并加以遏制的能力并不那么自信（见图 28）。

类似的差距出现在受访者对安全控制的回答：几乎所有受访者都认为其组织具有良好的安全控制，但大约四分之一的受访者认为他们的安全工具只是“有点”效果，而不是“非常”有效或“极为”有效（见图 29）。

对安全流程和实践的自信度似乎也因行业的不同而有所差异。公用事业/能源业公司和电信企业的首席信息安全官和安全运营经理看起来最自信，相比之下，政府、金融服务、医药和医疗保健类组织的自信度较低。例如，62% 的电信和公用事业/能源业的安全高管非常赞同其安全流程已经过优化；相比之下，这一比例在金融服务业仅为 50%，在政府中则为 52%。

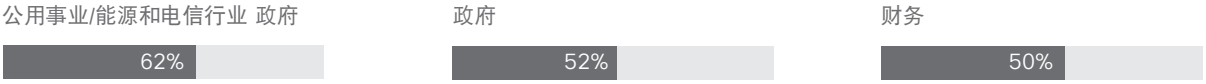
公用事业/能源业和电信业的安全专业人员在安全实践方面似乎最有经验；相比之下，政府和金融服务组织的安全专业人员则稍逊一筹。公用事业/能源业的组织往往拥有详尽的事件跟踪流程和程序。但是，这并不意味着这些组织比其他行业的组织更安全。

图 21. 主要发现（按行业和职位）

90% 的公司对自己的安全策略、流程和程序很有信心

但是，54% 的公司曾因安全漏洞而受到公众关注

非常赞同优化安全流程，而且现在致力于流程改进的公司所占比例：



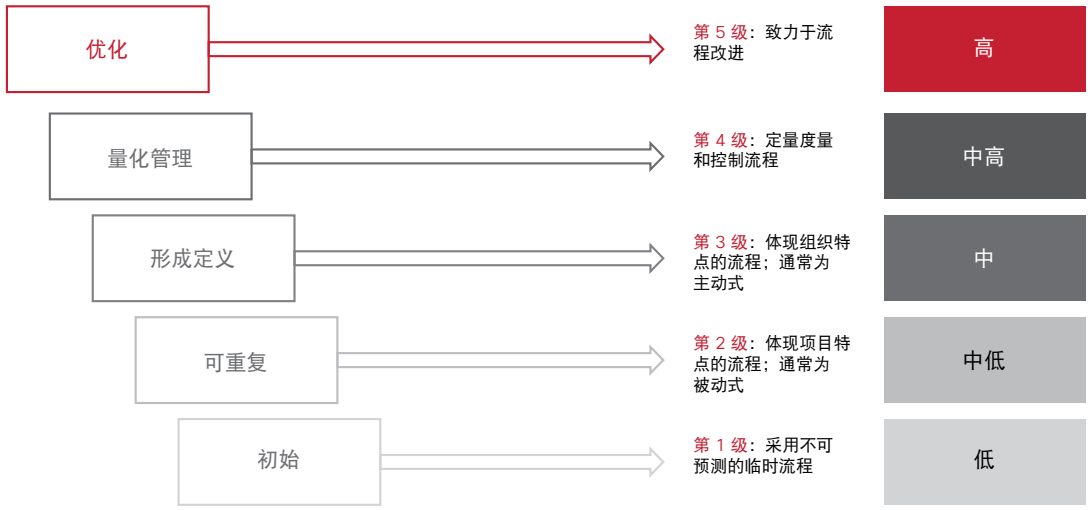
大型企业与中型企业之间几乎没有差异，这表明员工人数本身与安全完善程度关系不大。

来源：*思科安全功能基准研究*

分享报告

图 22. 完善度级别与当前样本之间的对应

思科探讨了多种样本分割方法，根据一系列与安全流程有关的问题，选择将样本分割为五类。 五类分割法与能力成熟度模型集成 (CMMI) 的对应关系相当紧密。



来源：*思科安全功能基准研究*

安全完善度的标志

*思科安全功能基准研究*还特别列举了安全状况相对更加完善的组织的特征。这些特征包括：

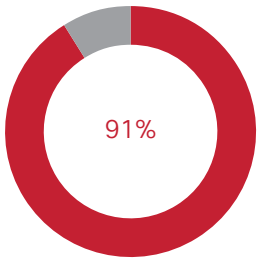
- 高层管理者将安全视为优先事项
- 有清晰明确且详尽的流程和程序
- 有可以协同工作的集成工具

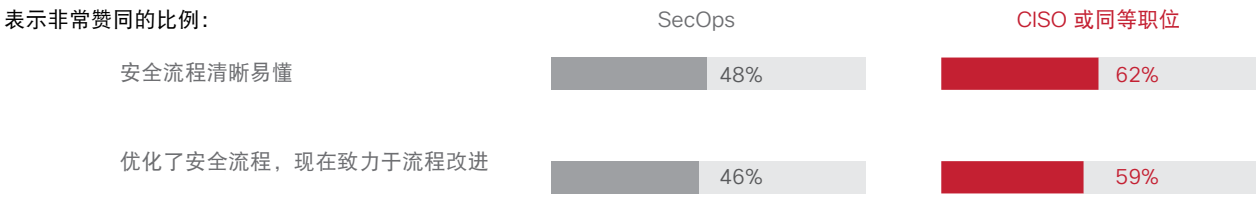
来自安全状况完善的公司的受访者中，有 91% 非常赞同公司高管已将安全视为优先事项；相比之下，来自安全状况最不完善的公司的受访者中仅有 22% 同意此观点。此外，来自安全状况完善的公司的受访者中，有 88% 非常赞同安全流程清晰明确且已被充分理解；相比之下，来自安全状况最不完善的公司的受访者中，这一比例为 0。

分享报告

图 23. 关于组织内安全事务领导的主要发现

91% 的受访组织由高管直接负责安全事务
通常是 CISO (29%) 或 CSO (24%)。





关于公司的安全状况，CISO（或同等职位）较 SecOps 经理更为乐观，这可能是因为他们距离日常安全工作更远。

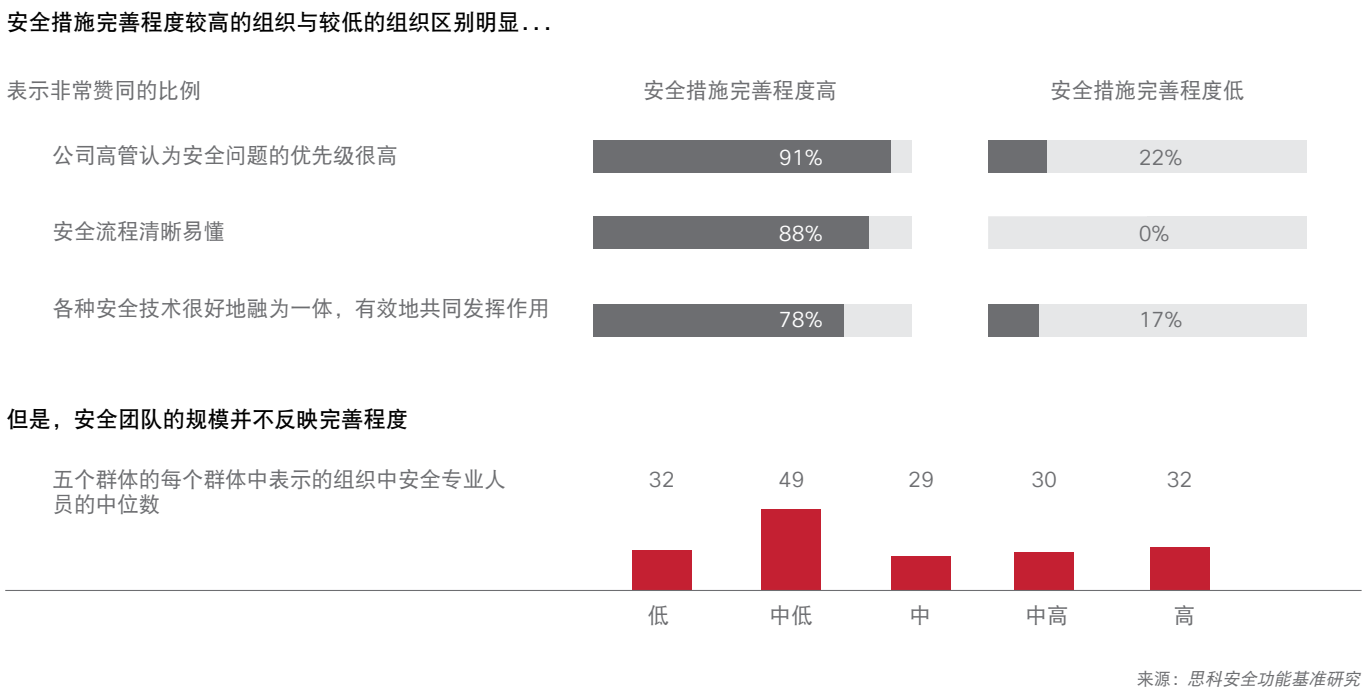
来源：思科安全功能基准研究

图 23 显示，91% 的受访者都报告称有一个直接负责安全的高层管理人员，最常见的是首席信息安全官 (CISO) 或首席安全官 (CSO)。组织从高级别管理人员中抽派专人负责安全是值得肯定的，因为若缺少安全事务领导，往往会造成流程定义不明确、沟通不畅和执行不力等情况。近期频发的重大安全漏洞已经促使组织专门设立一个负责安全管理的高管岗位。

安全状况完善程度较高的公司中，有 78% 的受访者都非常赞同安全技术得到了良好集成，可以高效地协同工作；而完善程度最低的公司中只有 17% 的受访者持此观点。

对于希望进一步完善安全流程的组织而言，好消息是，并不一定非要组建庞大的安全团队且团队成员还必须都是安全方面难得的人才。在完善程度最低的组织中，安全专业人员数量的中间值是 32 人；在完善度最高的组织中，安全团队人数的中间值也是 32 人。因此，雇佣更多的人似乎并不一定就能更有效地管理安全流程。组建安全团队的更好办法是找到公司中安全专业人员与全体员工数量的最佳比例。

图 24. 关于组织内安全事务优先级排定的主要发现



来源：*思科安全功能基准研究*

如图 24 所示，安全完善度不足的组织一般不认为高管会将安全视为头等大事，他们也不认为安全流程是明确且被充分理解的。

通过按国家/地区进行组织安全完善程度的比较，我们得到了更加令人欣慰的结果：在每一个国家/地区，安全完善度较高的组织都占较大比例。不过，在一些国家/地区，受访者对自身安全状况的看法比外界的看法更为乐观。某些国家的受访者过于自信的看法，可能部分源于文化的核心社会价值（例如需要让自己保持乐观态度，对其组织的看法也会是这样）造成的。

谨防过于自信

尽管首席信息安全官和安全运营经理们对安全运营方面都表示很有信心，但他们同时也表示并未使用有助于阻止安全漏洞的标准工具。不到 50% 的受访者使用的是下列工具：

- 身份管理和用户调配
- 补丁和配置
- 渗透测试
- 终端设备调查分析
- 漏洞扫描

分享报告

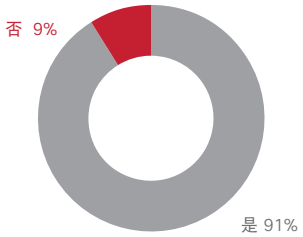
组织安全资源

图 25. 组织内专门负责安全的专业人员数量

组织平均拥有 123 名专业人员致力于安全问题。政府组织最有可能将他们的安全服务外包。

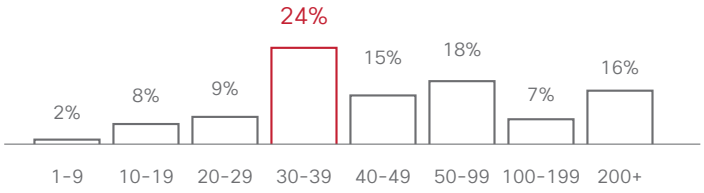
安全资源快照

贵组织是否有安全事件响应团队?



专职安全专业人员的平均人数

花在安全相关任务上的平均时间百分比



专职安全专业人员的数量

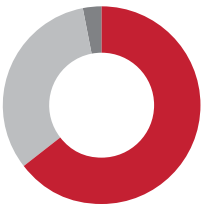
政府机构外包的安全服务比其他行业更多。

来源：*思科安全功能基准研究*

图 26. 组织使用的安全技术

大约三分之二的受访者称，他们的安全技术是最新的，并会经常更新。

您如何描述您的安全基础设施？ 基数：n=1738



64% 我们的安全基础设施非常新，还利用现有最好技术不断升级。

33% 我们定期更换或升级安全技术，但未配备最新最好的工具。

3% 只有在原有安全技术无法使用、已过时或有全新需求时，我们才会更换或升级安全技术。

更高比例的 CISO (70%) 表示其组织的基础设施非常新，相比之下，持这一看法的 SecOps 经理只占 (57%)。

电信公司最有可能声称自己的安全基础设施一直保持最新状态。

来源：*思科安全功能基准研究*

图 27. 组织使用的安全威胁防御措施

组织在 2014 年使用的各种安全威胁防御措施。

	组织使用的安全威胁防御措施		通过云服务管理的防御措施	
	SecOps n=797	CISO n=941	SecOps n=759	CISO n=887
网络安全、防火墙/入侵防御	57%	64%	30%	39%
网络安全	56%	62%	33%	41%
邮件/消息传送安全性	53%	58%	33%	41%
防数据丢失	55%	55%	-	-
加密/隐私/数据保护	52%	55%	-	-
访问控制/授权	55%	52%	24%	24%
身份验证	54%	51%	24%	22%
移动安全性	48%	54%	24%	32%
无线安全	47%	52%	22%	30%
终端保护/防恶意软件	45%	52%	24%	27%
漏洞扫描	44%	51%	24%	26%
VPN	49%	46%	25%	27%
身份管理/用户调配	43%	47%	16%	23%
安全信息和事件管理（SIEM）	39%	46%	-	-
网络调查分析	41%	43%	-	-
补丁和配置	38%	40%	-	-
渗透测试	39%	37%	20%	19%
DDoS 防御	35%	37%	-	-
终端设备调查分析	29%	33%	-	-

使用安全威胁防御措施的安全受访者；n=1646

13% 的受访者表示没有任何安全威胁防御措施是通过云服务管理的。 对于医疗保健、金融服务和制药行业来说，尤其如此。

来源：*思科安全功能基准研究*

分享报告

组织安全策略、规程和运营

图 28. 对组织安全策略的自信度和对组织侵害遏制能力的自信度

组织似乎对其安全策略颇有信心，但对其确定感染范围并加以遏制的能力明显信心不足。

对组织安全策略的自信度

安全策略 n=1738	SecOps n=797			CISO n=941		
	不赞同/赞同/非常赞同			不赞同/赞同/非常赞同		
盘点信息资产并明确地加以分类	11%	40%	49%	4%	38%	58%
我们的人力资源安全管理工作很出色	9%	45%	46%	4%	36%	60%
我的组织的计算机设备受到很好的保护	10%	39%	51%	4%	34%	62%
妥善管理系统和网络中的技术安全控制	6%	41%	53%	3%	31%	66%
网络、系统、应用、功能和数据的访问权限受到恰当控制	8%	35%	57%	4%	32%	64%
我们在将安全融入系统和应用方面做得很好	10%	38%	52%	4%	32%	64%
我们在将安全融入系统的购买、开发和维护流程方面做得很好	9%	41%	50%	4%	35%	61%

对组织侵害遏制能力的自信度

安全运营 n=1738	SecOps n=797			CISO n=941		
	不赞同/赞同/非常赞同			不赞同/赞同/非常赞同		
我们定期、正式、战略性地审查和改进安全实践	7%	42%	51%	3%	36%	61%
我们有相应的工具帮助我们执行审查，并且可提供有关我们安全实践能力的反馈	10%	41%	49%	4%	39%	57%
我们经常系统性地调查安全事件	11%	40%	49%	3%	37%	60%
如果需要，我们可加强对高价值资产的安全控制	10%	43%	47%	3%	38%	59%
我们定期检查网络连接活动，以确保安全措施在按预期目标正常工作	8%	39%	53%	4%	33%	63%
我们的威胁检测和阻止功能保持最新	9%	38%	53%	3%	36%	61%
我们的各种安全技术很好地融为一体，有效地共同发挥作用	9%	40%	51%	3%	37%	60%
安全很好地融入了我们组织的目标和业务能力中	10%	39%	51%	2%	34%	64%
我们能够轻松确定感染的范围，加以遏制，防止事态进一步扩大	15%	44%	41%	8%	42%	50%

与大型企业的受访者相比，更多中型企业的受访者非常赞同“我们定期、正式、战略性地审查和改进安全实践”。

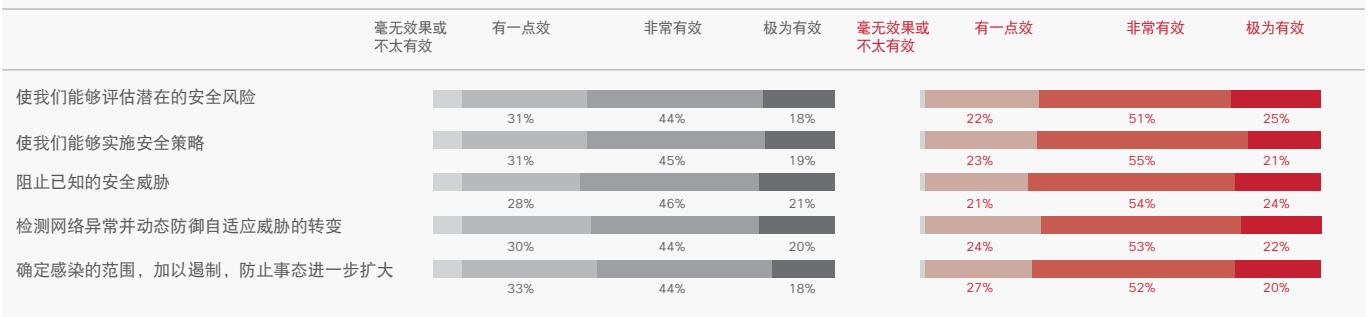
来源：思科安全功能基准研究

图 29. 受访者对公司安全控制措施和组织所使用的安全工具的看法

尽管安全专业人员相信其组织已具备有效的安全控制措施，但大约四分之一的受访者仍认为他们的安全工具收效甚微。

安全控制 n=1738	SecOps n=797			CISO n=941		
	不赞同/赞同/非常赞同			不赞同/赞同/非常赞同		
我们遵循标准化的事件响应做法，如 RFC2350、ISO/IEC 27035:2011 或美国认证标准	15%	42%	43%	6%	40%	54%
我们有高效的流程，可以解读将出现的事件报告，确定它们的优先顺序，并且理解它们	11%	46%	43%	4%	39%	57%
我们有很好的系统，可以验证安全事件是否实际发生	11%	41%	48%	4%	36%	60%
我们有很好的系统，可以对事件相关信息进行分类	10%	43%	47%	4%	37%	59%
在向利益相关方通报安全事件以及与之协作等方面，我们做得很好	10%	46%	44%	3%	40%	57%
我们有详尽的事件响应、跟踪流程和程序	9%	40%	51%	4%	35%	61%
我们的网络风险评估已纳入日常整体风险评估流程	10%	37%	53%	4%	36%	60%

公用事业/能源行业的受访者非常赞同“我们有详尽的事件响应、跟踪流程和程序”的陈述，其比例明显高于其他大多数行业。



对于组织检测和防御已知安全威胁的能力，交通运输行业安全专业人员的信心较低。

来源：*思科安全功能基准研究*

分享报告

图 30. 用于分析受侵害系统并消除安全事件根源的流程

安全专业人员最有可能使用防火墙日志来分析侵害，但这些日志的数据通常质量不高且其中的信息没有上下文。为了更好地分析侵害，安全专业人员应该定期查看 IDS 和 IPS 日志、代理、基于主机的入侵防御系统 (HIPS)、应用程序日志，以及 NetFlow。

我们也惊讶地发现“事件/日志关联分析”位于侵害分析工具列表上较低的位置。这可能意味着受访者并没有将数据关联或将数据源链接在一起，而其实，这将有助于提供更深入的安全事件分析。

被入侵系统的分析流程	SecOps	CISO
	n=797	n=941
防火墙日志	59%	62%
系统日志分析	58%	60%
恶意软件或文件回归分析	51%	58%
网络流量分析	51%	54%
注册表分析	48%	51%
完整数据包捕获分析	44%	48%
关联事件/日志分析	40%	44%
内存调查分析	39%	43%
磁盘调查分析	38%	41%
入侵指标 (ISSOC) 检测	38%	38%
外部[或第三方]事件响应/分析团队	36%	38%

与其他大多数行业相比，政府受访者倾向于使用更多流程来分析被入侵系统。

安全事件成因消除流程	SecOps	CISO
	n=797	n=941
隔离或删除恶意应用	55%	60%
根本原因分析	55%	56%
阻止恶意软件传播	51%	55%
其他监控	51%	53%
策略更新	50%	51%
阻止被感染的应用传播	47%	49%
长期修复方案开发	46%	48%
将系统重新镜像到以前的状态	43%	47%

除阻止恶意软件传播这一项外，CISO 和 SecOps 回答基本一致。

来源：思科安全功能基准研究

图 31. 首席信息安全官与安全运营专业人员对事后控制的响应

较之于安全运营专业人员，更多的首席信息安全官报告称实施了额外的事后控制。

受影响系统的恢复流程	SecOps	CISO
	n=797	n=941
根据事件后查明的漏洞，实施其他或全新检测和控制措施	55%	65%
修补和更新有漏洞的应用	59%	60%
用事件前的备份进行恢复	53%	60%
差异恢复	53%	58%
黄金映像恢复	33%	36%

电信和公用事业/能源行业的受访者表示其利用黄金映像恢复的情况多于其他行业。

图 32. 谁会收到安全事件通知

运营人员和技术合作伙伴最有可能通过更正式的流程收到安全事件的通知。

发生事件时通知的群体	SecOps	CISO
	n=797	n=941
运营	44%	48%
技术合作伙伴	42%	47%
工程技术	38%	37%
人力资源	37%	35%
法务	37%	35%
全体员工	38%	33%
制造	31%	36%
业务合作伙伴	31%	33%
营销	30%	31%
公关	30%	27%
外部机构	25%	20%

与其他行业相比，政府机构明显更可能有定义明确的通知流程，其通知群体的成员也更多。

来源：思科安全功能基准研究

组织安全完善度

图 33. 安全流程的完善度

大多数公司都满足更完善的安全配置。在所有国家（图 34）和所有行业确实是这样（图 35）。

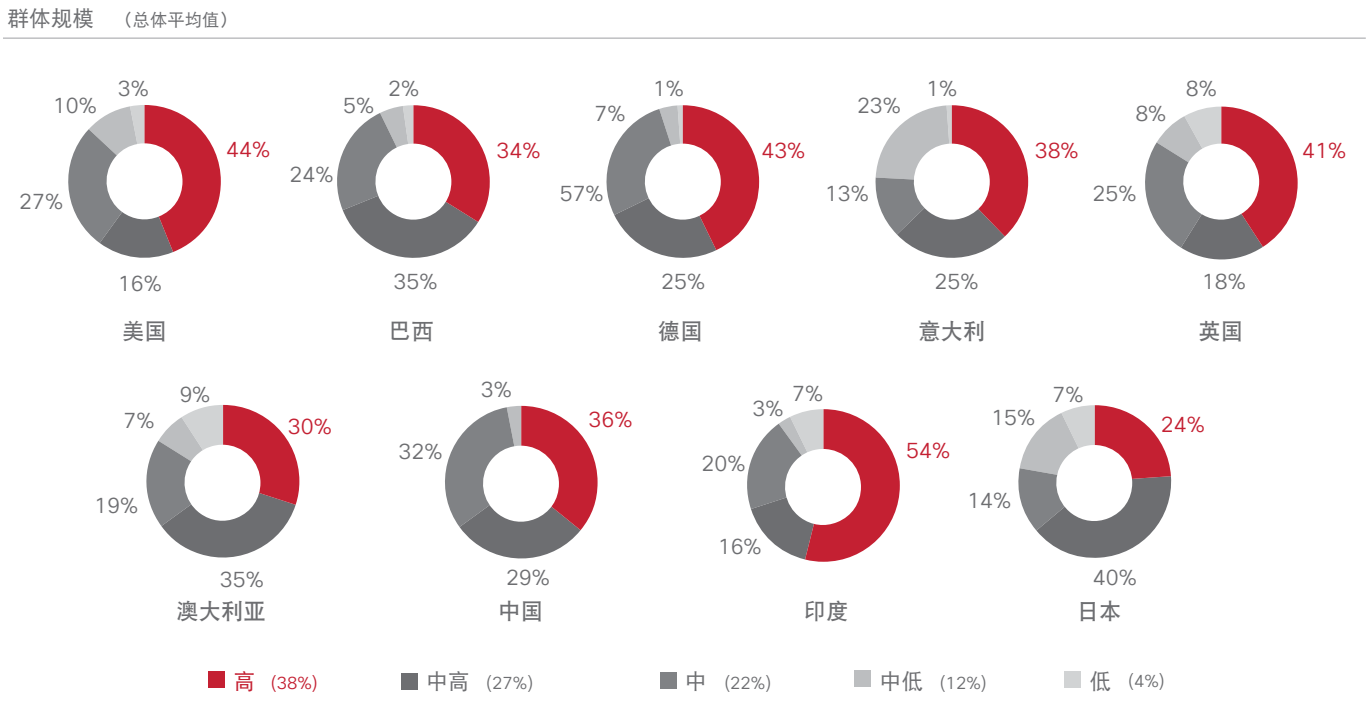
群体划分反映了与安全优先级相关的逐渐提高的完善程度，及其如何转化为流程和程序

群体规模

高	39%
中高	23%
中	26%
中低	8%
低	4%

来源：*思科安全功能基准研究*

图 34. 安全流程的完善度（按国家/地区）

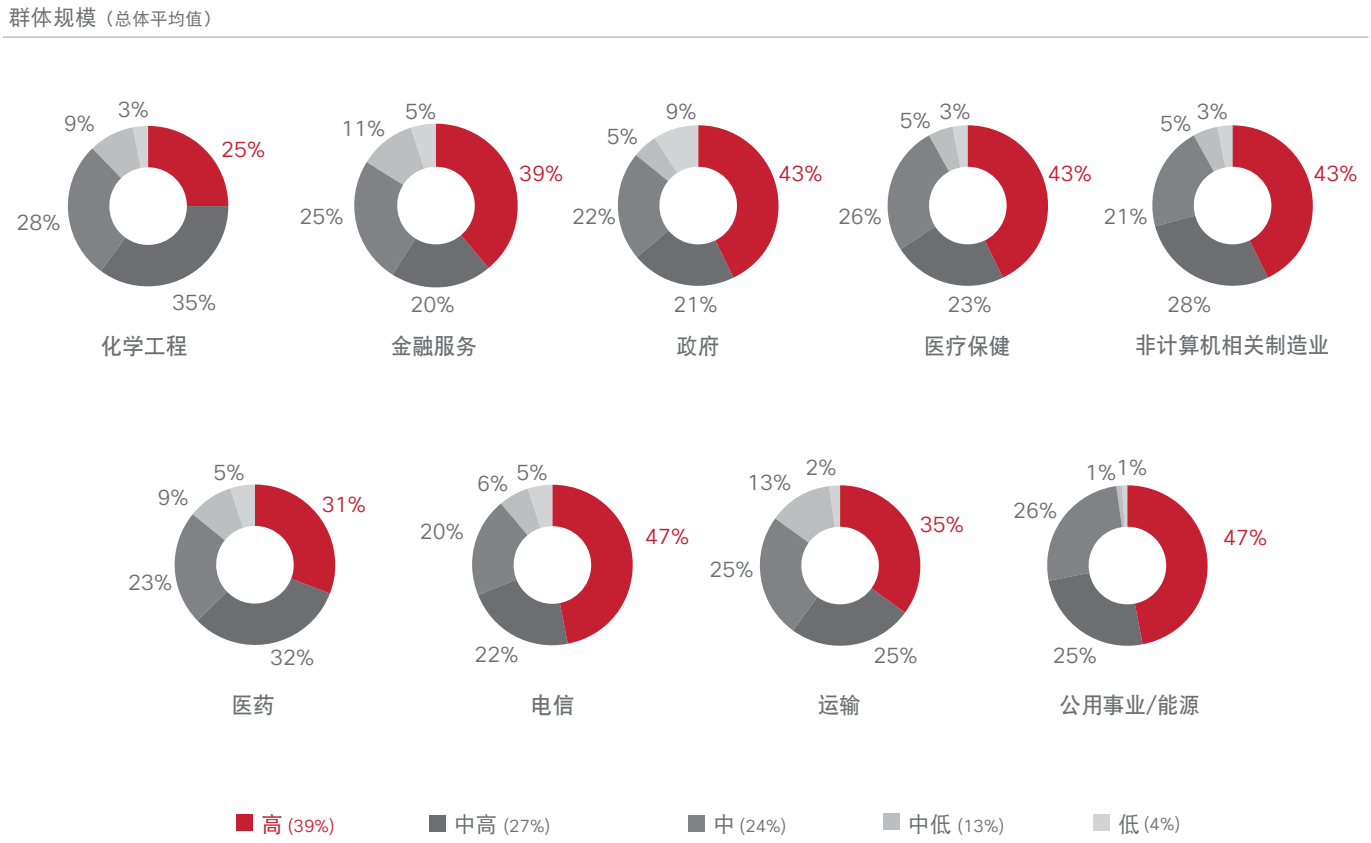


来源：*思科安全功能基准研究*

分享报告

图 35. 安全流程的完善度（按行业）

近半数的电信与公用事业/能源组织都被归入了安全度高度完善的类别。



来源：思科安全功能基准研究

中型组织似乎已为安全就绪性做好准备

超大型组织有望成功管理安全性，因为他们能够获得众多资源：购买最新技术的预算以及技能娴熟的安全管理人员。在对安全事件的响应能力方面，人们认为较大的中型企业（出于本研究的目的，定义为员工人数在 500 至 999 人之间的企业）应当落后于大型企业（员工人数在 1000 人以上的企业）。然而，*思科安全功能基准研究*表明，较大的中型企业由于组织灵活性和敏捷性更高，在诸多领域的安全就绪性不但能够比肩大型企业，甚至常常超过后者。

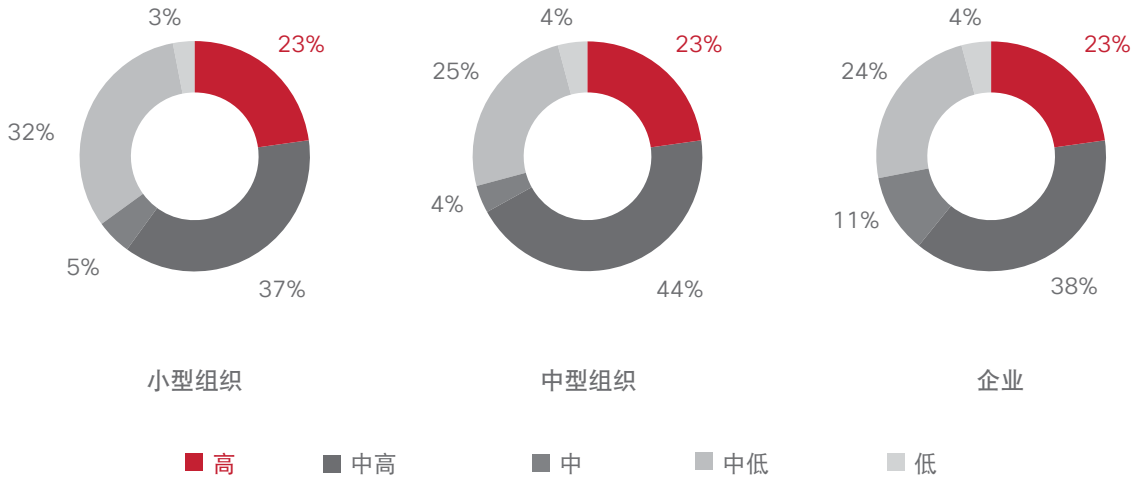
实际上，研究结果显示，较大的中型组织更可能具有高度完善的安全状况。如图 36 所示，在较大的中型组织类别，安全完善度处于中高级和高级的比例明显高于较小的中型组织（250-499 名员工）和大型企业组织（1000 名以上员工）。

作为经济复苏的主要动力，中型企业具备最高完善度的情况令人鼓舞。

中型企业及其安全状况基准调查主要发现：

- 92% 的中型组织内部设有事件响应团队，而大型企业的对应数字为 93%。
- 94% 的中型组织由一名高管直接负责安全事务，而大型企业的对应数字为 92%。

图 36. 较大的中型组织安全状况完善度



群体划分反映了组织内部与安全优先级相关的逐渐提高的完善程度，及其如何转化为流程和程序。

评级为中高和高的中型组织明显多于小型组织和企业。

至少有 60% 适合搭配安全措施完善程度更高的配置文件。

来源：思科安全功能基准研究

分享报告

3. 地缘政治趋势和行业趋势

思科安全专家、地缘政治专家和政策专家发现了已经存在及逐渐兴起的地缘政治趋势，需要各个组织（尤其是跨国公司）予以关注。这些专家还考察了全世界在数据主权、数据本地化、数据加密和数据兼容性领域的最新发展及潜在趋势。

网络犯罪在监管力度薄弱的地区疯狂肆虐

首席信息安全官及其他安全领导对于地缘政治形势的关注可能时有疏漏，这种情况亟待转变，跨国组织的工作者更应如此。地缘政治形势的变化可能直接影响到全球供应链，还会影响各个国家/地区的企业管理客户数据及员工数据的方式；同时，还可能增加法律及监管成本，并面临商业秘密泄露的风险、物理风险和名誉受损的风险。

网络犯罪在全球，尤其是在监管力度薄弱的地区十分猖獗。长久以来一直作为有组织犯罪温床的东欧就是一个例子。在监管力度薄弱的地区，时有证据显示政府情报部门与有组织网络犯罪团伙来往甚密。

美国当局表示，近期备受瞩目的多起针对美国境内资产发动的攻击很可能源于这样的地区。有些攻击并非源于经济利益，而是怀有收集情报或渗透基础设施的政治动机或企图。[7] 这可能表明，这些攻击的背后可能有国家支持，并且/或者由组织严密的网络犯罪组织精心策划。

越来越多国家的政府正在通力合作，旨在通过立法和监管加大网络监管力度。例如，中国在中共十八大四中全会上提出了“依法治国”主题。[8] 中国政府决心根除腐败并加大在企业及政府内部的执法力度。此举可能加强打击网络犯罪的执法力度和国际合作，让犯罪分子难以藏身。

跨国恐怖组织对互联网的利用

诸如所谓“伊斯兰国”（又称 ISIS 或 ISIL）之类跨国恐怖组织的出现，让我们看到另一种值得关注的地缘政治趋势。虽然没有迹象表明 ISIS 之类的组织参与过重大的网络犯罪活动，但他们却在依靠互联网（比如社交媒体）招募成员。目前，主要的跨国恐怖组织似乎可以通过敲诈勒索、贩卖人口和买卖石油等传统筹资活动筹集到足够的资金。然而，随着这些组织的发展壮大，他们可能转而通过实施网络犯罪为全球的恐怖活动提供资金支持。还有一种可能的趋势是，新兴的恐怖组织由于不能像较成熟的恐怖组织那样获得足够的资源，因此很可能会将网络犯罪作为迅速壮大组织的捷径。

请参阅思科博客文章“Cupcakes and Cyberespionage”，了解关于防范网络间谍活动的新建议。

关于数据主权、数据本地化和加密的复杂难题

爱德华斯诺登对美国政府过度监听的指控、数据主权（指的是数据受所在地法律管辖，而非受可能寻求单边数据访问的外国政府或法院管辖的概念）和数据本地化（政府规定数据存储在特定的地点）已经成为热点议题。

一些国家/地区正开始谋求对数据进行本地化，以此作为防止外国政府获取本国公民数据的手段。他们目前正在起草一些规章制度，要求数据不得向国外传输，或必须通过某些规定的途径传输，并且各公司必须使用本土生产的设备。

例如，巴西最近施行了一项新法律，该法律“所作的隐私规定覆盖了大范围的公司，限制这些公司共享用户个人信息、通信内容以及特定在线日志数据。”[9] 与此同时，俄罗斯最近也对其数据保护和信息法案做出修正，要求处理俄罗斯公民个人数据（包括互联网数据）的所有数据运营商将这些数据的副本存放在俄罗斯境内的服务器和数据库中；该项法律将于 2015 年生效。[10]

各国/各地区律令数据本地化的一个潜在弊端是制定的法规缺乏互操作性，导致跨国公司可能会面临相互冲突的法律规定。遵照一个国家/地区的法规履行复制、保留或销毁数据的义务可能会违反另一个国家/地区的法律。

除了可能导致相互冲突的法律义务以外，数据本地化规定还可能限制数据跨国境线流动。这不但会造成混乱，也使网络管理工作面临巨大挑战。供应链方面同样存在问题：越来越多的跨国供应链运营商都在采用云技术，以实现全球合作伙伴的互联互通。数据本地化可能妨碍甚至完全阻止这些商业网络中的数据交换，并可能妨碍跨国境活动乃至反网络犯罪活动。

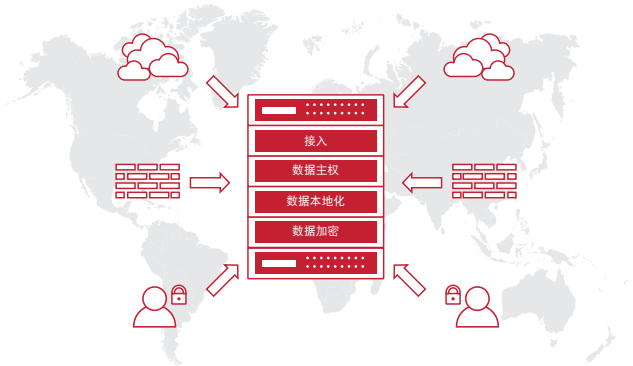
此外，由于一些国家/地区选择仅允许使用本土技术，或者对公民数据的处理者身份过多地施加限制，导致这些国家/地区可能被拒于全球人才库之门外，并因此丧失新思想交流所激发的创新能力。

美国一些主流技术公司希望能够采用端到端加密方式满足客户要求，在客户数据往来传输于无边界的互联网时为其提供保护。然而，美国政府担心这种加密方式会导致政府丧失保护公民的能力。英国国家通信情报局（类似于美国国家安全局）是英国最重要的信号情报组织，该局的新任局长甚至暗示，美国社交媒体技术巨头公司助纣为虐，因允许恐怖分子在全球发送加密的通信内容而为恐怖活动行方便之门。[11]

尽管有这些批评之声，但在政府实施能够体现自由言论和确保商业安全重要性的政策，并能消除对公共安全和国家安全构成的威胁之前，为了能够重新获得客户的信任，各技术公司很可能仍会寻求开发相应的技术措施并予以采纳。

对技术产品及其研发公司的信任将会对国家及其政府和民众树立信心，相信自己及自己的数据能够受到保护产生深远的影响。正如思科高级副总裁、总顾问兼秘书 Mark Chandler 年初在一篇思科博客文章中指出的那样：“认真努力解决这些问题可以树立信心，而最重要是，这样做能够让我们兑现对新一代互联网的承诺，那就是，打造一个能够通过人与设备的互联互通，让全人类享有更多自由、让社会更加繁荣并创造更多机会的世界。”[12]

图 37. 解决在数据主权、本地化和加密之间求得平衡的难题



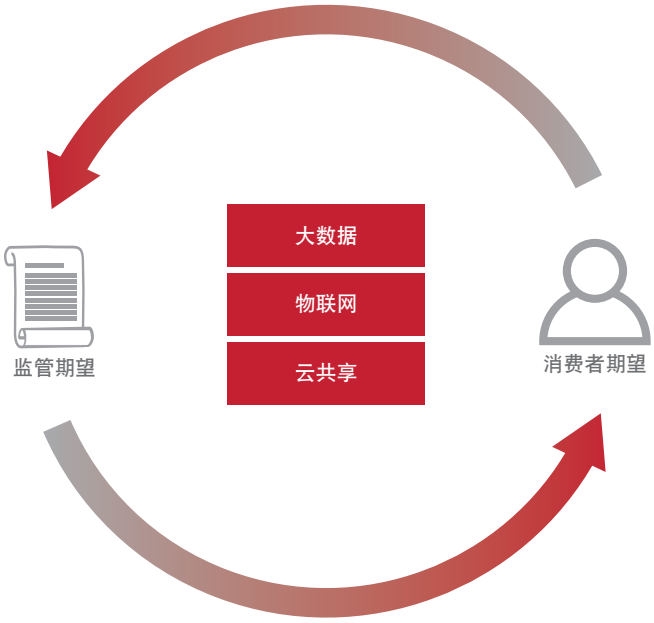
数据隐私的兼容性

个人或组织对数据隐私抱持的态度在很大程度上取决于其生活和工作环境。这些不同的观点影响着政府对数据隐私的监管方式，以及在这些监管政策相互冲突时企业如何开展业务。由思科发起、云安全联盟编写的***数据保护热度指数调查报告***详细介绍了以下企业面临的部分挑战：需要处理位于本国之外的数据；或需要处理属于业务运营国度之外的个人的数据。

随着云服务的增长，关于数据隐私兼容性（即达成全球统一的数据隐私处理办法）的讨论变得日益迫切。举例来说，如果一家总部设在美国的公司从一家位于印度的公司手里购买了云存储服务，然后使用该服务存储了位于德国的客户的数据。在这种情况下，到底该遵从哪个国家或地区的隐私法律?

此外，物联网 (IoT) 和大数据也迫切要求实现数据隐私的兼容性。企业纷纷考虑采取新的方式来实现设备互联，并利用大量数据集来制订商业决策，在这样的背景下，他们需要在全球范围内都适用的数据处理结构和规则。

图 38. 满足各种监管和消费者预期



目前，全球有多方正在努力协调跨地区或跨多个国家的数据隐私要求。例如，目前欧盟正在制订将更新现有数据保护框架的法规 - *通用数据保护条例*，以期实现数据保护法规的协调一致。目前，各方正在加大努力，以期在数据隐私和数据主权法律方面达成共识。在更大的地域范围内达成统一固然可喜，但不容忽视的是最终结果必须：以成果为导向、能够与其他地区互通，且顺应新的技术趋势。在亚太地区，亚太经合组织 (APEC) 已制订了跨境隐私执行协议，这有利于该地区经济体之间的数据共享。为满足一个更大的目标 - 打造能够促成数据跨国家和跨地区自由流动的开放互联网的全球公认标准，并在此基础上构建数据隐私和安全的兼容性体制，政府必须完成更多的工作。

随着各个国家和地区明确其数据隐私处理办法，企业将能够更好地在全球范围内实施统一的隐私保护措施，实现更有效的“隐私设计”框架，让隐私功能从一开始就内嵌于产品和服务之中。无论企业将产品部署在世界哪个角落，明确且一致的隐私监管框架都有助于其满足和超越隐私要求，从而鼓励创新的产品开发和数据使用。

数据隐私：全球共识

本次数据保护调查就区域数据监管政策、政府做法、用户内容和安全标准采访了北美、欧盟和亚太地区的全球隐私专家。结果表明，对数据隐私的含义和全球统一隐私标准的价值，各地受访者的理解高度一致。

- **数据的驻留和主权：**大多数国家/地区的受访者认为，个人数据及个人身份识别信息 (PII) 必须驻留在当地。
- **合法拦截：**受访者对何时以及如何拦截数据（例如，需要展开犯罪调查时）抱持一致的看法。
- **用户同意：**百分之七十三的受访者认为，应出台消费者隐私权法案，这是全球人民而非某地区人民的权利。百分之六十五的受访者表示，联合国应在制订此类法案的过程中发挥积极的作用。
- **隐私准则：**受访者被问及经济合作与发展组织的隐私准则将有助于数据的协调还是会制造更大的压力。对此，大多数受访的数据隐私专家倾向于采纳这些隐私准则。

总的说来，本次数据隐私调查似乎表明，许多专家都认为在全球范围内施行基本的隐私保护准则并将其标准化，将有助于商业的发展，而不是成为一种阻碍。此外，调查结果还表明，数据隐私专家普遍认为应制订适用于新技术解决方案的隐私准则，而不是试图改造这些解决方案来满足隐私要求。不过，目前的隐私监管框架还处于起步阶段，但发展迅速。

实现更高水平的协调后，企业和个人都将从中获益。但鉴于行业内的全球统一隐私框架还未达成，企业需要认真考虑隐私和数据保护问题，积极地调整产品和流程，以满足各式各样的客户和监管要求。

有关数据保护问题的更多信息，请参阅思科安全博客文章，“Data Protection in the Balance—EU Citizen Protection and Innovation”（数据保护悬而未决 - 欧盟公民的保护意识和创新举措）。

4. 改变看待网络安全的视角 – 从用户转移到企业高层

思科安全专家建议企业立即开始转变实现网络安全的思路，以便真正地提高组织的安全性。达成这一目标的战略包括：探索新的人员、流程、技术协调方案；将安全议题提升到企业董事会层面；以及采取更周密的安全控制措施，缩小终端和网络的攻击面，并在网络遭受攻击后对其进行强化。

安全访问：掌握网络中用户的身份、接入时间和接入方式

在访问网络信息和服务方面，首席信息安全官和其他安全专业人员面临着复杂的挑战。随着移动性和自带设备 (BYOD) 策略的日渐盛行，企业必须确保员工能够随时随地随意地访问企业资源。

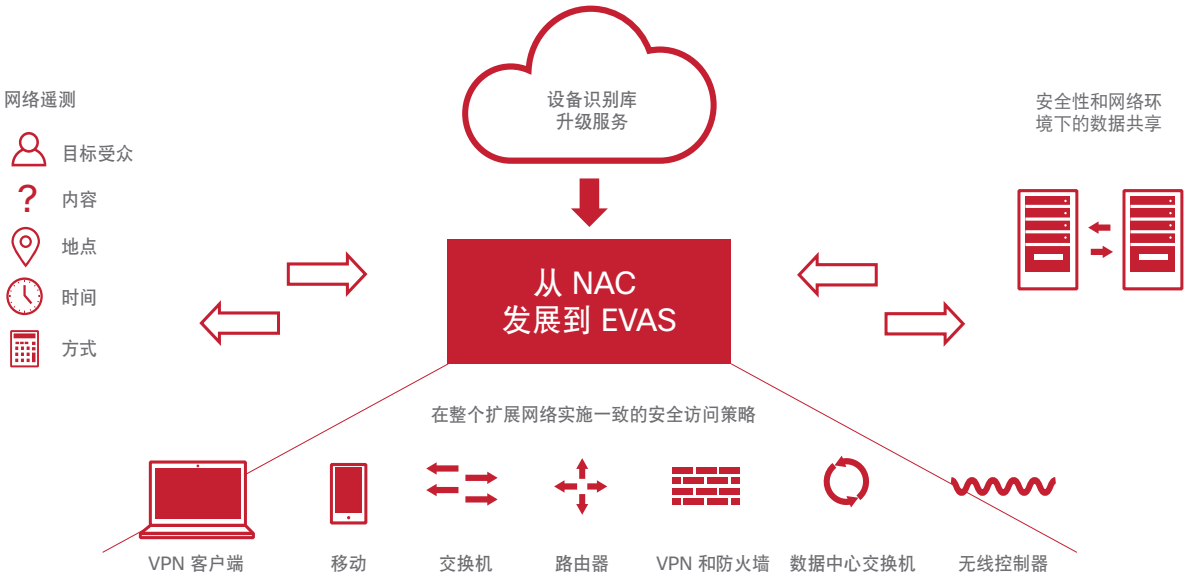
安全专业人员还需要保护网络免受未授权用户访问或犯罪分子的攻击，而且必须以不妨碍合法用户访问的方式进行。例如，虚拟专用网络 (VPN) 曾经是提供网络访问控制的标准解决方案。但某些 VPN 要求用户执行复杂的登录流程，且需要专用软件、限制用户接入网络的时间和方式。此外，许多 VPN 无法帮助 IT 部门确定是谁在何处访问网络，也无法识别所用的设备。VPN 正在不断发展，可在提供更高可视性的同时，营造更透明的用户体验，以提高终端的安全性。

网络访问控制 (NAC) 正在从基本的安全保护演变为更尖端的终端可视性、访问和安全性 (EVAS) 控制。与传统的 NAC 技术相比，EVAS 利用更精细的信息（例如用户角色、位置、业务流程考量、风险管理等数据）来执行访问策略。此外，EVAS 控制还有助于授予电脑以外其他设备的访问权限，使得网络管理员能够提供手机和物联网设备的接入。

EVAS 可帮助实现“网络即传感器”型的安全策略，在整个扩展网络允许或阻止访问—无论是通过远程设备 (VPN)、在连接网络服务之前，还是网络内部跨越敏感资源池的访问。此外，EVAS 还能帮助组织缩小终端和网络的攻击面，限制攻击的规模和范围，纠正问题解决流程，甚至是在受到攻击后强化网络。

有关 EVAS 解决方案及其如何帮助企业提高安全性的更多信息，请参阅思科安全博客文章：“New White Paper from Enterprise Strategy Group on the Evolution of and Need for Secure Network Access”（Enterprise Strategy Group 就安全网络访问的演进和需求发表的新白皮书）。

图 39. 从网络访问控制 (NAC) 到终端可视性、访问和安全性 (EVAS) 控制的演进



在攻击前，EVAS 能够：

- **识别有风险的资产。**随时监控连接到网络的所有资产，确定不符合要求的用户、设备和应用，并将此类信息与第三方漏洞评估工具相关联。
- **更好地降低风险。**收集有价值的情报，然后与其他安全和网络应用共享，以改进工作流程，简化运营，并按优先顺序安排补救措施。
- **实施精细的网络访问策略。**为精细的策略施行提供情景信息，限制对敏感内容、资产或网段的访问。

在攻击中，EVAS 能够：

- **与先进的基于网络的威胁防御系统集成。**在检测到恶意活动后共享知识，逐步关联终端连接、配置和行为模式等攻击数据。
- **阻止已受感染的系统构成“杀伤链”。**阻止已受感染的系统从受策略控制的非授权网络资产处窃取凭据、提升权限、盗走有价值的数据，从而阻截攻击者的横向攻击行动。
- **限制攻击范围。**限制并隔离行为异常的系统。

检测到攻击后，EVAS 能够：

- **检视终端配置文件，进行漏洞评估。**与漏洞分析工具分享来自 EVAS 数据库的信息，帮助 IT 运营人员确定修复优先级。
- **修复已受感染的系统。**在与安全信息与事件管理 (SIEM) 系统和终端安全系统集成时，EVAS 能够自动修复和监测进度。
- **精细调整访问策略和安全控制。**与网络和安全设备协作切分应用流量，或者添加新的防火墙规则或 IPS 签名。

EVAS 解决方案不同于以往过于复杂的网络访问控制，它是业务的推动者。随着企业着手实施 BYOD 策略、云计算和移动性举措，取得可视性、改善连接用户和设备的环境并有效地实施安全策略变得更加迫切。据思科安全专家预测，越来越多的首席信息安全官将转向使用 EVAS 解决方案来管理用户、设备、网络和云服务间的复杂的连接网络。

分享报告

网络安全的未来取决于企业高层今日的参与

*思科安全功能基准研究*指出，91% 的组织有直接负责安全事宜的高管。但对于现代企业而言，安全事务的领导需要提升到组织的更高级别：董事会级别。

涉及知名企业的最新大规模数据泄露、越来越多与数据安全相关的立法和监管政策、地缘政治动态，再加上股东们的期望，这些因素都在促使企业将网络安全议题摆到董事会的会议桌上。信息系统审计与控制协会 (ISACA) 的一份报告显示，今天 55% 的企业董事必须亲自了解网络安全问题并对之进行风险管理。[13]

这是个积极的进展，但思科安全领导认为早该如此。在现代的经济环境下，所有公司都离不开 IT。这使得安全与组织中从行政长官到新进雇员的每一个人息息相关，它再也不仅仅是职位或工作职责描述中带有“安全”字样的人员的专职。每个人都应该负起责任，学会如何不沦为受害者。

思科安全领导断言，董事会的更多参与是未来网络安全的核心组成部分。各行各业的企业董事会都需要了解企业面临哪些网络安全风险，以及它们具有哪些潜在影响。为真正理解影响组织的网络安全问题的范畴，某些董事会可能需要邀请技术和网络安全专家加入。

此外，董事会还需要开始考虑与安全控制有关的棘手问题：*我们采取了哪些控制措施？ 是否经过了严密测试？ 是否设有报告流程？ 对于不可避免的损失，我们多长时间能够得知并实施补救措施？* 也许，最重要的问题应该是：*我们还应该知道些什么？* 首席信息官必须做好准备，以回答董事会提出的此类问题。这些问题对董事会成员来说十分重要，同时也涉及到对业务的影响。

在《财富》杂志最近进行的一次采访中[14]，思科首席安全与信任官员 John Stewart 表示，董事会提出此类问题有助于引发“一系列有趣的下游效应”，并最终将安全行业领向成熟。他认为，到达该阶段后，接下来的重要一步（希望能实现）将是：厂商终于认识到必须将安全融入其产品之中。

Stewart 预计，随着物联网 (IoT) 的发展，“互联网上的无人监管设备会多于有人监管设备”，因而未来一定会爆发潜在规模巨大的“事故”。在设计之初即将安全融入到产品内部有助于规避许多此类问题，或至少是减轻其影响。

因此，技术制造商的董事会应向其安全负责人提出问题：*我们是否已将安全融入产品当中？ 如果不是，需要多久才能做到？*

观看思科首席安全与信任官员 John Stewart 就网络安全的透明性和董事会问责制的重要性所发布的视频博客：http://blogs.cisco.com/security/ensuring-security-and-trust-stewardship-and-accountability。

思科安全宣言：实现现实世界安全的基本准则

当今的首席信息安全官需要回答尖锐的问题：*潜在的安全问题出现时，如何使我们的安全团队第一时间介入？ 如何确保我们的团队拥有找出最关键的安全问题并采取行动所需的工具和可视性？ 如何确保用户 – 企业取得成功的关键 – 时刻远离危险?*

思科安全专家建议，首席信息安全官可通过实施并遵循一系列被称作思科安全宣言的安全准则来解决这些问题。

这一创始性安全宣言可帮助安全团队及其组织的用户更好地理解和应对当今世界面临的网络安全挑战。在通往安全的道路上，为比竞争对手更具活力、更具适应性、创新能力更强，企业可将这些准则用作基准：

1. **必须将安全视为业务的增长引擎。**安全绝不该是破坏用户工作效率或阻碍企业创新的障碍或包袱。但是，安全团队实行的技术解决方案却会如此。一个主要原因是：在探讨需要开发新技术的商业项目时，安全团队并未及时收到邀请，甚至根本不会被邀请。但在这种情况下，安全专业人员也不应该一直等待可能永远都不会收到的邀请。相反，他们必须采取积极措施，确保参与技术对话，理解如何通过安全流程帮助组织实现灵活性并取得成功，同时保障其数据、资产和形象的安全。

2. **安全工作必须对现有架构有效且切实可用。**安全团队不必尝试构建新架构，并在其中采纳旨在提高安全性的新技术解决方案。架构在本质上有其制约性。组织不必为了适应新的安全技术而改变其运营方式，或受已部署技术的限制而无法改变运营方式。“架构超载”的最终结果是，用户将绕过安全架构，降低组织的安全性。此外，如果某项安全技术对用户来说太难理解，且必须由难以找到的专业安全人才进行维护，它对组织而言无甚用处。

3. **安全必须透明且信息充分。**应向用户提供帮助信息，使其了解为何出于安全考虑不能进行某一特定操作。他们还需要知道怎样做能够安全地达到其目的，而不是以完成工作为名绕过安全措施。举个例子，当用户试图访问某个网页时，跳出一条消息：“您的管理员拒绝您访问该网站”，这里没给出任何不能访问该页面的理由。如果将消息改成这样：“访问该网站的请求被拒绝，因为在过去 48 小时内该网站存在多个恶意软件”，用户就会明白这里存在风险，不仅对组织，对他们这些个人用户来说也是一样。此外，安全技术还应为用户提供明确的建议，或引导他们访问适当的资源以及时取得援助，从而帮助他们安全地达成目标。

4. **安全必须具有可视性及适当的行动。**具有开放安全架构的安全解决方案能够允许安全团队判断这些解决方案是否真正有效。安全专业人员也需要工具来自动透视网络，使他们不仅能够查看流量，还能查看构成网络的资产。通过了解安全技术的工作原理，以及在 IT 环境哪些操作是正常的（或不正常的），安全团队可以减少管理工作量，同时更加积极、准确地识别和应对威胁，调整防御。采用这种方法，安全团队能够充分利用更具相关性和针对性的控制措施来在问题的解决过程中提供援助。

5. **必须将安全看成是“人的问题”。**以技术为中心的安全方案并不能提高安全性；事实上，这只会加重问题。技术只是能够增强人们环境安全保护能力的工具而已。安全团队需要教导用户养成安全的习惯，使他们无论身在何处（在办公室、在家、在路上）都能安全地使用技术。这样，当用户感到不对劲时，就会做出正确的决定，或积极主动地寻求援助。加强安全专业人员与用户之间的对话，也有助于帮助用户认识到技术本身并不能保证安全。要应对今日的威胁，人员、流程、技术必须形成统一战线。组织中从上到下的所有用户都付出努力和保持警惕才能实现安全。

思科安全宣言是对变革的一种呼吁。在现实世界中，安全技术、策略和最佳实践应能够提高组织内每一个人的平均安全级别，帮助企业做出下至每个用户的更明智的风险决策。在强大准则的指导下，用户能够清楚地理解为何不能采取某些特定操作，避开安全策略的操作会产生何种影响。

无论是思科安全宣言，还是反映该宣言核心准则的其他理论，都有助于提高用户和安全从业者对于安全的认知：许多威胁可以规避，但危害无法避免，不过我们可以迅速予以补救。我们的目标是在安全事故最终发生时减少解决问题所需的时间，而不仅仅是将精力放在试图避免此类事件上。

关于思科

思科提供贴近现实世界的智能网络安全解决方案和业界最全面的高级威胁防御解决方案组合，这些方案覆盖了最广博的攻击媒介。思科的以防御威胁为中心且运营化的安全方案可以降低复杂性并减少零散片断，同时可在攻击的整个过程中（攻击前、攻击中和攻击后）提供无与伦比的可视性、一致的可控性和高级威胁防御。

借助从海量设备和传感器、公共和私人来源及思科开源社区处取得的遥感勘测数据，来自综合安全智能 (CSI) 生态系统的威胁研究人员将行业领先的威胁情报汇聚到了一起。这相当于每日提取数十亿的网页请求和数以百万计的电子邮件、恶意软件样本和网络入侵数据。

我们先进的基础设施和系统利用这些遥感勘测数据，使机器学习系统和研究人员能够跟踪跨网络、数据中心、终端设备、移动设备、虚拟系统、网络、邮件以及来自云的威胁，以找出威胁的产生根源和爆发范围。我们将由此产生的情报转化为对我们产品和服务的实时保护，并立即交付到全球各地的思科客户手中。

CSI 生态系统由多组不同的特许组织构成：Talos、安全与信任组织、托管威胁防御 (MTD)、安全研究和运营 (SR&O)。

要详细了解思科的以威胁为中心的安全方法，请访问 www.cisco.com/go/security。

附录

更多安全功能基准研究发现

资源

安全预算是否包含在 IT 预算内?

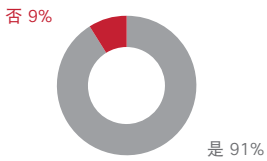
IT 部门成员; n=1720

安全策略、规程和运营

负责安全事务的最高行政职位通常为 CISO 或 CSO。

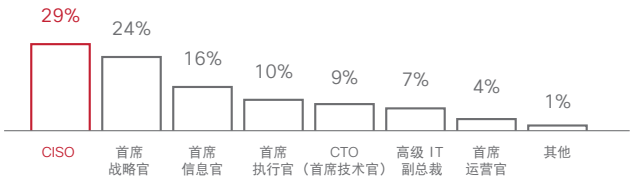
贵组织是否由高管直接负责安全事务

设有明确职位和职责的受访者; n=1603



高管头衔

由高管负责安全事务的受访者; n=1465



与其他行业相比，医疗保健行业较少由高管负责安全事务。

分享报告

近三分之二的受访者称高层管理者将安全视为优先重点。

高管参与 n=1738	SecOps n=797			CISO n=941		
	不赞同/赞同/非常赞同			不赞同/赞同/非常赞同		
我的组织的高层管理者将安全视为优先重点	8%	34%	58%	3%	30%	67%
我的组织的高管团队内包含明确的安全职位和职责	9%	39%	52%	2%	32%	64%
我的组织的高管团队制定有明确的安全计划有效性评估指标	11%	44%	45%	4%	37%	59%

在组织未因安全漏洞而受到公众关注的受访者中，多数非常赞同“我的组织的高层管理者将安全视为优先重点”。

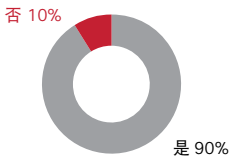
较高比例的受访者鼓励员工参与安全流程。

安全流程 n=1738	SecOps n=797			CISO n=941		
	不赞同/赞同/非常赞同			不赞同/赞同/非常赞同		
鼓励业务部门经理参与安全策略和程序	12%	39%	49%	6%	40%	54%
我的组织能够在安全事件全面爆发前检测到安全漏洞	13%	43%	44%	4%	39%	57%
我的组织鼓励员工报告安全故障和问题	11%	34%	55%	4%	36%	60%
我的组织有清晰易懂的安全流程和程序	13%	39%	48%	4%	37%	59%
我的组织的安全流程使我们能够主动预见并缓解潜在的安全问题	14%	40%	46%	3%	40%	47%
我的组织以定量数据度量和控制安全流程	13%	40%	47%	4%	35%	61%
我的组织优化了自己的安全流程，现在致力于流程改进	12%	42%	46%	4%	36%	60%

中型企业的安全专业人员比大型企业的专业人员更赞同实施安全流程项目。

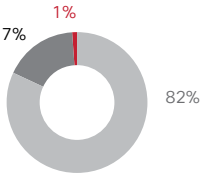
九成的受访者称安全员工会定期接受安全培训 - 通常由安全团队提供。

是否定期向安全人员传达安全意识和/或提供培训计划?
专门负责安全的受访者；n=1726



多久举办一次安全培训?
专门负责安全的受访者；n=1556

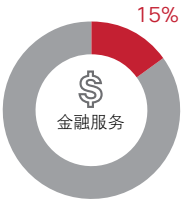
每年 1 次以上 1%
每年不到 1 次/每 2 年 1 次以上 17%
每 2 年不到 1 次 82%



安全培训由谁负责?
安全团队接受培训的受访者；n=1556

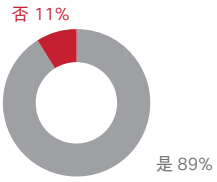
内部安全团队 79%
第三方承包商 38%
人力资源 25%
其他员工 10%
其他 1%

15% 的金融服务专业人士表示未定期举办安全培训。

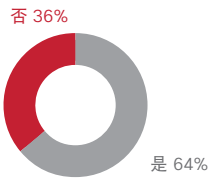


安全员工通常都会参加会议或培训；大约三分之二的受访者称他们加入了安全行业协会。

安全人员是否参加会议和/或外部培训以提高和维持其技能?
专门负责安全的受访者；n=1715

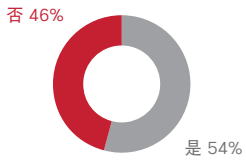


员工是否在安全行业理事会或委员会任职?
专门负责安全的受访者；n=1690

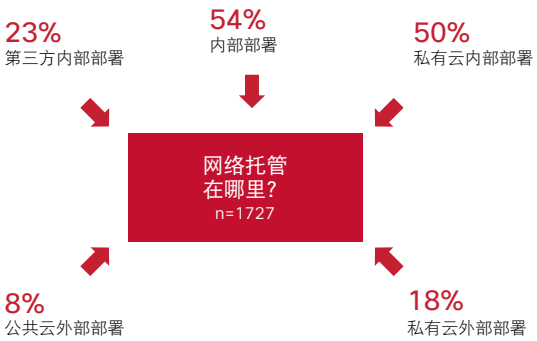


超过一半的受访者表示其组织曾因安全漏洞而受到公众关注。

贵组织是否曾因安全漏洞而受到公众关注?
专门负责安全的受访者；n=1701



组织的网络通常在内部托管；不到十分之一的受访者表示其网络托管在公共云中。



与 CISO 相比，更多的 SecOps 受访者表示其组织采取外部托管形式（包括私有云和公共云）。

复杂度

在许多安全措施完善程度指标方面，不同群体不出所料地呈现出差异...

	低	中低	中	中高	高
公司高管认为安全问题的优先级很高	22%	38%	45%	71%	81%
... 有明确的安全计划有效性评估指标	17%	19%	32%	52%	79%
公司有清晰易懂的安全流程/程序	0%	22%	15%	72%	88%
... 以定量数据度量和控制	0%	17%	33%	65%	76%
... 定期审查安全实践和工具，确保它们最新并且有效	0%	17%	33%	65%	76%
公司在入职、转岗、离职等事务方面有出色的人事安全规程	16%	27%	36%	52%	76%
盘点信息资产并明确地加以分类	17%	26%	40%	58%	73%
我的组织的计算机设备受到很好的保护	17%	21%	41%	63%	80%
各种安全技术很好地融为一体，有效地共同发挥作用	17%	21%	38%	59%	78%
... 公司能够在安全事件全面爆发前检测到安全漏洞	0%	23%	25%	63%	70%

但以下方面差异不大 ...

	低	中低	中	中高	高
由高管直接负责安全事务	85%	91%	88%	93%	93%
公司有覆盖整个组织的正式书面安全战略，并且会定期进行审查	59%	47%	58%	65%	60%
公司遵循标准化的信息安全政策实践，例如 ISO27001	47%	44%	50%	59%	54%

尾注

1. *思科 2014 年中安全报告：*http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027。
2. 有关 CMS 漏洞的详情，请参见“Wordpress Vulnerabilities: Who Is Minding the Store?”（Wordpress 漏洞：谁来看管？），*思科 2014 年中安全报告：*http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027。
3. “Goon/Infinity/RIG Exploit Kit Activity”（Goon/Infinity/RIG 利用漏洞攻击包的活动），思科 IntelliShield：安全活动公告，2014 年 7 月：http://tools.cisco.com/security/center/mviewAlert.x?alertId=34999。
4. *思科 2014 年中安全报告：*http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027。
5. “Cisco Event Response: POODLE Vulnerability”（思科事件响应：POODLE 漏洞），2014 年 10 月 15 日：http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_Poodle_10152014.html。
6. “OpenSSL Heartbleed vulnerability CVE-2014-0160 – Cisco products and mitigations”（OpenSSL Heartbleed 漏洞 CVE-2014-0160 – 思科产品和遏制方案），思科安全博客，2014 年 4 月 9 日：http://blogs.cisco.com/security/openssl-heartbleed-vulnerability-cve-2014-0160-cisco-products-and-mitigations。
7. “JP Morgan and Other Banks Struck by Hackers”（摩根大通等几家银行遭黑客攻击），Nicole Perlroth，*纽约时报*，2014 年 8 月 27 日：http://www.nytimes.com/2014/08/28/technology/hackers-target-banks-including-jpmorgan.html?_r=0；“‘Trojan Horse' Bug Lurking in Vital U.S. Computers Since 2011”（木马漏洞自 2011 年起即潜伏在美国最关键的计算机系统中），Jack Cloherty 和 Pierre Thomas，ABC 新闻，2014 年 11 月 6 日：http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476。
8. “4 Things We Learned from China's 4th Plenum”（从中国四中全会发现的 4 件事），Shannon Tiezzi，*《外交家》杂志*，2014 年 10 月 23 日：http://thediplomat.com/2014/10/4-things-we-learned-from-chinas-4th-plenum/。
9. “Brazil's New Internet Law Could Broadly Impact Online Privacy and Data Handling Practices”（巴西新互联网法规可能大面积影响在线隐私和数据处理方法），*Chronicle of Data Protection*，2014 年 5 月 16 日：http://www.hldataprotection.com/2014/05/articles/international-eu-privacy/marco-civil-da-internet-brazils-new-internet-law-could-broadly-impact-online-companies-privacy-and-data-handling-practices/。
10. “Russian data localization law may now come into force one year ahead of schedule, in September 2015”（俄罗斯数据本地化法规可能提前一年于 2015 年 9 月实施），Hogan Lovells、Natalia Gulyaeva、Maria Sedykh 和 Bret S. Cohen，Lexology.com，2014 年 12 月 18 日：http://www.lexology.com/library/detail.aspx?g=849ca1a9-2aa2-42a7-902f-32e140af9d1e。
11. “GCHQ Chief Accuses U.S. Tech Giants of Becoming Terrorists' 'Networks of Choice'”（英国政府通讯总部负责人指责美国技术巨头成为恐怖分子的“首选网络”），Ben Quinn、James Ball 和 Dominic Rushe，*卫报*，2014 年 11 月 3 日：http://www.theguardian.com/uk-news/2014/nov/03/privacy-gchq-spying-robert-hannigan。
12. “Internet Security Necessary for Global Technology Economy”（互联网安全对全球技术经济不可或缺），Mark Chandler，思科博客，2014 年 5 月 13 日：http://blogs.cisco.com/news/internet-security-necessary-for-global-technology-economy。
13. “Cybersecurity: What the Board of Directors Needs to Ask”（网络安全：董事会需要关注什么），ISACA 和国际内部审计师协会研究基金会，2014 年 8 月：http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask.aspx。
14. “It's Time for Corporate Boards to Tackle Cybersecurity. Here's Why”（企业董事会是时候对网络安全问题采取行动了，我们来告诉你为什么），Andrew Nusca，《财富》杂志，2014 年 4 月 25 日：http://fortune.com/2014/04/25/its-time-for-corporate-boards-to-tackle-cybersecurity-heres-why/。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。

思科和思科徽标是思科和/或其附属公司在美国和其他国家或地区的商标或注册商标。有关思科商标的列表，请访问此 URL： www.cisco.com/go/trademarks 。本文提及的第三方商标均归属其各自所有者。使用"合作伙伴"一词并不暗示思科和任何其他公司存在合伙关系。(1110R)