思科 2016 年度安全报告

执行摘要

安全专业人员必须走出传统模式，重新思考防御策略。

攻击者和防御者都在开发日益精尖的技术和策略。恶意攻击者正在构建强大的后端基础设施，借以发起并支持其攻击活动。网络犯罪分子在继续窃取数据和知识产权的同时，还在不断改进向受害者榨取钱财，以及逃避检测的手段。

《思科 2016 年度安全报告》结合思科安全研究部门的研究、见解和观点，重点说明在攻击者正在采用数量庞大且不断翻新的工具来开展攻击这一趋势下，防御者在检测和阻止攻击方面所面临的挑战。本报告还将介绍 Level 3 Threat Research Labs 等外部专业机构的研究，更深入地阐明当前的威胁趋势。

我们将详细列出思科研究人员整理的数据，以展示随时间推移而发生的变化，就这些数据的意义提供见解，并说明安全专业人员应该如何应对这些威胁。

在本报告中，我们介绍和讨论以下内容：

威胁情报

本节介绍思科研究人员所发现的网络安全领域的一些最引人注目的趋势，以及有关 Web 攻击媒介、Web 攻击方法和漏洞的最新信息。此外，还包括对勒索软件等不断增长的各种威胁的更全面分析。为了对在 2015 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范围的遥感勘测数据。

行业见解

本节探讨影响企业的各种安全趋势，包括加密技术越来越多的使用，以及由此带来的潜在安全风险。我们将分析中小企业在保护自身网络方面存在的弱点。此外，我们还将介绍针对一些特定企业进行的研究，这些企业正在依靠过时、不受支持或寿命已终止的软件来为自身 IT 基础设施提供支持。

安全功能基准研究

本节提供思科第二次安全功能基准研究的结果，此项研究的重点是安全专业人员对其组织内安全状态的看法。通过将 2015 年与 2014 年的调查结果进行比较，思科发现首席安全官和安全运营经理对其安全基础设施是否达到最新水平或能否抵御攻击越来越不自信。但是调查也表明，企业正在加强培训和其他安全流程，以巩固他们的网络。这次调查的结果仅在《思科 2016 年度安全报告》中提供。

展望

本节概述影响安全性的地缘政治格局。我们将讨论两项思科调查的结果，其中一项分析高管对网络安全的担忧，另一项重点分析 IT 决策者们对安全风险和可信度的看法。我们还将介绍思科在降低“检测时间”(TTD) 方面取得的最新进展，并强调转用集成威胁防御架构抵御攻击的价值。

目录

主要发展和发现

主要发展和发现

网络犯罪分子对后端基础设施进行了改进，以更有效且利润更高的方式展开攻击。

- 通过 Level 3 Threat Research Labs 的帮助以及托管服务提供商 Limestone Networks 的合作，思科确定并击败了美国最大的 Angler 漏洞攻击包活动。该威胁活动每天针对 90,000 名受害者发起攻击，每年为幕后的威胁发起者带来数千万美元的收入。
- SSHPsychos（93 组）是思科研究人员观察到的最大的分布式拒绝服务 (DDoS) 僵尸网络之一，在思科与 Level 3 Threat Research Labs 的通力合作下，此僵尸网络已被显著削弱。与前面提到的 Angler 案例研究一样，这次成功也证明了行业协作对战胜攻击者的重要性。
- 恶意浏览器扩展程序可能是企业数据泄露的一个主要原因，也是一个普遍存在的问题。在接受调查的组织中，我们估计受到恶意浏览器扩展程序影响的企业超过 85%。
- 在我们于 2015 年 7 月对一组机构所受影响的分析中，Bedep、Gamarue 和 Miuref 等臭名昭著的僵尸网络依然是僵尸网络命令与控制活动的主要代表。
- 通过分析各种经验证为“已知恶意”的恶意软件，思科发现：大多数 (91.3%) 的恶意软件均使用域名服务 (DNS) 来执行攻击活动。通过对 DNS 查询进行追溯调查，思科发现在客户网络上存在活动的“恶意”DNS 解析器。客户并不知道员工们将这些解析器用作其 DNS 基础设施的组成部分。
- 网络犯罪分子仍继续大肆利用 Adobe Flash 漏洞。但是，软件供应商正努力通过 Flash 技术来降低用户遭受恶意软件攻击的风险。
- 通过对 2015 年的各种趋势进行观察，我们的研究人员认为 HTTPS 加密流量已经达到一个临界点，即将成为互联网流量的主要形式。尽管加密可帮助保护消费者，但也会削弱安全产品的有效性，使安全业界更加难以跟踪威胁。一些恶意软件会通过大量不同的端口发起加密通信，使得挑战进一步加剧。
- 恶意攻击者开始利用已被入侵的基于流行 Web 开发平台 WordPress 创建的网站进行犯罪活动。他们可在这些网站上封送服务器资源并逃避检测。

- 基础设施老化不断加剧，导致组织愈加容易受到入侵。我们分析了互联网上 115,000 个思科®设备，发现在我们抽查的设备中，有 92% 的设备正在运行存在已知漏洞的软件。此外，这项分析所涉及的现场思科设备中，有 31% 的设备已经“终止销售”，8% 的设备“寿命已终止”。
- “思科 2015 年安全功能基准研究”显示，在 2015 年，安全高管对其安全工具和流程的信心不如 2014 年。例如在 2015 年，59% 的组织认为他们的安全基础设施“达到了最新水平”。而在 2014 年，持有这种看法的组织占到 64%。但是，他们对安全越来越多的担忧也在促使他们改善防御。
- 基准研究表明，中小企业使用的防御方案少于大型企业。例如，在 2015 年，48% 的中小企业表示已使用 Web 安全方案，而在 2014 年这一比例为 59%。此外，在 2015 年，29% 的中小企业表示已使用修补和配置工具，而在 2014 年这一比例为 39%。这方面的不足会使中小企业的企业客户面临风险，因为攻击者攻击中小企业的网络会更容易。
- 从 2015 年 5 月开始，思科已经将网络中已知威胁的检测时间 (TTD) 平均值降至大约 17 小时，不到一天。这远远低于业界当前的 TTD 估计值，即 100 至 200 天。

目标明确:
现代网络犯罪分子将赚钱作为首要目标

目标明确：现代网络犯罪分子将赚钱作为首要目标

以前，很多网络犯罪分子潜伏于互联网中。他们仅对企业网络进行短暂入侵并发起漏洞攻击，以此尝试躲过检测。如今，一些胆大妄为的网络犯罪分子已开始入侵合法的在线资源。他们会大量消耗服务器容量，窃取数据，甚至挟持网络受害者的信息，然后向其索取赎金。

这些攻击活动俨然已将防御者和攻击者之间的战争急剧升级。如果攻击者可以在网络上发现更多可以利用的信息源，那么所造成的影响将呈指数级增长。

在本报告中，思科安全研究人员重点介绍威胁发起者用于构建稳定的基础设施以实施更强大、更有效的攻击活动的策略。攻击者不断采用更高效的方法以提升收益，很多攻击者特别关注利用服务器资源。

勒索软件的激增就是一个最好的例证（请参阅**第 10 页**）。勒索软件为犯罪分子提供了一种直接向用户榨取更多金钱的简单方法。通过开展攻击活动，在只有极少阻碍甚至没有任何阻碍的情况下每天攻击数万用户，攻击者所获得的“报酬”丰厚得让人震惊。除了开发更好的方法来牟取利益，攻击者还开始侵占合法资源，作为发起攻击的跳板。

某些勒索软件变体的创建者以及其他漏洞攻击的开发者正在将流量切换至遭受过黑客攻击的 WordPress 网站，作为躲避检测和使用服务器空间的一种方法（请参阅**第 33 页**）。SSHPsychos 是思科研究人员迄今为止发现的最大的僵尸网络之一，其作案者在标准网络上运行僵尸网络，几乎没有什么干扰，直到思科和 Level 3 Threat Research Labs 携手合作说服运营商阻止此僵尸网络创建者的流量，一举将其击败。

威胁情报

威胁情报

思科在收集并分析了全球范围的遥感勘测数据的基础上编制了这份报告。我们针对已发现的威胁（如恶意软件流量）进行持续研究和分析，能够帮助人们了解未来可能出现的犯罪行为，且有助于检测威胁。

专题报道

思科借助行业协作击败影响广泛且盈利性强的漏洞攻击包和勒索软件攻击活动

Angler 漏洞攻击包是市场上使用量最大而且最有效的漏洞攻击包之一。它与多个臭名昭著的恶意广告和勒索软件攻击活动有关， 是导致勒索软件活动总体呈激增态势的一个主要因素，我们的威胁研究人员最近几年来一直在密切监控勒索软件活动。犯罪分子使用勒索软件将用户文件加密，然后向用户索要赎金（通常在 300 美元到 500 美元不等），再向用户提供解密密钥。

正如《思科 2015 年年中安全报告》中所指出的，比特币等加密货币和 Tor 等匿名网络使犯罪分子可以更容易进入恶意软件市场并快速开始获得收入。恶意软件的泛滥与两大有利因素相关：一是威胁发起者只需执行少量维护操作，二是由于用户直接向攻击者支付加密货币，攻击者可以很快取得收入。

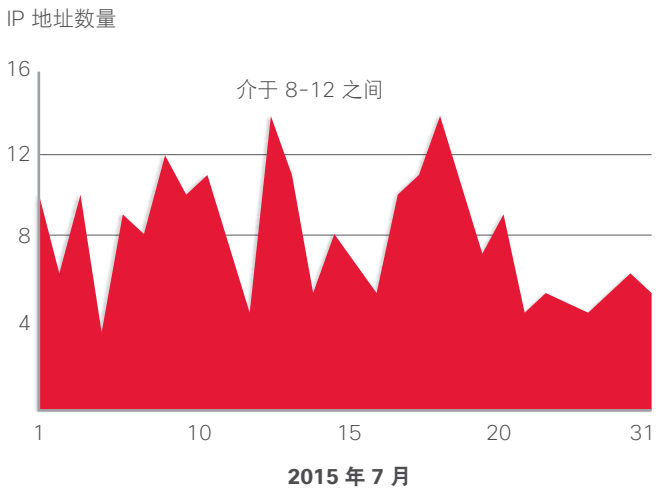
通过对 Angler 和相关勒索软件趋势进行研究，思科已经确定一些漏洞攻击包操作者将大量全球代理服务器用于 Agler，而这些服务器由 Limestone Networks 运营。这种使用服务器的手法有力地证明了我们的研究人员在近来的影子经济中持续观察到的另一种趋势：威胁发起者混合使用合法资源和恶意资源混合来执行攻击活动。

分享

在这种情况下，支持 Angler 的 IP 基础设施规模不是很大。每天处于活动状态的系统数量通常为 8 到 12 个之间。大多数系统仅在某一天处于活动状态。图 1 显示思科在 2015 年 7 月观察到的唯一 IP 地址的数量。

思科发现 Angler 操作者实际上在以线性方式滚动 IP 地址，以隐藏其威胁活动，防止其牟利活动出现任何中断。

图 1. 2015 年 7 月按日期划分的 Angler IP 地址的数量



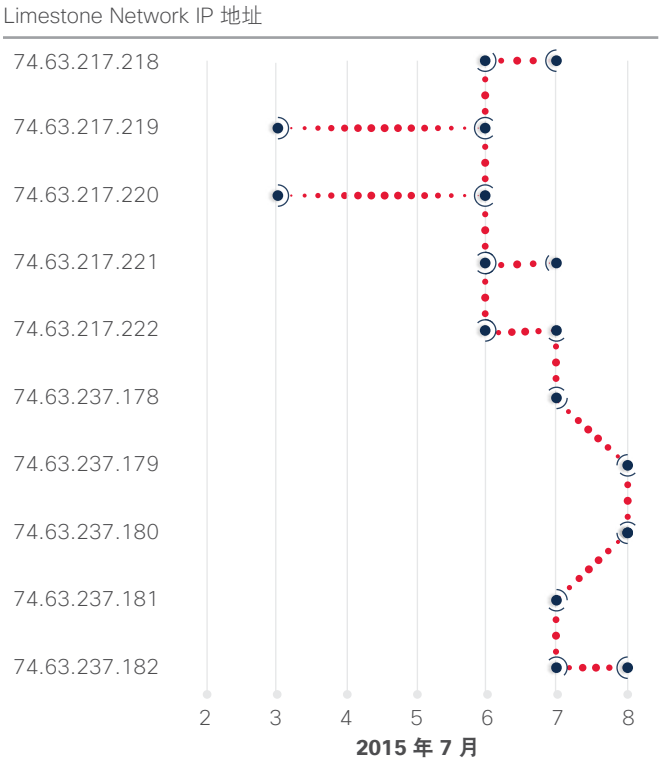
来源：思科安全研究部门

如图 2 所示，Angler 从某个 IP 地址（此处为 74.63.217.218）开始。当系统攻击用户并遇到“干扰”（防御程序开始执行检测）时，攻击者会切换至邻近的 IP 地址 (74.63.217.219)。这种活动在单个托管服务提供商提供的 IP 空间近乎连续的地址块中一直持续。

思科分析了这些 IP 信息，以确定其自治系统编号 (ASN) 以及与这些 IP 地址相关的提供商。我们确定与 Angler 相关的大多数流量来自两个合法托管服务提供商：Limestone Networks 和 Hetzner 运营的服务器（图 3）。在 7 月一个月内，他们在总流量中所占的比例接近 75%。

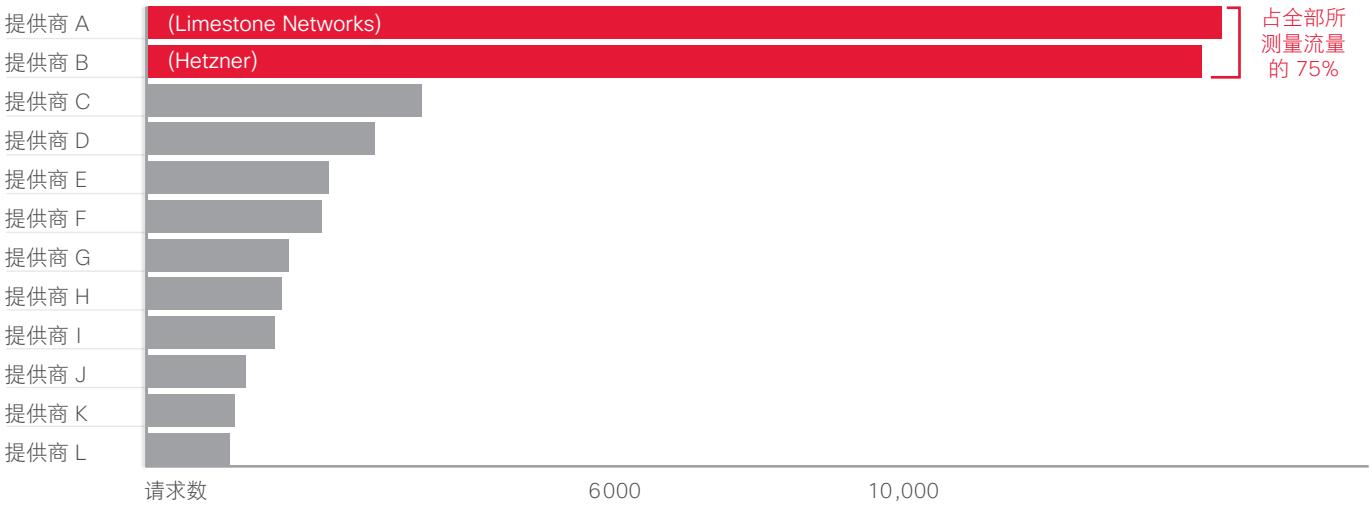
思科首先联系了 Limestone Networks，结果发现此提供商承载了全球最多的 Angler。Limestone 公司欣然同意对此给予合作。由于攻击者使用虚假的姓名和信用卡随机分批向该公司购买价值数千美元的服务器，该公司每个月都要处理大量信用卡退单。

图 2. 支持 Angler 的低 IP 基础设施



来源：思科安全研究部门

图 3. 2015 年 7 月按提供商划分的 Angler HTTP 请求



来源：思科安全研究部门

攻击者购买服务器的方式使得该公司难以将欺诈活动与单个行为人关联。例如，攻击者可能在某天购买三四台服务器，然后第二天用不同的姓名和信用卡购买三四台服务器。这样，当防御者发现了受入侵的服务器并且使之离线时，攻击者仍可以从一个 IP 地址切换至下一个 IP 地址。

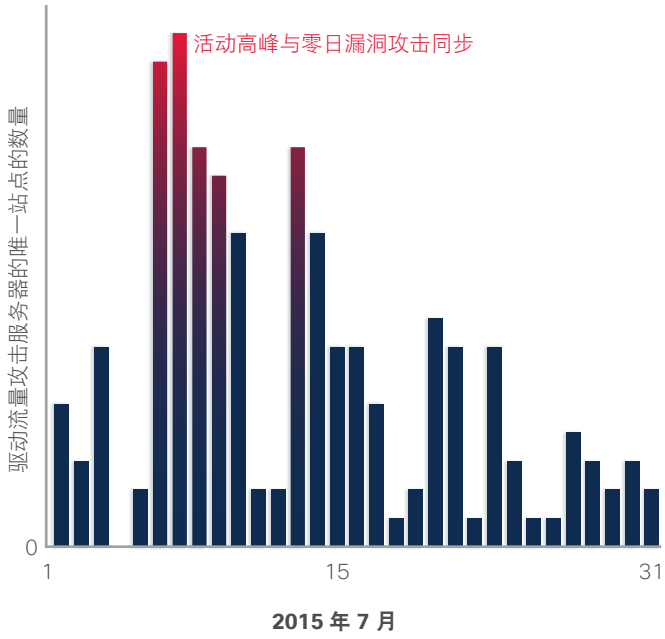
为了调查此活动，思科向 Level 3 Threat Research Labs 和 OpenDNS（思科旗下公司）寻求帮助。Level 3 Threat Research Labs 能够提供更全面的全球性威胁见解，让思科能够更深入了解威胁范围及其在高峰状态下的影响范围。同时，OpenDNS 针对与威胁相关的域活动提供了独特呈现方式，让思科可以更全面了解攻击者如何采用域遮蔽等技术。

然后，思科威胁研究人员具体调查了用户如何遇到 Angler 并继而感染恶意负载。研究人员观察发现到一些流行网站通过恶意广告将用户重定向至 Angler 漏洞攻击包。这些虚假广告被投放到数百个主要的新闻、房地产和流行文化网站上。这些类型的网站在安全业界通常被视为“已知可信”网站。

此外，思科威胁研究人员还发现无数看似毫无关系的小网站也在执行同类重定向操作，包括美国某家乡村报纸上刊发的某个人的讣告，也被嵌入重定向链接。后面这一策略很可能是针对老年人而设计的。老年人这一群体通常更可能使用 Microsoft Internet Explorer 等默认网络浏览器，而且他们了解需要定期修补 Adobe Flash 漏洞的可能性更小。

这种 Angler 活动的另一个显著特点是其唯一引用站点数量之大及其使用频率之低（图 4）。我们发现了超过 15,000 个唯一站点将用户推送至 Angler 漏洞攻击包，其中 99.8% 的站点使用频率低于 10 次。因此，大多数引用站点仅在很短时间内处于活动状态，然后在对若干用户发起针对性攻击之后就被删除。在我们 2015 年 7 月的分析中，我们注意到其活动高峰与各种 Hacking Team 零日漏洞（CVE-2015-5119、CVE-2015-5122）同步。[1]

图 4. 2015 年 7 月按日期划分的唯一引用站点



来源：思科安全研究部门

思科确定通过这种特殊操作传输的 Angler 负载中大约 60% 都是在传输某种类型的勒索软件变体（大多数是 Cryptowall 3.0）。其他类型的负载包括 Bedep，这是安装点击欺诈攻击活动恶意软件常用的一种恶意软件下载程序。（请参阅“浏览器感染：传播广泛并且是数据泄露的一个主要原因”**[第 16 页]**。）这两种类型的恶意软件都旨在帮助攻击者从受攻击的用户身上非常快速、轻松甚至毫不费力地获取大量收入。

[1] “Adobe 修复 Hacking Team 的 Flash 播放器零日攻击”，作者：Eduard Kovacs，*SecurityWeek*，2015 年 7 月 8 日 **http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day**。

Angler 收入

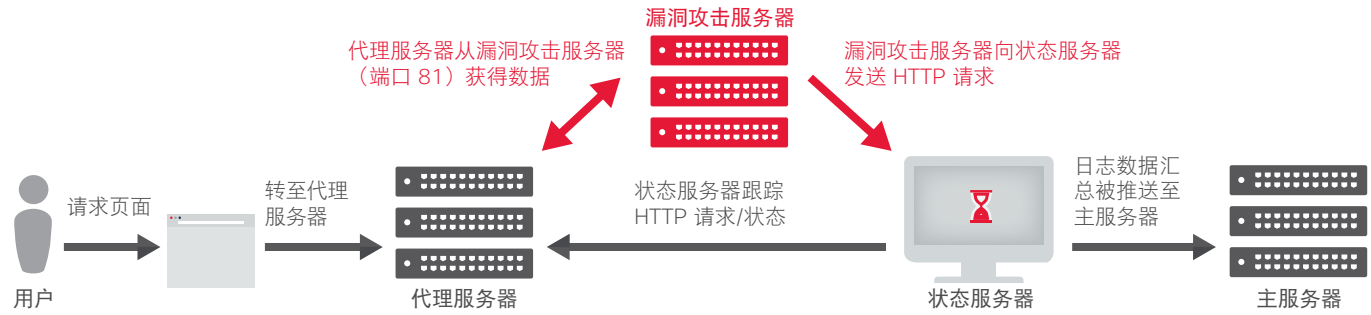
来源：思科安全研究部门

根据思科的研究，在这一特定攻击活动中承担约一半 Angler 漏洞攻击包活动的主要攻击者，平均每天攻击多达 90,000 名受害者。以此估算，此攻击活动使攻击者每年可获得 3,000 万美元以上的收入。

分享

据推测，在 Hetzner 之外的网络也会达到类似的成功率。这意味着在思科执行观察分析这一时段，威胁发起者利用 Limestone Networks 和 Hetzner 服务器发起了约一半的全球 Angler 攻击活动。思科研究人员估计此项攻击操作每年能够产生 6,000 万美元的总收入。

图 5. Angler 后端基础设施



来源：思科安全研究部门

思科同时发现用户连接的服务器实际上并没有承载任何恶意 Angler 活动。它们只是充当管道。用户会进入重定向链并提交登陆页面的 GET 请求，这样就会登录到代理服务器。代理服务器会将流量路由至某个不同国家/地区或不同提供商的漏洞攻击服务器。在我们的研究中，我们发现一个漏洞攻击服务器会与多个代理服务器关联。（请参见图 5。）

思科已明确有一个状态服务器在处理运行状况监控等任务。状态服务器监控的每个代理服务器都有一对唯一 URL。如果路径受到查询，状态服务器会返回 HTTP 状态代码“204”消息。攻击者可以唯一标识每个代理服务器，并确保其不仅在运行，而且未受到防御者干预。利用另一个 URL，攻击者可以从代理服务器收集日志并确定其网络运行效率。

行业协作是思科能够调查 Angler 漏洞攻击包活动的一个关键要素。思科通过合作最终停止了重定向至美国某个运营商的 Angler 代理服务器，并且让人们开始注意这个每天都在影响数千用户的高度复杂的网络犯罪活动。

分享

思科与 Limestone Networks 紧密合作，在新服务器上线时进行识别，然后进行密切监控，确保记录下这些服务器。不久，攻击者就远离了 Limestone Networks，随后全球 Angler 活动也有所减少。

有关思科如何阻断 Angler 漏洞攻击包所产生的大量国际性收入流的更多信息，请参阅思科安全博客文章“**威胁聚焦：思科 Talos 挫败大规模国际漏洞攻击包仅仅利用勒索软件每年产生 6,000 万美元收入**”。

行业合作帮助挫败互联网最大的 DDoS 僵尸网络之一

集成威胁防御技术通常可以在大规模攻击影响企业网络之前予以制止。但是，在很多情况下，击溃一次潜在的大规模攻击不仅需要技术防御，而且需要运营商、安全供应商和行业团体之间相互合作。

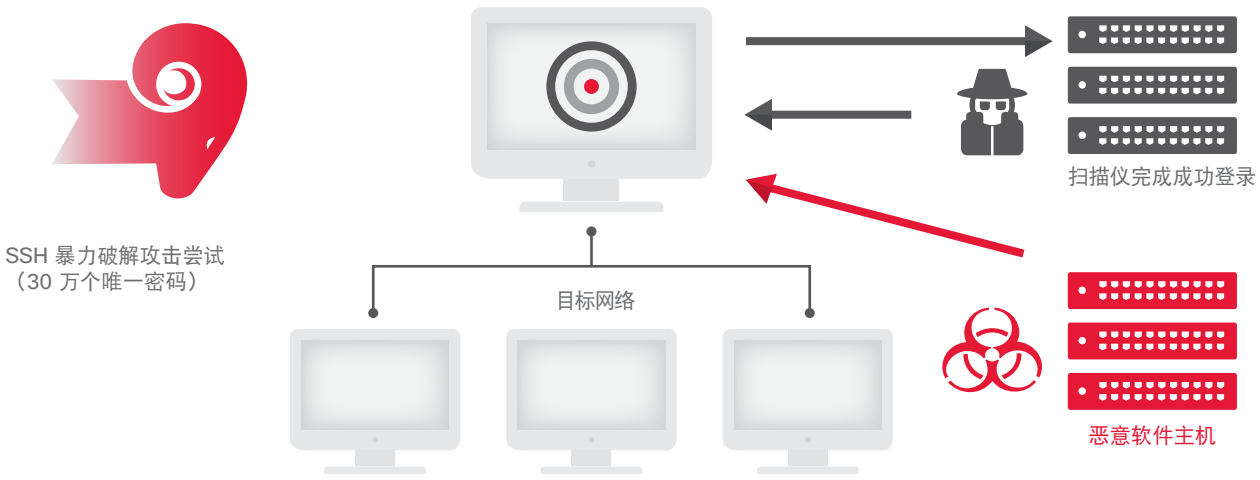
随着犯罪分子越来越注重以牟利为目的开展活动，技术行业需要通过更好的合作来消灭犯罪攻击活动。SSHPsychos（又称为 93 组）是思科安全研究人员曾观察到的最大 DDoS 僵尸网络之一，经过思科与 Level 3 Threat Research Labs 的合作，这一僵尸网络已经被显著削弱。

独特的威胁

出于一些原因，SSHPsychos DDoS 网络可被视为一种独特的威胁。因为它可以利用互联网上分布的数万台设备，所以能够发起无法按设备逐一解决的分布式拒绝服务 (DDoS) 攻击。在这种情况下，攻击者就开始利用涉及安全外壳 (SSH) 流量的暴力破解攻击创建僵尸网络（图 6）。SSH 协议用于允许安全通信，通常用于系统远程管理。根据思科和 Level 3 的分析，有时候，SSHPsychos 占到了全球所有互联网 SSH 流量的 35% 以上（图 7）。

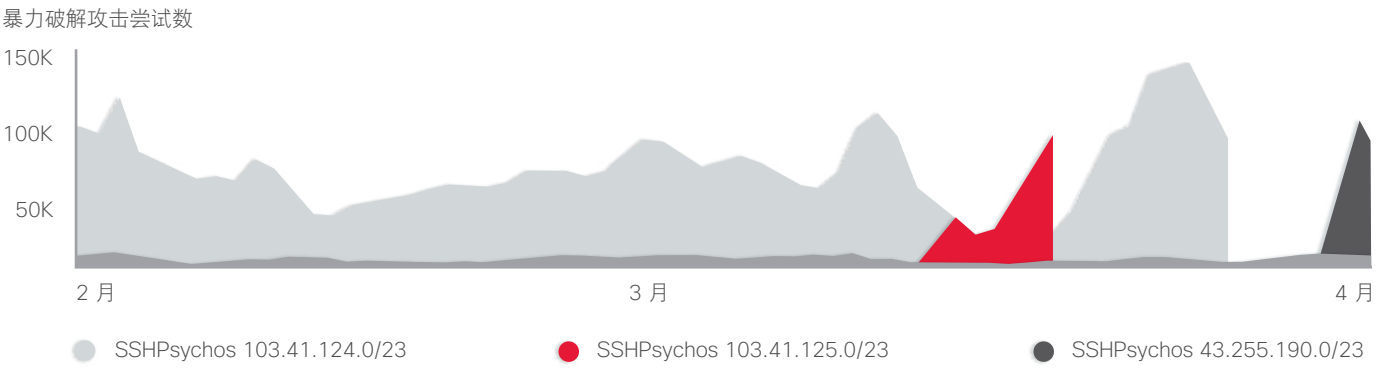
SSHPsychos 可在中国和美国两个国家运行。这种暴力破解登录尝试使用 300,000 个密码，源自位于中国的某个托管服务提供商。当攻击者能够通过正确猜测的根密码登录时，暴力破解攻击就停止了。24 小时后，攻击者会从一个美国 IP 地址登录并在受影响设备上安装 DDoS Rootkit。这显然是减少引起网络管理员怀疑的一种策略。僵尸网络的目标不断变化，但是在很多情况下都是大型互联网服务提供商 (ISP)。

图 6. SSHPsychos 使用暴力破解攻击



来源：思科安全研究部门

图 7. SSHPsychos 在高峰期间占全球互联网流量的 35%



来源：思科安全研究部门

与安全专家协作

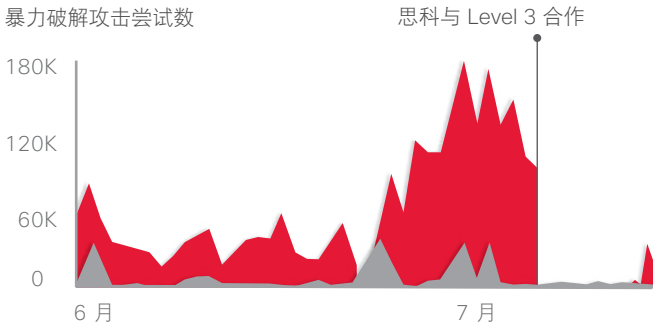
由于 DDoS 网络规模很大，我们的研究人员认为其造成的损失将难以控制。我们必须与能够有效地从互联网上消除暴力破解团体的组织合作。但是，主干网运营商都对过滤客户的内容犹豫不决。

思科于是联系了 Level 3 Threat Research Labs。Level 3 分析了被认为存在 SSHPsychos 的网段或 IP 地址范围的流量 (103.41.124.0/23)。其确认往返该地址的流量都是不合法的。他们在自己的网络中将这些网络流量进行空路由。然后，他们联系了相关域的运营商，要求他们删除这些网络流量。

这项工作的效果立竿见影（图 8）。原网络几乎没再出现任何新活动。然而，在网 43.255.190.0/23 上的一个新网络出现了大量 SSH 暴力破解攻击流量。其行为与 SSHPsychos 的相关行为相同。在突然再度出现这种类似 SSHPsychos 的流量之后，思科和 Level 3 决定对 103.41.124.0/23 以及新网段 43.255.190.0/23 采取行动。

消除 SSHPsychos 使用的网段并未永久地禁止 DDoS 网络，但是明显削弱了其创建者执行其运营活动的能力，至少暂时阻止了 SSHPsychos 传播至其他新设备。

图 8. SSHPsychos 流量在干预之后显著下降



来源：思科安全研究部门

因为网络犯罪分子会构建大型攻击网络，安全行业在面临 SSHPsychos 之类的威胁时必须探索各种协作方式。当网络犯罪分子在旨在仅承载合法流量的网络上发起漏洞攻击时，顶级域提供商、ISP、托管服务提供商、DNS 解析运营商和安全供应商再也不能袖手旁观。换句话说，当犯罪分子开始明目张胆地传输恶意流量时，整个行业都必须清除连接这些合法网络的恶意通道。

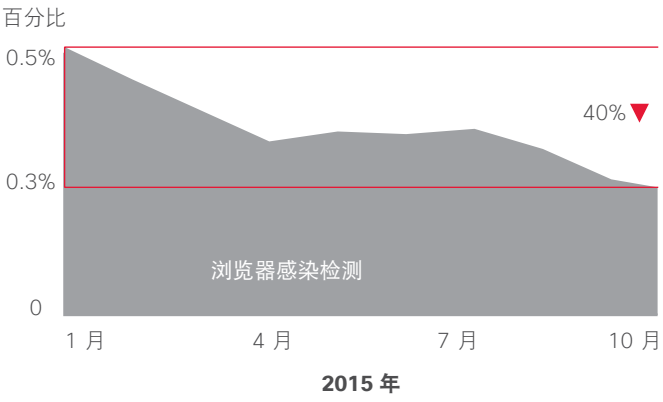
要了解关于思科和 Level 3 Threat Research Labs 应对 SSHPsychos 威胁的更多信息，请阅读思科安全博客文章“**威胁聚焦：SSHPsychos**”。

浏览器感染：传播广泛并且是数据泄露的一个主要原因

安全团队通常将浏览器插件视为严重性较低的一种威胁。然而，他们应该更加注重监控这些插件，以便可以尽快确定这些类型的感染并进行补救。

这个问题之所以如此紧迫，是因为我们的研究发现，浏览器感染的传播速度远远超出很多组织的想象。从 2015 年 1 月至 10 月，我们检查了 26 个系列的恶意浏览器插件（图 9）。纵观这几个月浏览器感染的模式，其感染数量似乎总体上呈下降趋势。

图 9. 2015 年 1 月到 10 月的浏览器感染情况



来源：思科安全研究部门

但是，这种趋势只是表面现象。这几个月来 HTTPS 流量大增，由于加密导致无法查看 URL 信息，使得我们难以确定通常与我们所跟踪的 26 个系列的浏览器相关的威胁指标。（有关加密及其给防御者带来的挑战的更多信息，请参阅“加密：日益发展的趋势 - 也是防御者面临的挑战”[**第 30 页**]。）

恶意浏览器扩展程序会盗取信息，而且会成为数据泄露的主要原因。每当用户使用被入侵的浏览器打开一个新网页时，恶意浏览器扩展程序都会收集数据。它们不仅会窃取用户访问的每个内部或外部网页的基本详细信息， 而且还会收集 URL 中嵌入的高度敏感的信息。这些敏感信息可能包括用户凭证、客户数据和关于组织内部 API 和基础设施的详细信息。

多功能恶意浏览器扩展程序通过软件捆绑包或广告软件传输。它们被设计为通过多种方式攻击用户，牟取暴利。在一个感染的浏览器上，恶意浏览器扩展程序会导致用户点击陈列式广告或弹窗等恶意广告。它们还可以通过引诱用户点击已感染链接或下载在恶意广告中遇到的已感染文件，传播恶意软件。它们可以劫持用户的浏览器请求，然后将恶意网页注入搜索引擎结果页面。

在我们抽查的 45 家公司中，我们发现在我们执行观察的每个月中，超过 85% 的组织都受到了恶意浏览器扩展程序的影响，这项发现突显了这些恶意活动的规模之大。由于受感染的浏览器通常会被视为相对较小的威胁，因此会持续数天甚至更长时间在未被检出或未予解决的情况下继续运行，从而为攻击者提供了更多的时间和机会来执行其攻击活动（请参阅“检测时间：不断缩短空档期的竞赛”[**第 60 页**]）。

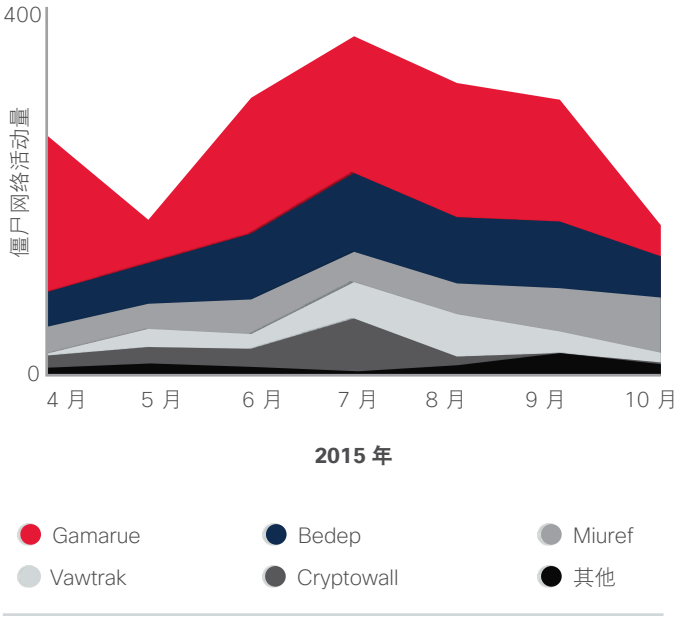
因此，我们建议安全团队应花时间利用更多资源来监控此风险，以及考虑日益增多的自动化功能，以帮助确定威胁优先级。

僵尸网络命令和控制：全球概况

僵尸网络是感染了恶意软件的计算机网络。攻击者可以将这些计算机作为一个整体进行控制并命令他们执行特定任务，例如发送垃圾邮件或发起 DDoS 攻击。这些年来，其规模和数量都一直在增长。要更好地从全球范围了解当前的威胁格局，从 2015 年 4 月至 10 月，我们分析了 121 家公司的网络，寻找八大常见僵尸网络的踪迹。我们将数据归一化，以提供僵尸网络活动的总体概况信息（图 10）。

我们发现在此期间，Gamarue（一种模块化、多功能信息窃取恶意软件，已经横行多年）是最常见的命令和控制威胁。

图 10. 各项威胁的增长（感染用户的比例）



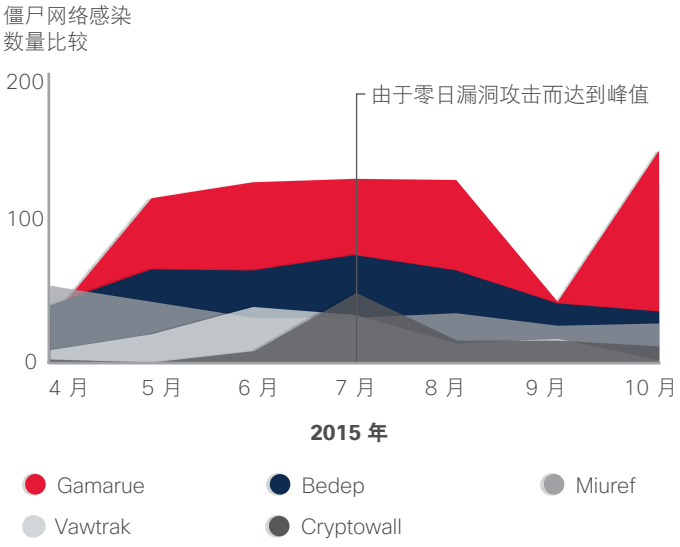
来源：思科安全研究部门

7 月份我们发现与勒索软件 Cryptowall 3.0 相关的感染数量出现显著高峰。这主要是 Angler 漏洞攻击包导致的，已知其会投放 Cryptowall 负载。据《思科 2015 年年中安全报告》所报告，Angler 和其他漏洞攻击包的创建者都很快利用了 Adobe Flash 的“修补缺口”，即 Adobe 发行更新的时间与用户实际进行升级的时间之间的间隔。[2] 思科威胁研究人员认为 2015 年 7 月出现的威胁高峰是 Flash 零日漏洞 CVE-2015-5119 导致的，此漏洞是 Hacking Team 泄露的一部分。[3]

Angler 漏洞攻击包还传输 Bedep 特洛伊木马，用以执行点击欺诈攻击活动。7 月该威胁的爆发量也略有上升（图 11）。

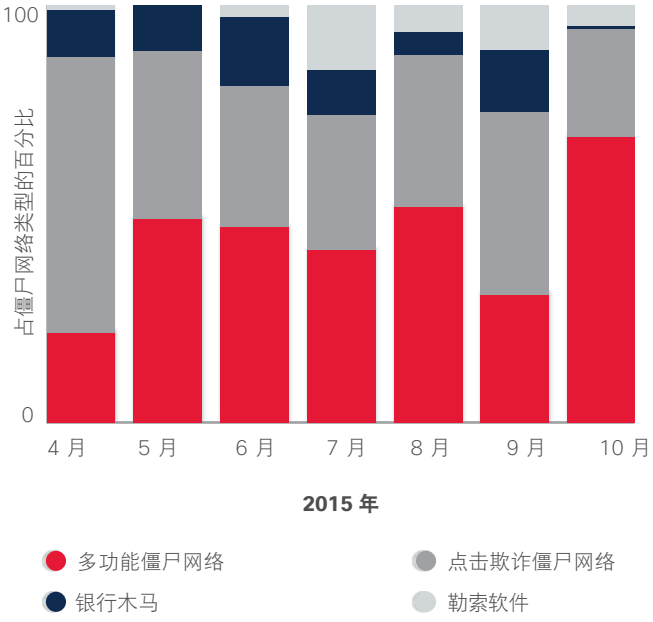
Bedep、Gamarue 和 Miuref（可执行点击欺诈的另一特洛伊木马和浏览器劫持程序）占我们所分析的用户群所遭受的僵尸网络命令和控制活动的 65% 以上。

图 11. 根据感染用户数量的每月威胁覆盖率



来源：思科安全研究部门

图 12. 根据威胁类别的每月威胁覆盖率



来源：思科安全研究部门

Bedep 感染的比例在我们分析的时间段内保持相对稳定。然而，我们发现 Miuref 感染看似有所减少。我们认为其原因是 HTTPS 流量增加，帮助隐藏了 Miuref 的感染指标。

图 12 显示引起我们监控期间大多数感染的僵尸网络的类型。Gamarue 和 Sality 等多功能僵尸网络是罪魁祸首，其次是点击欺诈僵尸网络。第三个是银行木马，监控表明此类威胁虽然由来已久，但是仍然很广泛。

[2] 思科 2015 年年中安全报告：**http://www.cisco.com/web/offers/lp/2015-midyear-security-report/index.html**。
[3] “Adobe 修复 Hacking Team 的 Flash 播放器零日攻击”，作者：Eduard Kovacs，*SecurityWeek*，2015 年 7 月 8 日：**http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day**。

消除 DNS 盲点：将 DNS 用于命令和控制的攻击

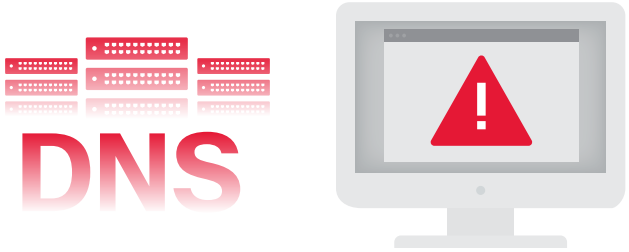
思科对于经验证为“已知恶意”的恶意软件的分析发现大多数 (91.3%) 的恶意软件都使用域名服务 (DNS) 来执行以下三种活动之一：

- **获得命令和控制**
- **窃取数据**
- **重定向流量**

为得出这一比例，我们从我们拥有的各种沙盒发掘了各种样本行为。我们从要分析的样本中删除了经确定不以任何方式使用 DNS 或仅将其用于执行互联网“运行状况检查”的恶意软件。剩余的恶意软件都在使用 DNS 连接经验证为恶意或被视为可疑的站点。

尽管攻击者依靠 DNS 帮助进一步开展恶意软件攻击活动，但是很少有公司会出于安全目的监控 DNS（或出于任何原因而监控 DNS）。这种缺乏监控的情况使得 DNS 成为攻击者的一个理想渠道。根据我们最近执行的一项调查（请参阅图 13），68% 的安全专业人员都报告他们的组织不监控来自递归 DNS 的威胁。（递归 DNS 名称服务器向请求的主机提供预期域名的 IP 地址。）

图 13. 监控来自递归 DNS 的威胁



来源：思科安全研究部门

为什么 DNS 是如此之多组织的安全盲点？ 一个主要原因是安全团队和 DNS 专家通常在公司的不同 IT 团队工作，他们并不经常沟通。

但是，他们应该经常沟通。监控 DNS 对于发现和控制已在将 DNS 用于前述三项活动中任一活动的恶意软件感染很重要，也是设计其他可以用于进一步调查攻击（包括从确定支持攻击的基础设施的类型到发现其来源）的要素的重要第一步。

不过，监控 DNS 不仅要求安全团队和 DNS 团队之间进行协作， 而且要求采用适当的技术和专业知识进行相关性分析。（有关更多见解，请参阅“思科借助行业协作击败影响广泛且盈利性强的漏洞攻击包和勒索软件攻击活动”[**第 10 页**]，了解 OpenDNS 如何帮助思科对 Angler 漏洞攻击包使用的 IP 获得更大域可见性。）

追溯性 DNS 分析

思科对 DNS 查询和后续 TCP 与 UDP 流量的追溯调查可确定多种恶意软件来源。其中包括命令与控制服务器、网站和分发点。追溯性调查还可利用来自威胁列表的情报、社区威胁报告、所观察的网络威胁趋势和对客户行业面临的独特漏洞的了解，检测高风险威胁内容。

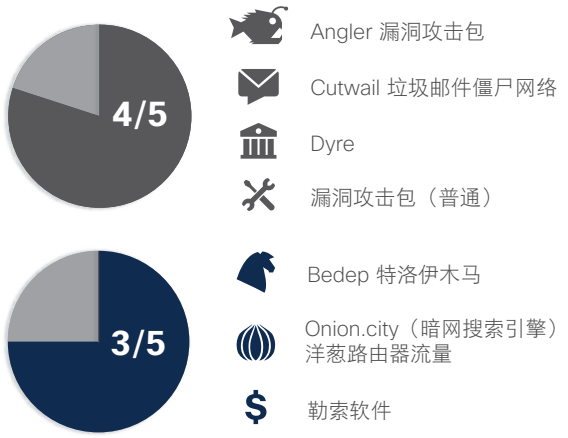
我们的追溯性报告可识别高级持续性威胁 (APT) 行为常用的“低带宽慢速”数据窃取尝试，在很多情况下传统威胁检测技术都无法捕获此类威胁。该分析的目标是在庞大数量的出站通信流量中识别出异常情况。这种“自内而外”的方法可以找出那些可能被忽略的潜在数据威胁和破坏性网络活动。

这是我们在客户端网站上发现正在使用的“恶意”DNS 解析器的方法。客户并不知道员工们将这些解析器用作其 DNS 基础设施的组成部分。无法有效管理和监控 DNS 解析器的使用可能导致恶意行为，例如 DNS 缓存投毒和 DNS 重定向。

除了发现和识别恶意 DNS 解析器之外，追溯性调查还可以发现客户网络中的以下问题：

- **在第三方垃圾邮件和恶意软件黑名单上发现客户地址空间**
- **针对已知 Zeus 和 Palevo 命令与控制服务器的客户地址空间信标**
- **活跃的恶意软件攻击活动，包括 CTB-Locker、Angler 和 DarkHotel**
- **可疑活动，包括使用 ToR、电子邮件自动转发和在线文档转换**
- **针对在中国注册域的渗透性 DNS 隧道传输**
- **DNS“误植域名”[4]**
- **绕过客户信任的 DNS 基础设施的内部客户**

通过分析多个垂直行业的一系列思科定制威胁情报客户示例，我们还发现了以下类型恶意软件及其出现于所调查的总客户数量中的相应比例：



[4] 误植域名是指注册与现有域名相似域名的行为；这是攻击者用于对无意中输错预期域名的用户发起针对性攻击的一种策略。

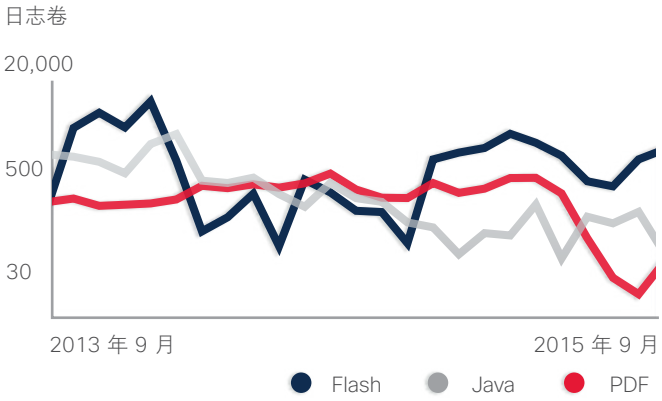
威胁情报分析

Web 攻击媒介

ADOBE FLASH：终将被放弃

尽管在刚过去的一年里，Flash 恶意软件的总量有所下降（请参阅下一节**“Adobe Flash 和 PDF 内容趋势”**），但它仍然是漏洞攻击开发者钟爱的一种工具。事实上，2015 年，Flash 恶意软件并未出现明显增加或减少的趋势（图 14）。在一段时间内，Flash 相关的恶意软件可能继续担任主要漏洞媒介：值得注意的是，Angler 漏洞攻击包作者就主要以 Flash 漏洞为目标。

图 14. 攻击媒介共享，2 年的比较



来源：思科安全研究部门

行业内对从浏览体验中删除 Adobe Flash 的要求导致网络上 Flash 内容数量减少（请参阅下一节**“Adobe Flash 和 PDF 内容趋势”**）。这类似于近些年 Java 内容所发生的情况，那次变化使 Java 恶意软件数量呈稳定下降趋势（实际上，Angler 作者甚至已不再考虑采用 Java 漏洞攻击）。同时，PDF 恶意软件数量保持相对平稳。

Microsoft Silverlight 作为攻击媒介的情况也有所减少，因为很多供应商都停止对 Silverlight 用于与浏览器集成的 API 提供支持。随着许多公司开始采用基于 HTML5 的技术，他们都摒弃了 Silverlight。Microsoft 已经表示近期不会推出新版本的 Silverlight，而且现阶段也只发布安全相关的更新。

ADOBE FLASH 和 PDF 内容趋势

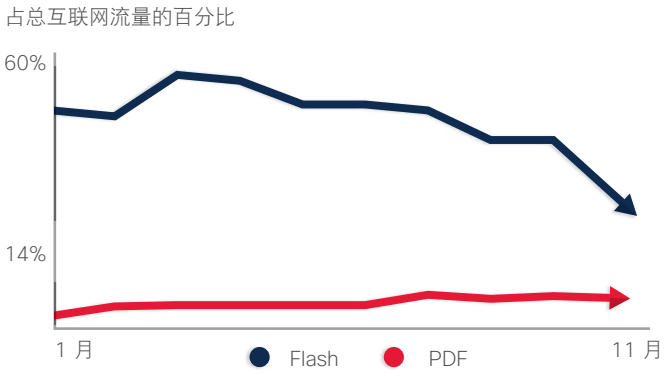
思科研究人员注意到网络中 Adobe Flash 内容数量总体上有所下降（图 15）。亚马逊、谷歌和互联网空间的其他巨头最近所采取的行动是 Flash 内容减少的一个原因。这些公司或者不再接受使用 Flash 的网络广告，或者阻止这种广告。

与此相对比，PDF 内容在过去一年中保持相对稳定，而且可能继续保持稳定。但是，它已有一段时间不再是主要 Web 攻击媒介。

Flash 内容的数量可能会继续下降，而且近期甚至发生加速下降，因为 Adobe 已经宣布将淘汰 Flash。[5] 不过，Flash 内容可能还需要一段时间才会逐渐消失。Flash 已经嵌入到 Google Chrome、Microsoft Internet Explorer 和 Microsoft Edge 等浏览器中，而且在游戏和视频内容等网络内容中仍广泛被使用。

然而，接下来几年内，随着新技术（例如 HTML5 和移动平台）的采用，Java、Flash 和 Silverlight 等 Web 攻击可利用媒介的长远趋势已越来越清晰。随着时间的推移，它们将不再那么风行一时。因此对只顾赚钱的攻击者而言，将它们作为攻击媒介的吸引力可能会下降，攻击者关注的是让他们轻松攻击大量用户并快速获得收入的媒介。

图 15. Flash 和 PDF 占总流量的百分比

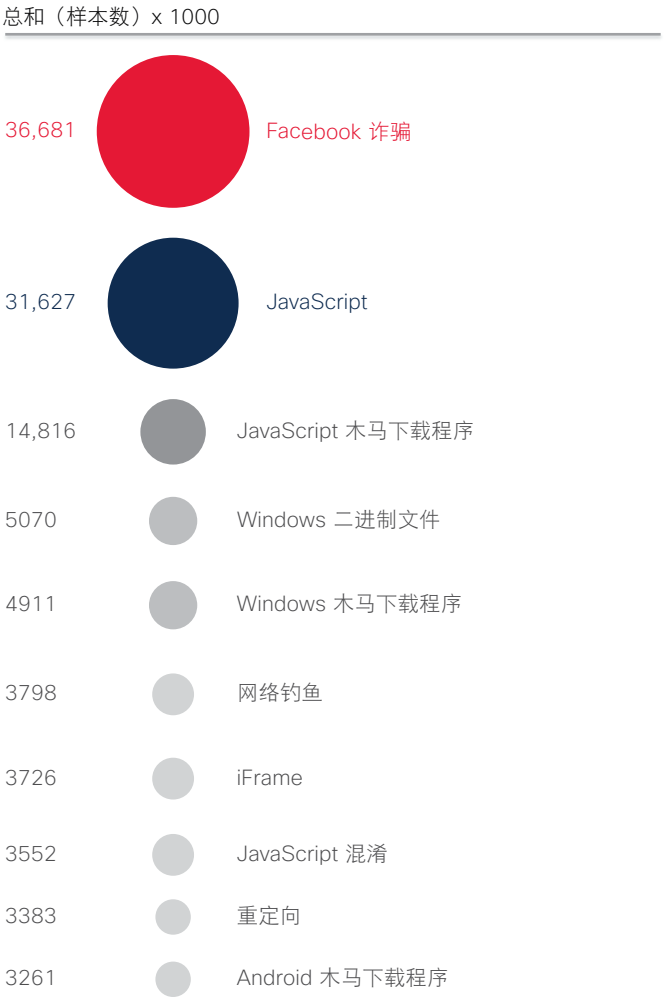


来源：思科安全研究部门

Web 攻击方法

图 16 和 17 显示了各种类型的恶意软件，攻击者使用这些恶意软件获取组织网络的访问权限。图 16 显示最常见的恶意软件：广告软件、间谍软件、恶意重定向程序、iFrame 漏洞和网络钓鱼。

图 16. 观察到最常用的恶意软件



来源：思科安全研究部门

[5] “Adobe 新闻：Flash、HTML5 和开放式网络标准”Adobe,2015 年 11 月 30 日：**http://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html**。

图 16 基本上可以视为犯罪分子用于获取初始访问权限的恶意软件的类型集合。这些都是行之有效并且最具成本效益的相对轻松地攻击大量用户的方法。根据我们的研究，JavaScript 漏洞攻击和 Facebook 诈骗（社交工程）是最常用的攻击方法。

图 17 显示了少量使用的恶意软件。请注意，“少量”并不意味着“低效率”。根据思科安全研究部门的观点，少量使用的恶意软件可能代表新兴威胁或高度有针对性的攻击活动。

这些更复杂的方法中很多都是为了从受入侵的用户挖掘尽可能多的价值。他们盗取高价值数据或挟持用户的数字资产以索要赎金。

因此，监控 Web 恶意软件时，只关注最常见类型的威胁远远不够。必须仔细考虑全部的攻击。

图 17. 观察到的少量使用恶意软件的示例

总和（样本数）< 40

来源：思科安全研究部门

最新威胁信息

ADOBE FLASH 主要漏洞列表

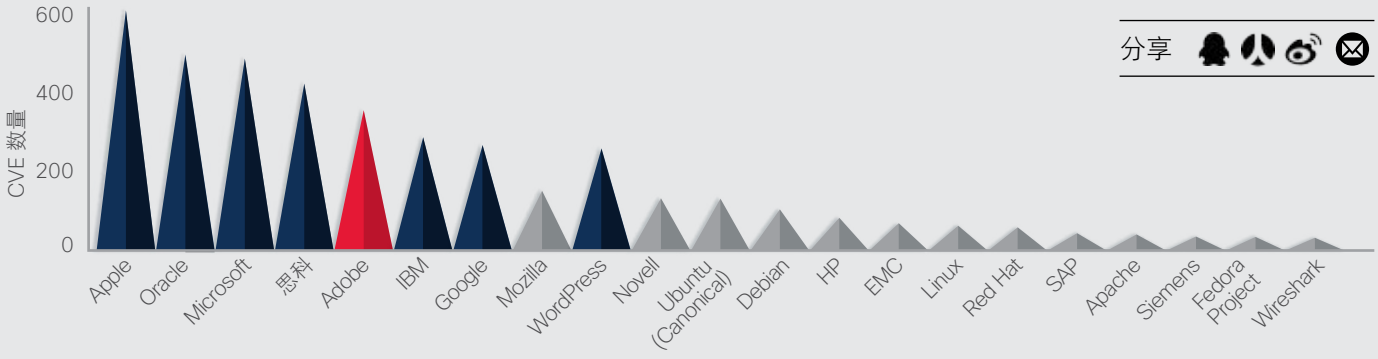
Adobe Flash 平台多年以来一直是犯罪分子偏爱的一种威胁媒介。Flash 漏洞攻击仍然频繁出现在高度紧迫警报列表中。在 2015 年，值得肯定的是经常发生这些漏洞攻击的网络浏览器等产品的供应商已认识到这个缺点并开始采取措施来减少攻击机会。

犯罪分子在 2016 年则很可能将漏洞利用和攻击集中于 Adobe Flash 用户身上。针对一部分 Flash 漏洞的攻击方法已经可以在线获得，包括公开的信息或以漏洞攻击包形式出售。（如**第 21 页**所述，Flash 相关的内容数量已经减少，但 Flash 仍然是主要的漏洞攻击媒介。）

继采取策略成功降低另一常见威胁媒介 Java 的影响之后，很多网络浏览器针对 Flash 采取阻止或沙盒技术以保护用户。虽然这是一种良性发展，但必须铭记今后一段时间内攻击者仍会成功发起漏洞攻击。用户可能无法根据需要更新浏览器，犯罪分子将继续发动针对旧版本浏览器软件的漏洞攻击。

但是，思科研究人员认为一些常用网络浏览器和操作系统目前内置的保护将可以降低犯罪分子对 Flash 的依赖。由于网络攻击者专注于尽可能最高效地获得最佳效果（例如高利润），所以对于投资回报可能较小的攻击，他们花费的精力也会比较少。

图 18. 按供应商划分的 VE 总数



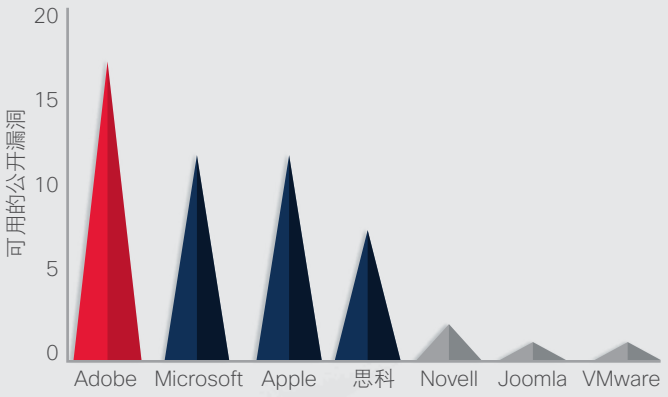
来源：思科安全研究部门美国国家漏洞数据库

上图显示 2015 年发布的按供应商划分的 CVE 总数。请注意，Adobe 在本图中并没有在右图中那样突出，右图显示漏洞攻击可以利用的漏洞。

此外，WordPress 在 2015 年自身产品仅显示 12 个漏洞。其他 240 个漏洞来自第三方提供商创建的插件和脚本。

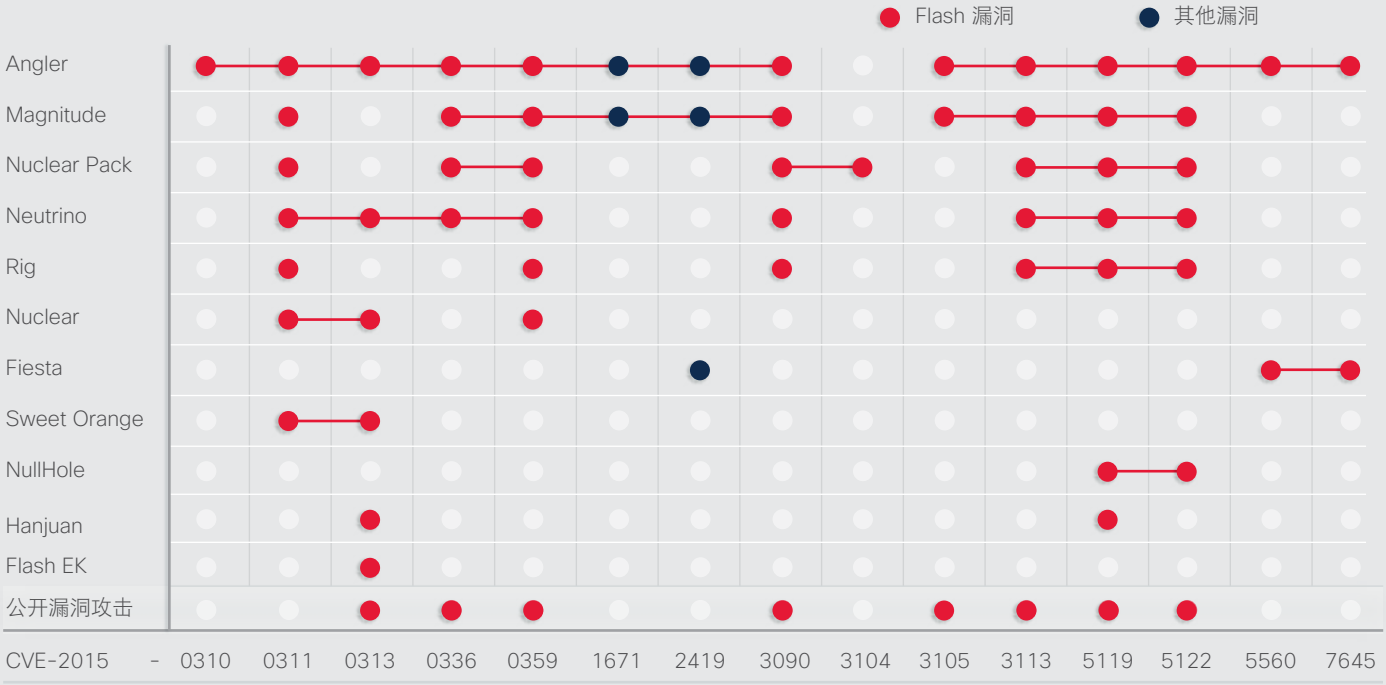
如图 20 所示，漏洞和相关漏洞攻击的列表可以为安全专业人员提供指导。安全专业人员可以将其用于管理高风险常见漏洞，确定漏洞优先级，以高于低风险漏洞的速度更快地修补这些漏洞。有关各供应商 CVE 的更多信息，请参阅 CVE 详细信息网站 **(https://www.cvedetails.com/top-50-products.php)**。

图 19. 按供应商漏洞划分的可用公开漏洞攻击数量



来源：思科安全研究部门 Metasploit 漏洞攻击数据库

图 20. 常见漏洞



来源：思科安全研究部门

图 20 显示高风险的漏洞，并指出漏洞是已经被漏洞攻击包所利用（请参阅“Flash 漏洞攻击包”行），还是可以公开得到漏洞攻击相关信息（请参阅“公开漏洞攻击”行）。哪些漏洞攻击可以利用的漏洞具有高修补优先级。

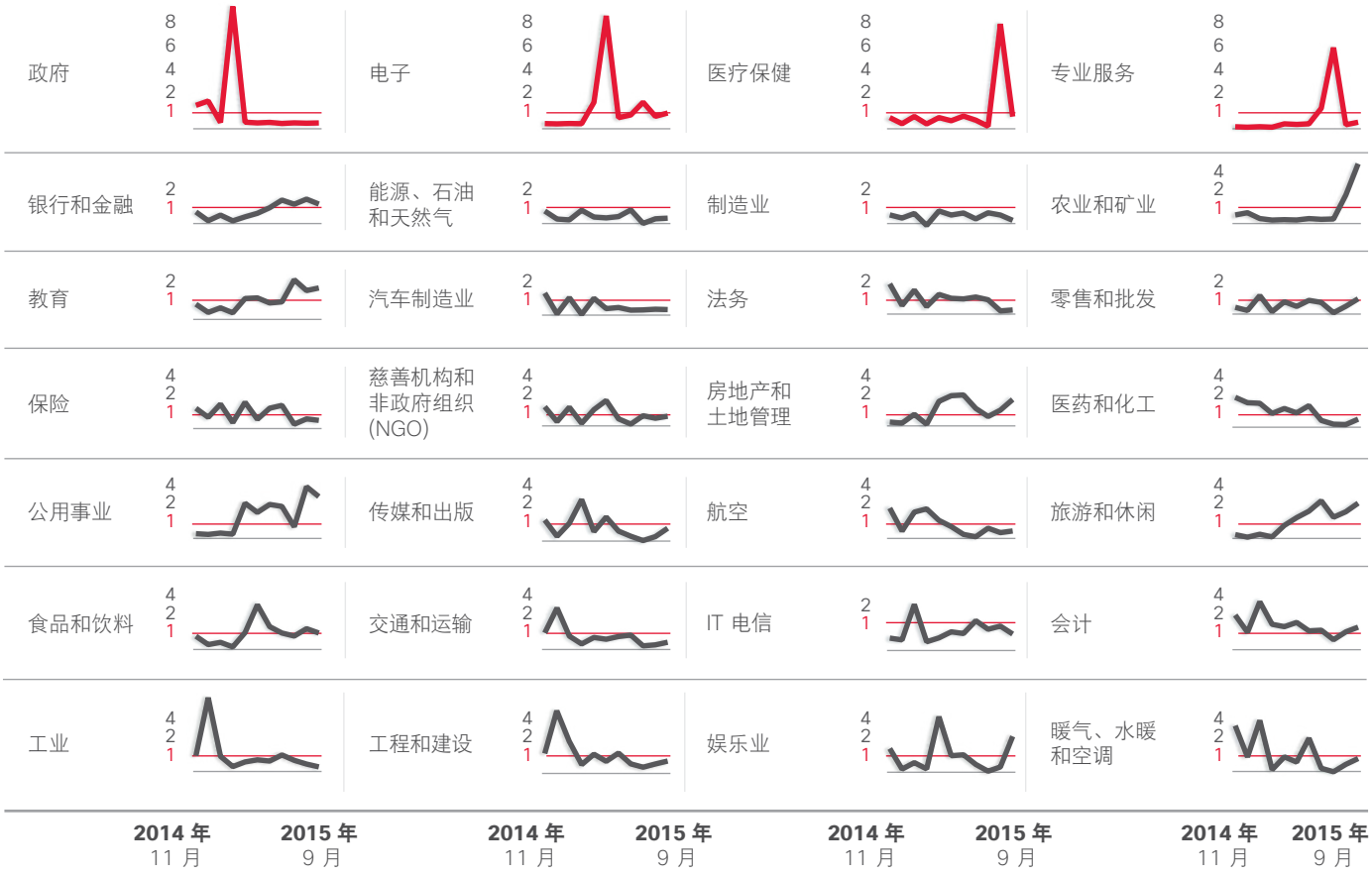
此列表可用于帮助安全专业人员确定修补和补救活动的优先级。对于特定产品，如果存在某个漏洞攻击，无论是公开漏洞攻击还是已被加入漏洞攻击包，并不一定意味着正在发生攻击。

垂直行业遭受恶意软件攻击的风险

为了跟踪遭受 Web 恶意软件攻击的高风险垂直行业，我们分析了攻击流量的相对数量（“阻止率”）以及“常规”或预期流量。

图 21 显示了 28 种主要行业及其相关阻止活动，以占常规网络流量的比率表示。比率为 1.0 意味着阻止活动的数量与观察到的数据流量相称。任何高于 1.0 的比率则表示阻止率高于预期，任何低于 1.0 的比率表示阻止率低于预期。

图 21. 2014 年 11 月至 2015 年 9 月期间每月的垂直行业阻止率

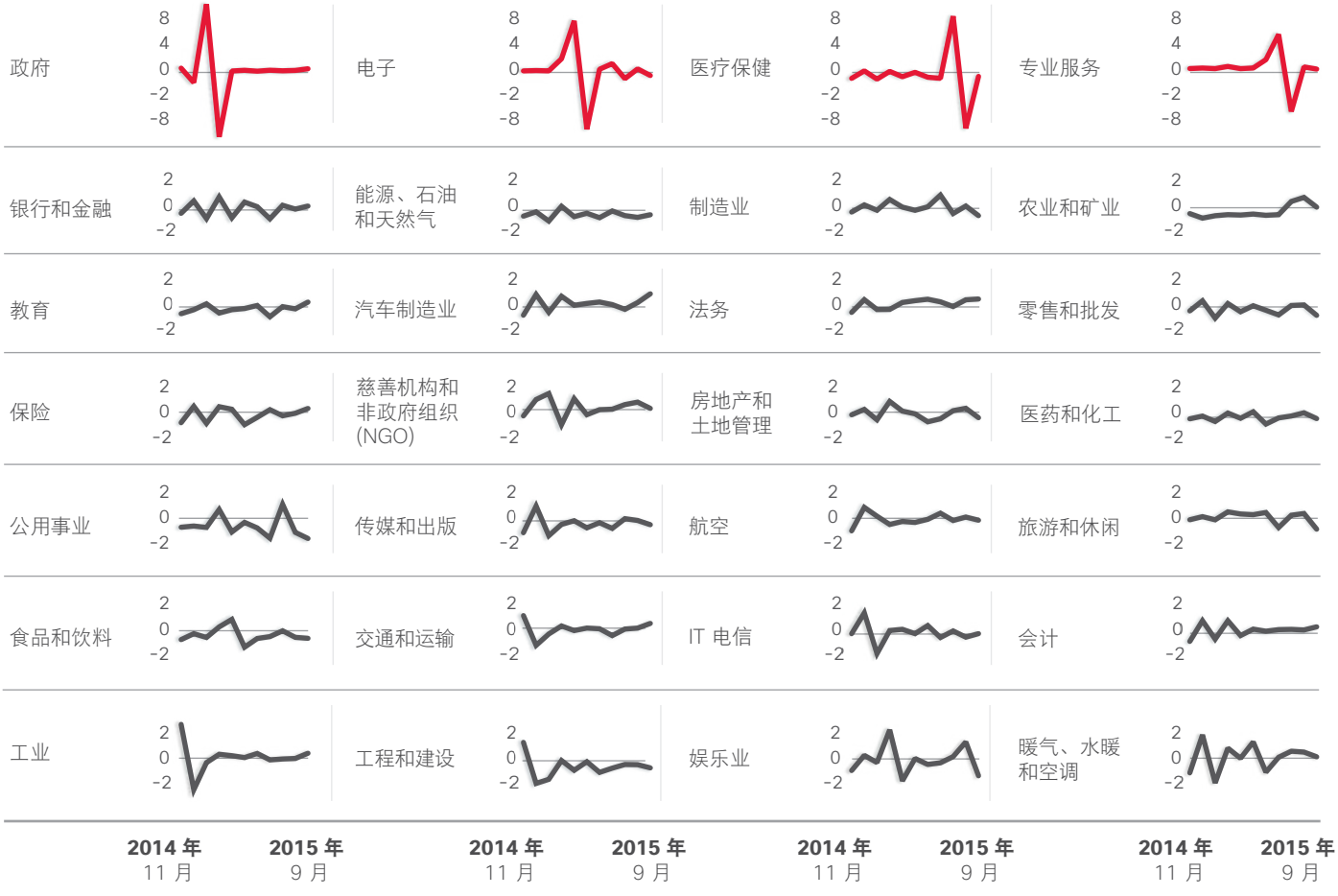


来源：思科安全研究部门

图 22 说明攻击者对特定垂直行业的关注如何可以转瞬即逝。（零代表无净变。） 2015 年 1 月到 3 月，政府是阻止率最高的垂直行业。3 月至 5 月，是电子行业。仲夏期间，专业服务行业一举夺魁。在 2015 年秋季，医疗保健行业的阻止率则高于所有其他垂直行业。

根据我们的调查，2015 年阻止活动最多的四个垂直行业都曾被作为特洛伊木马相关攻击的目标。政府垂直行业还面临过大量的 PHP 注入攻击，而专业服务垂直行业则曾遭到大量 iFrame 攻击。

图 22. 垂直行业相对阻止率逐月比较



来源：思科安全研究部门

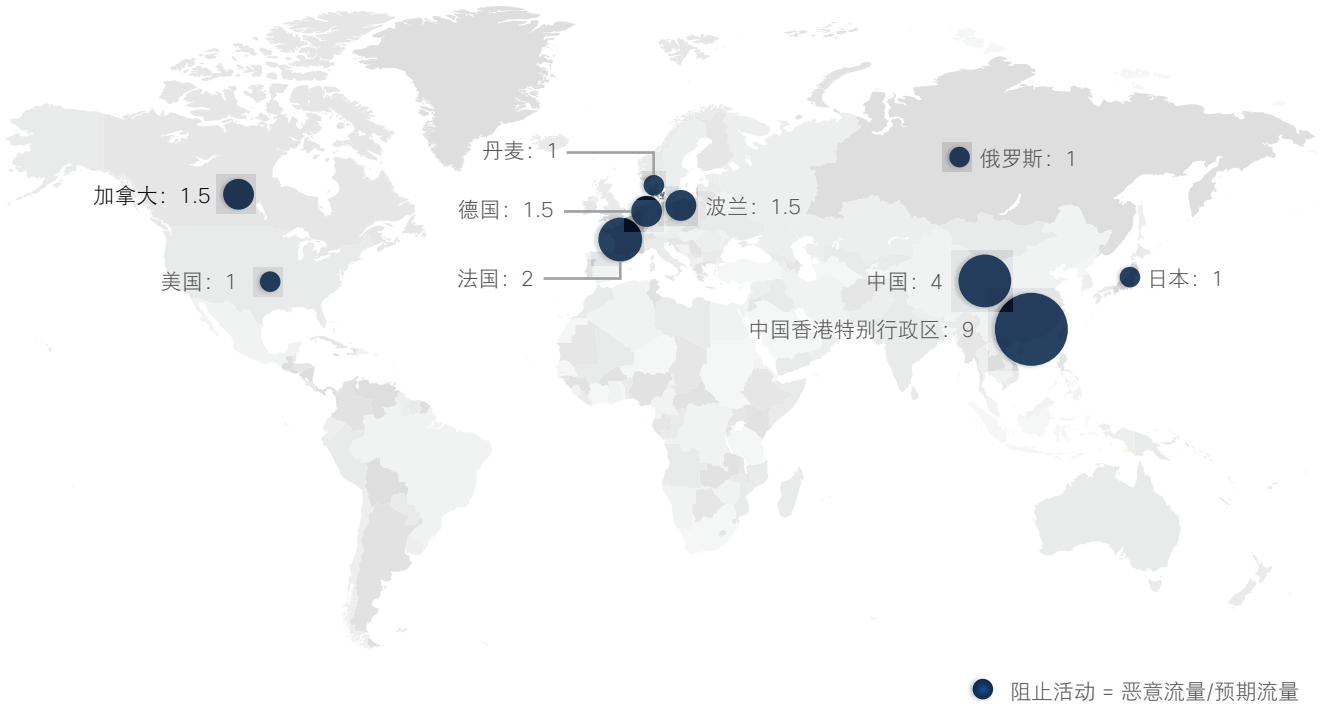
分享

Web 阻止活动：地域概况

如图 23 所示，我们还按照国家或地区对基于恶意软件阻止活动的发源地进行了分析。依据这些国家/地区的互联网流量，选择相应国家/地区来进行研究。“阻止率”值为 1.0 表示所观察到的阻止数量与网络规模相符。

我们认为，在阻止活动高于正常水平的国家和地区，其网络中可能存在大量带有未修补漏洞的 Web 服务器和主机。恶意攻击者无视国家/地区边界，并且在恶意软件能够发挥最大效果的任意位置部署恶意软件。

图 23. 按国家或地区的 Web 阻止



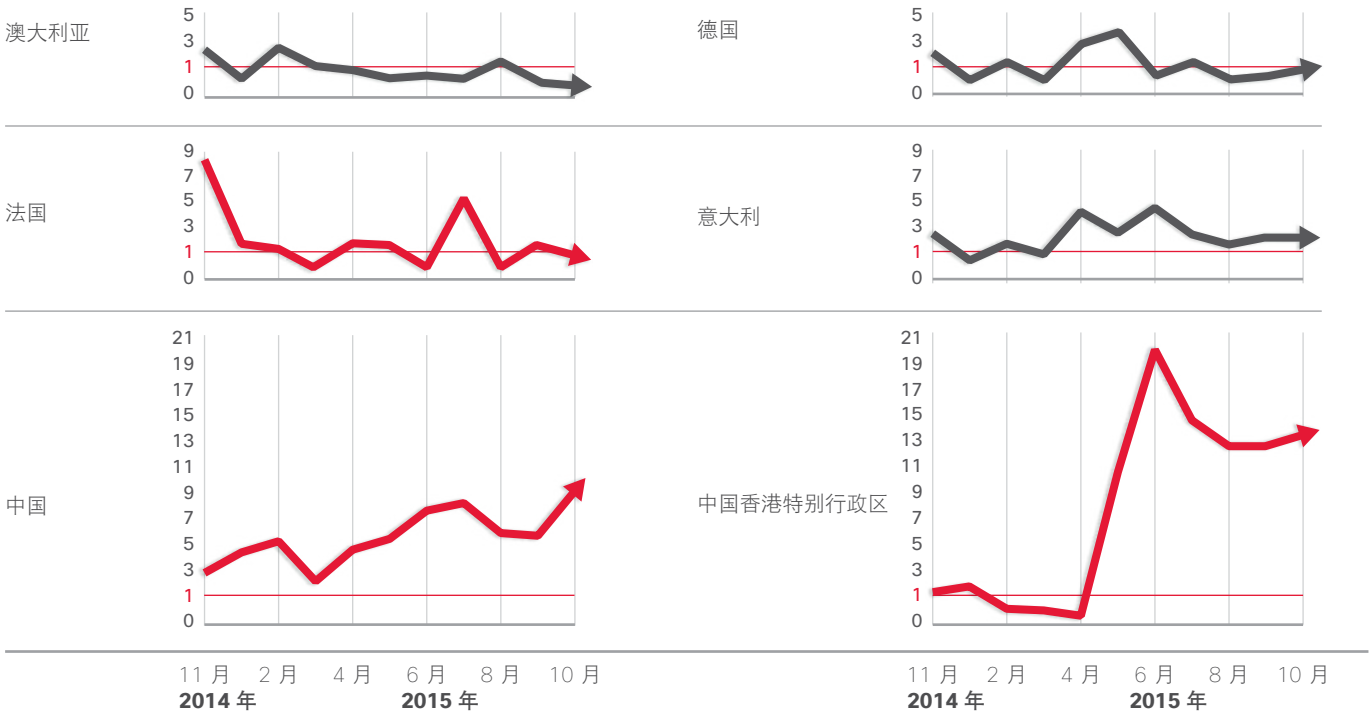
来源：思科安全研究部门

阻止活动比例高的另一个因素是，这些国家/地区存在着处理大量互联网流量的大型商用网络，这也是为什么中国香港位于我们的列表之首的一个原因。

图 24 显示从 2014 年 11 月至 2015 年 10 月期间按国家或地区划分的 Web 阻止活动数量的逐月对比，为这些排序提供了更多背景信息。

请注意，从 2015 年春季开始，中国香港出现了高于常规的 Web 阻止活动，法国也是如此。然后，中国香港和法国都出现了 Web 阻止活动显著下降的情况，但由于今年年初活动阻止率远高于基准水平，尽管最近的阻止活动有所下降，但仍然使中国香港年底的阻止率高于年初的阻止率。在仲夏期间，法国阻止活动从峰值回归到正常水平。

图 24. 2014 年 11 月至 2015 年 10 月按国家或地区的 Web 阻止活动逐月比较



来源：思科安全研究部门

行业见解

行业见解

思科提供有关安全趋势和安全实践的研究和分析。令人意外的是，有些趋势和实践可能会使防御者更加难以跟踪威胁，也使得组织和个人用户面临更大的威胁或攻击风险。

加密：日益发展的趋势 - 也是防御者面临的挑战

加密是一种合理的需求，因为公司需要保护知识产权和其他敏感数据，广告商希望确保广告内容和后台分析的完整性，而企业则更加注重保护客户的隐私。

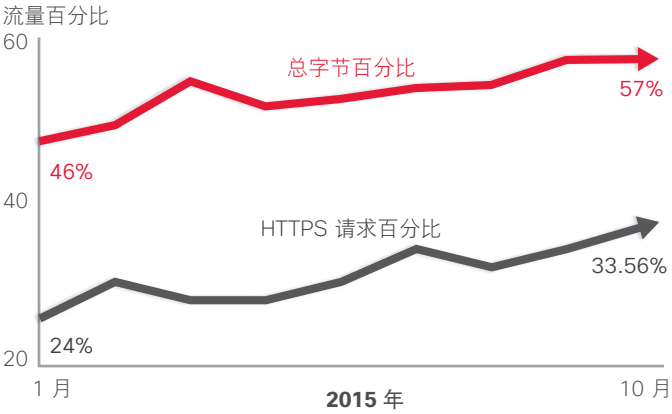
但是，加密也为组织带来了安全问题，其中包括虚假的安全感。组织已经提高了在不同实体之间传输数据时加密数据的能力，但是静止数据却通常未受到保护。过去几年间许多最值得注意的漏洞都利用了数据中心和其他内部系统中存储的未加密数据。对攻击者而言，这就像是尾随一辆戒备森严的供给卡车进入未上锁的仓库。

组织还必须要认识到，端到端加密会降低某些安全产品的有效性。加密会掩盖用于确定和跟踪恶意活动的危害表现。

但是，对敏感数据加密是无可置疑的做法。安全工具及其操作人员都需要适应这种新的局面，通过收集数据流的报头和其他未加密部分以及其他情景信息来源来分析加密流量。那些依赖负载可视性的工具（例如完整数据包捕获方法）的有效性正在逐渐降低。如今，执行 Cisco NetFlow 分析和其他基于元数据的分析势在必行。

在观察了 2015 年的趋势之后，我们的研究人员认为加密流量（特别是 HTTPS 流量）已经达到一个临界点。虽然这种流量尚未占到所有事务的大多数，但很快就会成为互联网上的主要流量形式。事实上，我们的研究表明，由于 HTTPS 的较大开销以及通过 HTTPS 发送的更大内容（例如向文件存储站点的传输活动），这种流量在传输字节中所占的比例已经保持在 50% 以上（图 25）。

图 25. SSL 百分比



来源：思科安全研究部门

任何 Web 事务都需要发送（出站）和接收（入站）一定数量的字节。HTTPS 事务的出站请求比 HTTP 出站请求额外多出约 2000 字节。不仅如此，HTTPS 入站请求也有开销，但是相对于更大的响应开销，此开销并不明显。

通过合并每个 Web 事务的入站和出站字节，就可以确定使用 HTTPS 加密的每个 Web 事务涉及的所有字节的整体百分比。我们发现，由于 HTTPS 流量的增长及其更高的开销，HTTPS 字节在所有网络流量中所占的比例从 2015 年 1 月的 46% 增至 10 月的 57%（图 25）。

通过网络流量分析，我们还确定 HTTPS 请求一直在逐渐增加，只是自 2015 年 1 月开始增幅显著。如图 25 所示，1 月份有 24% 的请求使用 HTTPS 协议；其余请求使用 HTTP。

而在 10 月，我们所观察的请求中，有 33.56% 属于 HTTPS 请求。此外，我们发现入站 HTTPS 字节的百分比也有所增加， 而且全年如此。由于使用 HTTPS 的流量增加，需要的带宽也随之增加。每个事务需要增加 5 kbps 带宽。

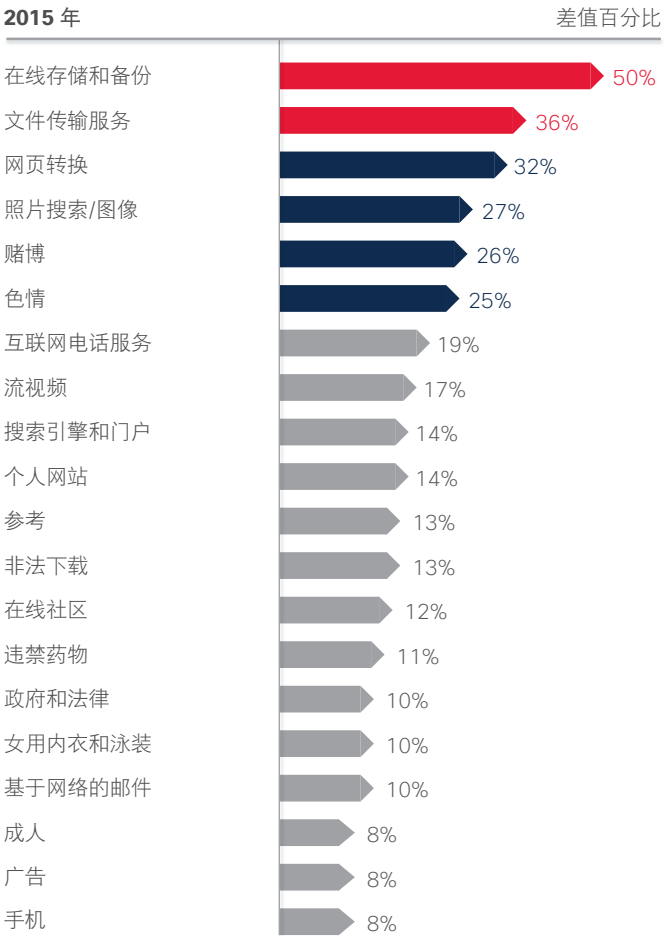
我们认为，加密网络流量的整体增加主要归因于以下因素：

- **来自应用的移动流量增加，这些流量本身就是加密流量**
- **来自用户的加密视频下载请求增加**
- **向保存敏感“静止数据”（这也是网络攻击者意图利用的数据）的存储和备份服务器发出的请求增加**

事实上，图 26 显示，向在线存储和备份资源发出的 HTTPS 请求自 2015 年初以来已提高 50%。同一时期，文件传输服务也大幅增加，增幅为 36%。

最终，加密活动在加密事务的数量和每个事务的加密字节数这两方面都有所增加。这种增长不仅体现了这两方面各自的优势，也喻示着这两方面各自潜在的风险，因此需要采用有助于提高可视性的集成式威胁防御方法。

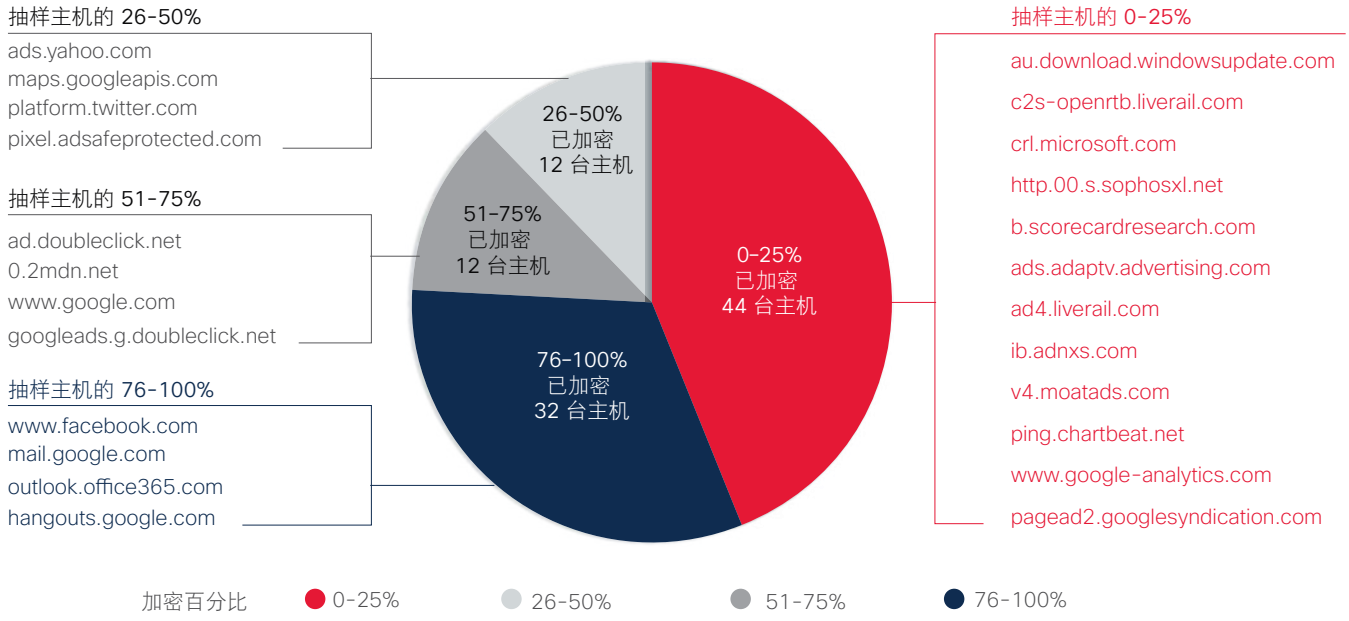
图 26. HTTPS 请求：2015 年 1 月到 9 月的最大变化



来源：思科安全研究部门

分享

图 27. 加密 HTTPS 流量最多的主机



来源：思科安全研究部门

通过观察请求量排名靠前的域（图 27）可以看出，Google 和 Facebook 的许多主要内容页面都经过加密。通常，这些网站的广告流量只有 10% 经过加密。

尽管存在诸多挑战，但是在当前的威胁形势下，对数据加密势在必行。攻击者对规避用户访问控制轻车熟路，因此在所有存储或传输阶段，都必须对关键信息实施保护。

正因如此，安全团队必须监控网络流量模式，确保 HTTPS 请求不会来自或发往可疑位置。需要提醒的一点是：不要仅关注一组预定义端口上的加密流量。正如下一节所述，我们的研究表明，恶意软件可能会通过各种不同端口发起加密通信。

熵因素

高熵是喻示存在加密或压缩文件传输或通信的明显迹象。[6]对安全团队而言，值得高兴的是熵相对比较容易监控，因为不需要知道底层加密协议。

从 2015 年 6 月 1 日开始的三个月时间内，思科安全研究人员观察到有 7,480,178 个流来自 598,138 个“威胁分数：100”恶意软件提交样本。在此期间的高熵流为 958,851 个，占 12.82%。

我们还发现，通过传输层安全 (TLS) 协议传输的流为 917,052 个 (12.26%)。此外，有 8419 个 TLS 流流经安全 HTTP 的默认端口 443 以外的端口。观察到的恶意软件用于进行通信的端口包括端口 21、53、80 和 500。

随着加密互联网流量持续增加，对组织而言，采用集成式威胁防御架构将变得越来越重要（请参阅“集成式威胁防御的六个原则”[**第 62 页**]）。单点解决方案并不能有效识别加密流量中的潜在威胁。集成式安全平台可为安全团队提供更强的可视性，使其了解设备或网络中发生的情况，从而更轻松地识别可疑活动模式。

[6] 熵：在计算中，熵（无序或不可预测）是操作系统或应用收集的随机数，用于加密或需要随机数据的其他用途。

加密的发展：案例数据

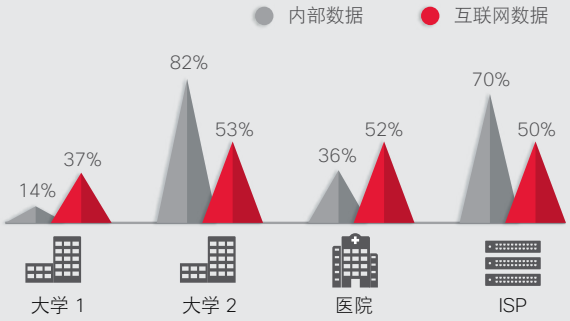
思科旗下公司 Lancope 对三个工商部门（两所大学，一间医院和一家 ISP 提供商，总部全都位于美国）的内部和互联网流量进行了加密率分析。

在一所大学中，Lancope 发现几乎所有内部流量都经过加密 (82%)。此外，该大学 53% 的互联网流量也经过加密。这些结果与 Lancope 在其他行业中观察到的趋势水平相当。

医院的内部数据只有 36% 经过加密。但是，有超过一半 (52%) 的互联网流量经过加密。

而那一家领先的 ISP 提供商有 70% 的内部流量经过加密，50% 的互联网流量经过加密。

Lancope 的研究表明，各个部门正在广泛采用数据加密。思科建议，现在应该对静止数据的加密给予同样的关注，以便限制组织所受危害的影响。



来源：Lancope 威胁研究实验室

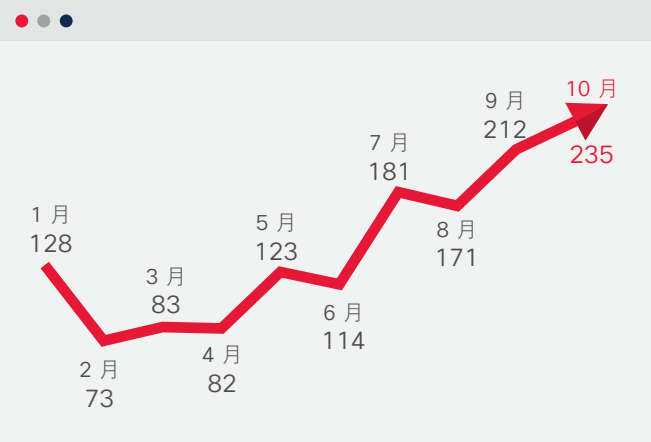
网络犯罪分子增加了在使用 WordPress 所创建网站上的服务器活动

正如本报告序言中所述，网络犯罪分子不断想方设法，使其犯罪活动效率更高且成本更低；同时，他们也在寻觅逃避检测的新手段。越来越多的网络犯罪者发现，利用基于 WordPress（常用的网站和博客开发平台）创建的网站可以达到这样的效果。在不同的 WordPress 站点中，攻击者可以控制数量稳定的受感染服务器，借此创建支持勒索软件、银行欺诈或网络钓鱼攻击的基础设施。互联网上充满使用 WordPress 创建的废弃网站，没有从安全角度对其进行维护；当出现新的安全问题时，这些站点通常会受到感染，被攻击活动所利用。

通过分析用于支持勒索软件和其他恶意软件的系统，思科安全研究人员发现，许多网络犯罪分子正将在线活动转向受感染的 WordPress 服务器。2015 年 2 月到 10 月之间，犯罪分子利用的 WordPress 域的数量增长了 221%（请参阅图 28）。

思科研究人员认为，这种犯罪平台的转变是由多个原因造成的。当勒索软件使用其他工具对加密密钥或其他命令和控制信息进行通信时，这些通信可以被检测到或被阻止，致使加密过程无法完成。但是，通过受感染的 WordPress 服务器中继加密密钥的通信可能看起来是正常的，这就提高了文件加密成功完成的可能性。换句话说，WordPress 站点被用作中继代理。

图 28. 恶意软件作者利用的 WordPress 域的数量



来源：思科安全研究部门

为了回避其他技术的弊端，犯罪分子已转而使用 WordPress 来承载恶意软件负载以及命令和控制服务器。WordPress 站点具有几项优势。例如，这类站点存在许多废弃站点，让犯罪分子有更多机会侵入安全防护薄弱的站点。

使用受感染系统运行恶意软件操作的风险在于，被侵入的服务器可能会在发现受到威胁时被关闭。如果在攻击活动中途发生这种情况，恶意软件下载程序可能就无法检索其负载，或者恶意软件可能无法与其命令和控制服务器通信。思科安全研究人员注意到，恶意软件使用多台 WordPress 服务器来克服这个问题；思科甚至还发现了数据共享站点（例如 Pastebin）上存储的受感染 WordPress 服务器列表。

恶意软件使用这些列表查找工作的命令和控制服务器，使恶意软件即使在某台受感染服务器发生故障时也能正常运行。研究人员还发现一些恶意软件下载程序包含用于存储负载的 WordPress 站点的列表。如果某个下载站点无法正常工作，恶意软件会转到下一个站点，并从工作的 WordPress 服务器下载恶意负载。

受到感染的 WordPress 站点通常运行的并非最新版本的 WordPress、使用的管理员密码安全性较弱，而且使用的插件没有安全补丁。

攻击者可以利用这些漏洞将 WordPress 服务器纳为己用，将其作为恶意软件基础设施（请参阅图 29）。

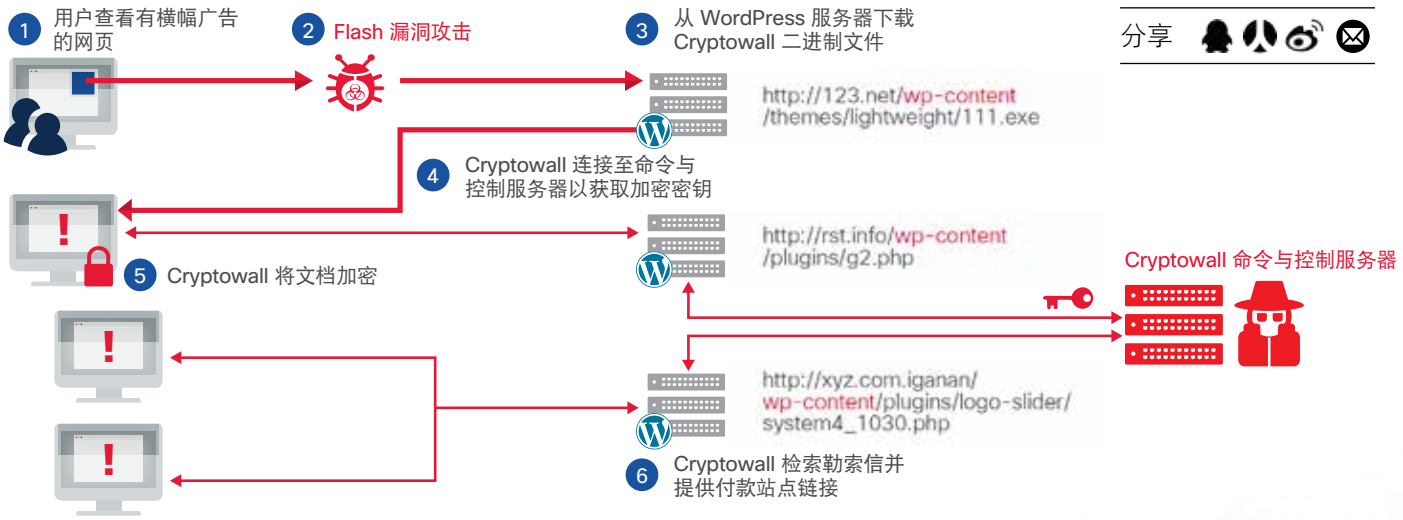
思科研究人员已经确定了一些经常寄宿在受感染 WordPress 站点中的软件和文件类型：

- 属于漏洞攻击包攻击负载的可执行文件
- Dridex 和 Dyre 等恶意软件的配置文件
- 用于中继命令和控制通信以隐藏命令和控制基础设施的代理代码
- 用于收集用户名和密码的网络钓鱼网页
- 将流量重定向至漏洞攻击包服务器的 HTML 脚本

此外，思科研究人员还确定了使用受感染 WordPress 网站作为基础设施的许多恶意软件系列：

- Dridex 信息窃取木马
- Pony 密码窃取程序
- TeslaCrypt 勒索软件
- Cryptowall 3.0 勒索软件
- TorrentLocker 勒索软件
- Andromeda 垃圾邮件僵尸网络
- Bartallex 木马植入程式
- Necurs 信息窃取木马
- 假冒登录页面

图 29. WordPress 站点如何受到感染



来源：思科安全研究部门

安全专业人员如果担心被犯罪分子操控的 WordPress 所造成的威胁，就应借助 Web 安全技术检查来自基于 WordPress 创建的站点的内容。如果网络从 WordPress 站点下载的不仅有网页和图像，还包括程序（虽然 WordPress 站点也可托管合法程序），则可认为此类流量存在异常。

基础设施老化：10 年累积下来的问题

如今，所有公司都要依赖 IT（信息技术）和 OT（运营技术）基础设施来实现连接和数字化并取得成功，所以从某种程度上来说，所有公司都是 IT 公司。这意味着他们需要将 IT 安全视为优先要务。但仍有许多组织依赖于由老旧过时的组件构成的网络基础设施，这些组件运行的是易受攻击的操作系统，并且不具备网络恢复能力。

我们最近分析了互联网上和客户环境中的 115,000 台思科设备，希望促进人们关注由于基础设施老化和不注意修补漏洞而造成的安全风险。

我们通过扫描互联网然后“从外向内”（从互联网视角到企业内部）检查设备来确定一天抽样的 115,000 台设备。通过扫描和分析，我们发现，这 115,000 台设备中有 106,000 台设备运行的软件存在已知漏洞。这意味着在我们的样本中，有 92% 的互联网上的思科设备易受已知漏洞的感染。

思科还发现，这些设备运行的软件版本平均有 26 个漏洞。此外，我们得知许多组织的网络基础设施上运行的也是过时软件（图 30）。我们发现，金融、医疗保健和零售行业的一些客户使用的思科软件是 6 年前的版本。

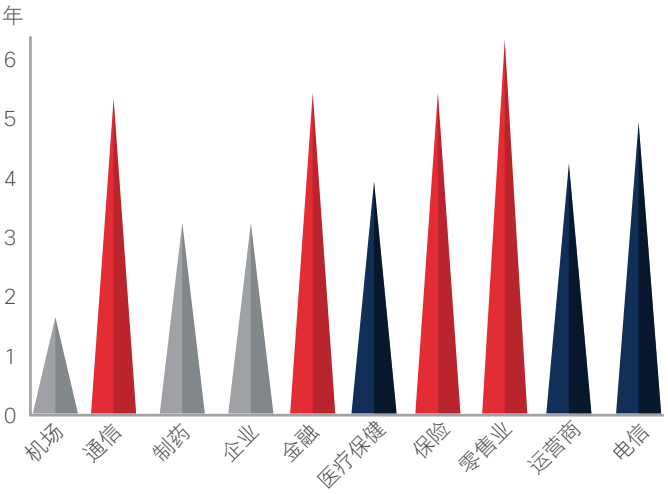
有关本主题的详细信息，请阅读思科安全博客文章：

“IT 安全：当成熟度被高估时”

“对思科 IOS 设备的攻击之演变”

“SYNful 降临：检测并减轻思科 IOS 软件攻击”

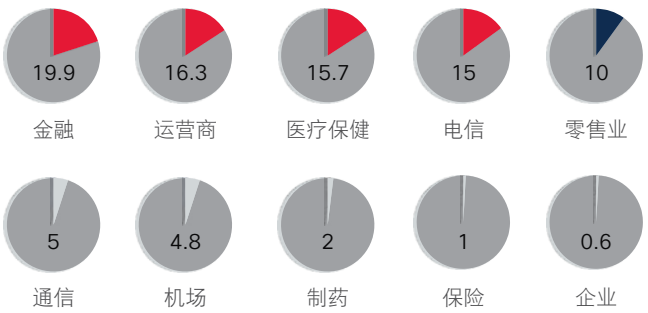
图 30. 平均软件使用年数



来源：思科安全研究部门

我们还发现，我们分析的许多基础设施设备已达到最后支持日期 (LDoS)，这意味着这些设备已无法更新和提高安全性（图 31）。而且，这些设备甚至收不到已知漏洞的补丁，因此也就无法获得有关新威胁的信息。客户已经意识到这个问题。

图 31. 基础设施设备的 LDoS 百分比



来源：思科安全研究部门

此外，在我们分析的 115,000 台样本设备中，有 8% 的设备已达到寿命终止阶段，另有 31% 的设备将于一到四年内达到支持终止时间。

对组织而言，老化过时的 IT 基础设施就是漏洞。随着我们逐渐向物联网 (IoT) 和万物互联 (IoE) 发展，确保企业能够依靠安全的网络基础设施来保证通过网络传输的数据和通信的完整性就变得更加重要。这一点对于新兴的万物互联取得成功具有至关重要的意义。

许多思科客户的网络基础设施建于十年以前。当时，许多企业根本没有考虑到他们会 100% 依赖于这些基础设施， 也没有料到他们的基础设施会成为网络攻击者的主要目标。

由于价格昂贵并且需要中断网络，组织往往不会进行基础设施更新。在某些情况下，简单的更新也不足以解决问题。有些产品太过陈旧，以致无法通过升级来整合保护企业安全所需的最新安全解决方案。

这些事实本身就足以证明维护基础设施的重要性。组织需要对定期升级做出规划，并认识到抢在网络攻击者前面主动控制关键基础设施的价值。

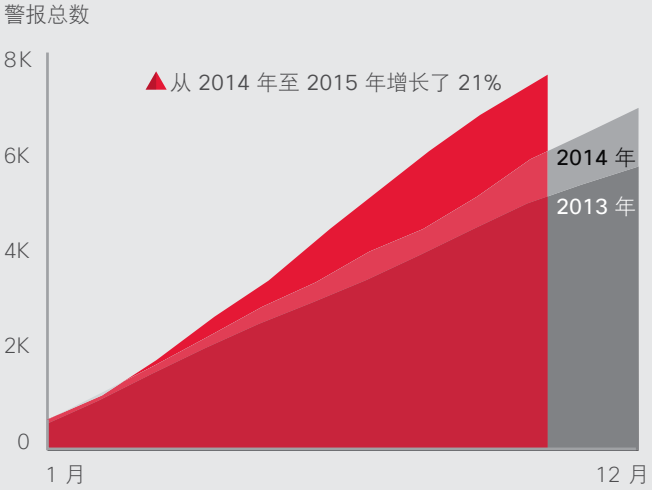
累计警报总数表明对管理漏洞的呼声越来越高

把住老化基础设施不放的做法为攻击者提供了可乘之机。不过，累计警报数的增加（包括开源和专有解决方案中的产品漏洞）则是一个积极的迹象，表明技术行业正在密切关注如何消除可被攻击者利用的机会。

从 2014 年到 2015 年，累计警报总数增加了 21%。2015 年 7 月到 9 月的增幅特别高。这种增加在很大程度上归因于 Microsoft 和 Apple 等供应商的主要软件更新，因为产品更新导致软件漏洞报告增多。

如今，主要软件供应商积极发布更多补丁和升级，而且这些活动也变得更加透明。补丁和升级数量的增加是组织实施漏洞管理自动化的主要动因，组织通过使用安全情报和管理平台来帮助管理系统数量和软件资产、漏洞和威胁信息，从而实现漏洞管理自动化。使用这些系统和应用编程接口 (API) 可以在大型和小型组织中实现更加有效、及时和高效的安全管理。

图 32. 年度累计警报总数



来源：思科安全研究部门

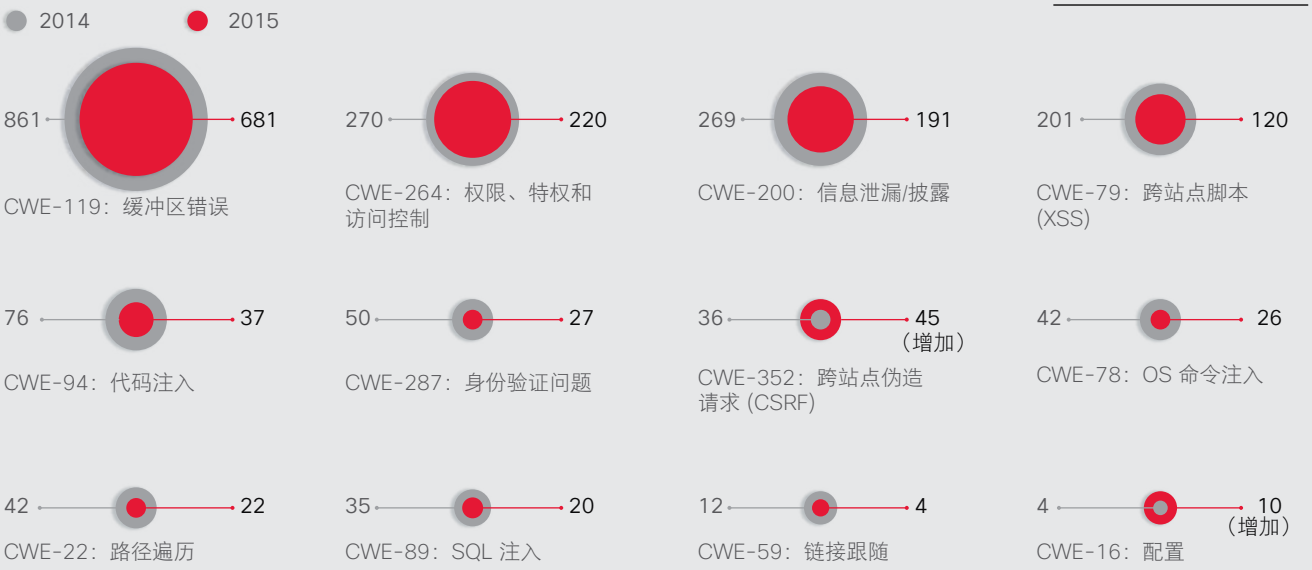
分享

威胁类别：缓冲区错误、信息泄漏和披露数下降

仔细审视常见漏洞类别可以看出，从 2014 年到 2015 年，跨站点脚本 (XSS) 漏洞减少了 47%（图 33）。这种减少可能是对漏洞测试加大关注的结果。供应商已经能够更加熟练地在产品进入市场之前确定并修复这些特定漏洞。

2015 年，信息泄漏或信息披露漏洞减少了 15%。这些漏洞涉及以无明确访问权限的各方为对象的意外信息披露。供应商已经开始留意对允许或禁止访问数据的控制，使这种常见漏洞不再频繁出现。

图 33. 各类常见漏洞的数量



来源：思科安全研究部门

中小企业是否是企业安全方面薄弱的一环？

中小企业在国家经济中具有重要作用。受客户委托保管数据时，中小企业还要负责防止这些信息受到网络攻击者的攻击。但是，正如思科 2015 年安全功能基准研究所述（请参阅**第 41 页**），有迹象显示中小企业对攻击者的防御并未达到其面临的挑战所要求的防御强度。反过来，这些薄弱环节会让中小企业的大型企业客户处于风险之中。可以突破中小企业网络的攻击者也可以找到入侵大型企业网络的途径。

根据思科 2014 年安全功能基准研究的结果来判断，中小企业今年用于分析威胁的流程和使用的威胁防御工具均少于去年。例如，48% 的中小企业在 2015 年表示使用了 Web 安全工具；而 2014 年有 59% 的企业使用。只有 29% 的企业表示他们在 2015 年使用了修补和配置工具，而 2014 年这一比例为 39%。

此外，在没有高管负责安全事务的中小企业受访者中，近四分之一受访者认为他们的企业不是网络犯罪分子的高价值目标。这种看法暗示着他们过于自信自己的企业能够击败当今复杂的网络攻击，或者，更有可能是对自己的企业不会遭到攻击过于自信。

中小企业使用事件响应团队的可能性较低

在许多情况下，中小企业组建事件响应团队和威胁情报团队的可能性比大型企业低。其原因可能是预算限制：受访者指出，预算问题是采用高级安全流程和技术的最大障碍之一。72% 的大型企业（员工超过 1000 人的企业）设有这两个团队，而员工少于 500 人的企业中只有 67% 这样做。

中小企业用于分析威胁、消除事件原因并将系统恢复到事件发生前水平的流程也更少（图 35）。例如，员工超过 10,000 人的企业有 53% 使用网络流量分析工具分析受感染的系统，而员工少于 500 人的企业中只有 43% 这样做。员工超过 10,000 人的企业有 60% 会修补和更新有漏洞的应用，而员工少于 500 人的企业中只有 51% 会这样做。

图 34. 中小企业的最大障碍

您认为下面哪些项是采用高级安全流程和技术的最大障碍？

公司规模	250-499	500-999	1000-9999	10,000+
预算限制	40%	39%	39%	41%
与旧版系统的兼容性问题	34%	30%	32%	34%
优先事项冲突	25%	25%	24%	24%

来源：思科 2015 年安全功能基准研究

图 35. 中小企业使用的安全流程少于大型企业

您的组织目前使用下列哪些流程（如果有）来分析受入侵的系统？

公司规模	250-499	500-999	1000-9999	10,000+
内存调查分析	36%	36%	35%	34%
网络流量分析	43%	47%	52%	53%
关联事件/日志分析	34%	34%	40%	42%
外部（或第三方）事件响应/分析团队	40%	32%	34%	39%
系统日志分析	47%	51%	55%	59%
注册表分析	43%	47%	52%	53%
IOC 检测	31%	34%	37%	36%

您的组织使用什么流程将受影响的系统恢复到发生事件之前的运行状态？

修补和更新视为有漏洞的应用	51%	53%	57%	60%
实施额外或新的检测和控制	49%	55%	57%	61%

来源：思科 2015 年安全功能基准研究

中小企业对某些威胁防御工具的使用呈下降趋势。例如，2014 年有 52% 的中小企业使用移动安全产品，但 2015 年只有 42% 的中小企业这样做。此外，2014 年有 48% 的中小企业使用漏洞扫描产品，而 2015 年的这一比例为 40%（请参阅图 36）。

图 36. 2015 年中小企业防御措施的减少

您的组织目前使用以下哪个类型的安全威胁防御方案（如果有）？	2014 年	2015 年
移动安全	52%	42%
无线安全	51%	41%
漏洞扫描	48%	40%
VPN	46%	36%
安全信息和事件管理 (SIEM)	42%	35%
渗透测试	38%	32%
网络调查分析	41%	29%
补丁和配置	39%	29%
终端设备调查分析	31%	23%

来源：思科 2015 年安全功能基准研究

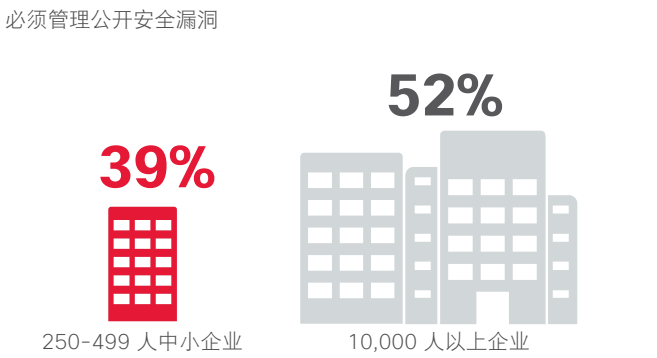
中小企业采用的防御措施少于比其规模大的企业这一点为什么重要？ 在攻击者正在开发更具有欺骗性的网络入侵策略而且仍未被检测出来的安全环境中，没有哪家企业能够不对网络采取保护措施，或者不使用相关流程来监控威胁发生过程从而避免未来再发生此类威胁。

此外，中小企业可能并未认识到，自己的漏洞会转化为大型企业客户及其网络的风险。如今的犯罪分子通常以入侵一个网络为跳板来寻找进入另一个更有利可图的网络的突破口，而中小企业可能就会成为此类攻击的第一站。

经历过公开的数据泄露事件的可能性较低

中小企业处理过公开的安全漏洞事件的可能性比大型企业低，这可能是从网络角度来看其影响范围较小的结果。员工超过 10,000 人的企业有 52% 曾成功应对过公开的安全漏洞事件的后果，而员工少于 500 人的企业只有 39% 曾经遇到过同样的情况。

图 37. 中小企业报告的公开漏洞较少

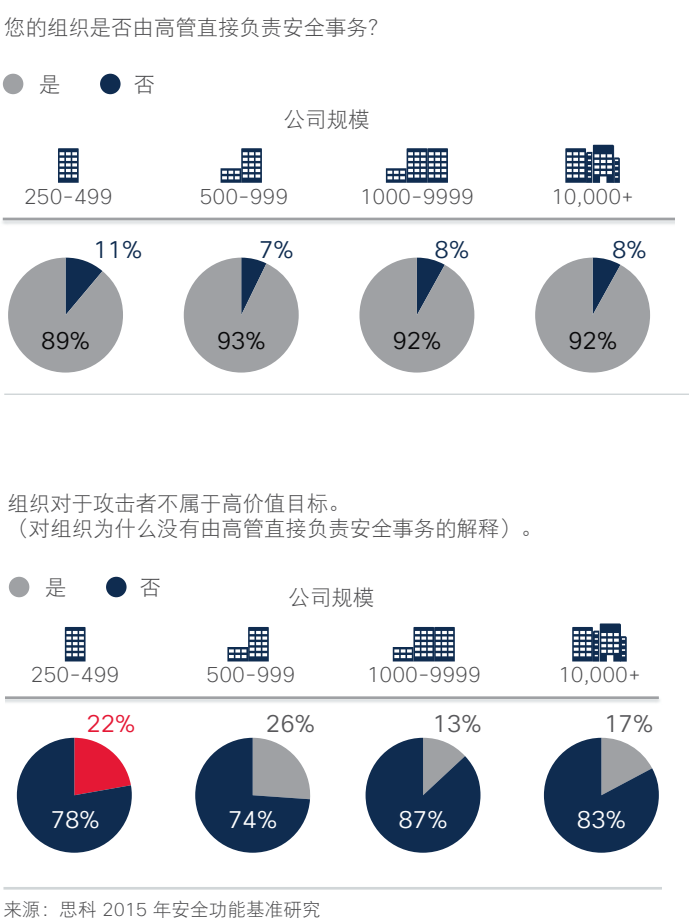


来源：思科 2015 年安全功能基准研究

分享

公开的安全漏洞事件显然对企业具有破坏性和危害，但也有一个好处：它们通常能促使企业更仔细地审视并考虑加强自己的安全防护。思科调查数据（请参阅**第 74 页**）表明，当大型企业遇到公开的数据泄露事件后，他们会大幅升级安全技术并实施功能更强的流程。

图 38. 中小企业不认为自己是高价值目标



来源：思科 2015 年安全功能基准研究

中小企业对于自己的企业作为网络犯罪者攻击目标的看法可能表明他们对威胁形势的认知存在差距。正如图 38 所示，22% 的员工少于 500 人的企业表示他们没有直接负责安全事务的高管，因为他们不认为自己是高价值目标。

2015 年中小企业将安全职能外包的可能性更高

尽管调查结果显示，整体而言，将一些安全职能外包的中小企业比大型企业多，但是中小企业外包建议与咨询等服务的可能性比大型企业低。例如，55% 的大型企业将建议与咨询服务外包，而员工少于 500 人的企业只有 46% 这样做。外包安全审核任务的大型企业达到 56%，而员工少于 500 人的企业只有 42% 这样做（请参阅图 39）。

不过，2015 年有更多中小企业至少外包了一些安全服务。201.4 年，24% 的员工少于 499 人的中小企业称其没有外包任何服务。2015 年，只有 18% 的中小企业如此回答。

更多中小企业采用外包作为管理安全事务的办法是个好消息。这表示中小企业正在寻求以灵活的工具保护网络安全，这些工具不会给他们比较少的人手或比较保守的预算造成负担。但是，中小企业可能会错误地以为，外包安全流程能够大幅减少出现网络漏洞的可能性。或者，他们可能会将安全责任加诸第三方身上。这种观点未免有些痴心妄想，因为只有真正集成的威胁防御系统（能够检查、减轻并预防攻击的系统）才能提供大型企业级的安全防护。

图 39. 更多中小企业在 2015 年外包安全服务

在安全性方面，以下哪些类型的服务（如果有）是全部或部分外包给第三方?

公司规模	250-499	500-999	1000-9999	10,000+
建议与咨询	46%	51%	54%	55%
监控	45%	46%	42%	44%
审计	42%	46%	46%	56%
事件响应	39%	44%	44%	40%
威胁情报	35%	37%	42%	41%
补救	33%	38%	36%	36%
-	18%	12%	11%	10%

为什么您的组织（250-499 人中小企业）选择外包这项/这些服务?

来源：思科 2015 年安全功能基准研究

分享

思科安全功能基准研究

思科安全功能基准研究

为了评估安全专业人员对其组织中的安全状况的认知，思科就首席安全官 (CSO) 和安全运营 (SecOps) 经理对安全资源和安全程序的看法对其进行了调查，调查对象来自多个国家/地区不同规模的组织。思科 2015 年安全功能基准研究提供了有关当前采用的安全运营和安全实践成熟度的见解，并将这些结果与 2014 年首次研究的结果进行了比较。

准备工作频增表现出信心下降

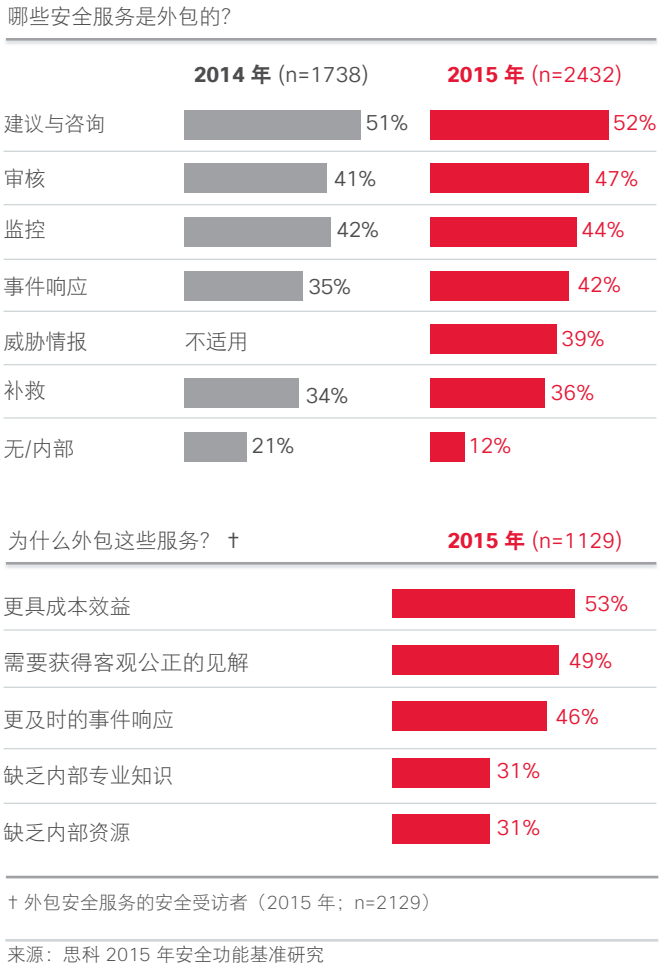
思科研究表明，面对更加复杂的威胁，安全专业人员的信心似乎正在下降。另一方面，对安全问题的担心加深也改变了这些专业人员保护网络的方式。例如，我们发现安全培训、正式的书面政策以及安全审核、咨询和事件响应等任务的外包都有所增加。简而言之，种种迹象显示，安全专业人员正在采取措施抗衡逼近网络的威胁。

培训和外包的增长属于良性发展，但是安全行业不能就此止步。安全行业必须不断增加工具和流程的使用，从而改善威胁的检测、遏制和补救。鉴于预算限制和解决方案兼容性障碍，安全行业还必须钻研出能够提供集成式威胁防御的有效解决方案。此外，安全行业还必须在公开漏洞发生时（例如 SSHPsychos 僵尸网络；请参阅**第 14 页**）与其他组织更好地协作，因为知识共享可帮助预防未来的攻击。

资源：组织采用外包的可能性更高

随着安全专业人员开始警惕各种威胁，他们可能会设法改善防御措施，例如将那些可由顾问或供应商更有效地管理的安全任务外包。2015 年，接受调查的公司有 47% 将安全审核外包，比 2014 年的 41% 有所增加。同样，2015 年有 42% 的公司外包事件响应流程，也高于 2014 年的 35%（图 40）。

图 40. 外包服务概况



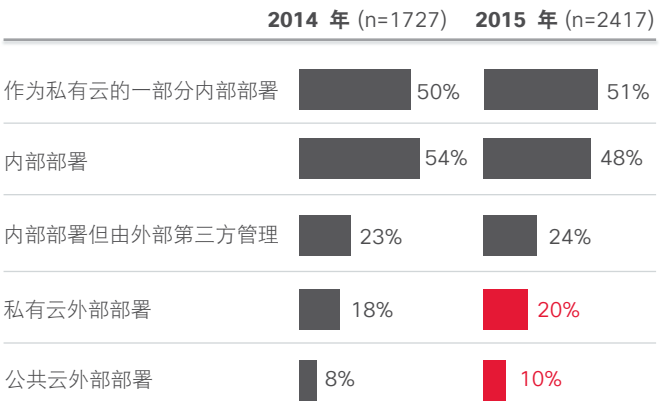
† 外包安全服务的安全受访者（2015 年；n=2129）

来源：思科 2015 年安全功能基准研究

此外，有更多安全专业人员至少外包了一些安全职能。2014 年，21% 的调查受访者称其没有外包任何安全服务。2015 年，这一数字显著下降至 12%。53% 的受访者表示外包服务是因为这样做更具成本效益，而 49% 的受访者则称其外包服务是为了获得没有偏见的见解。

安全专业人员指出，为了增加对网络和数据的保护，他们乐于接受在外部托管网络的概念。虽然内部承载仍是优先选择，但使用外部解决方案的专业人员数量有所增加。2015 年有 20% 的受访者使用外部私有云解决方案，而 2014 年这一比例为 18%（图 41）。

图 41. 外部托管有所增加



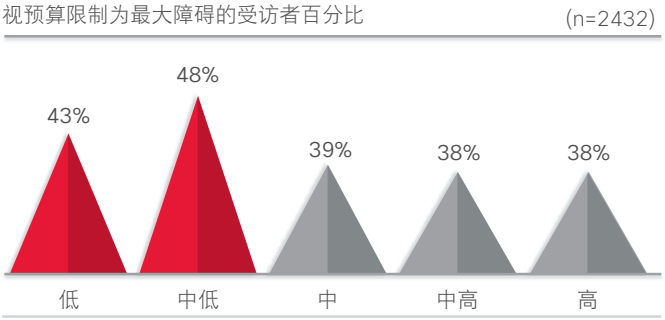
来源：思科 2015 年安全功能基准研究

图 42. 预算限制是安全升级的主要障碍

来源：思科 2015 年安全功能基准研究

接受思科调查的安全团队更有意于提高网络保护的有效性，但其执行计划的能力可能受到限制。在安全专业人员对选择或拒绝安全服务和工具的可能原因的排名中，预算限制 (39%) 居于首位，其次是技术兼容性问题（32%；请参阅图 42）。对于列入低和中低成熟度的企业，预算限制的问题更严重（请参阅图 43）。在所有安全专业人员的回答中，有 39% 的回答将预算限制列为采用高级安全流程的障碍。这一数字在属于低成熟度的企业中为 43%，而在属于中低成熟度的企业中为 48%。

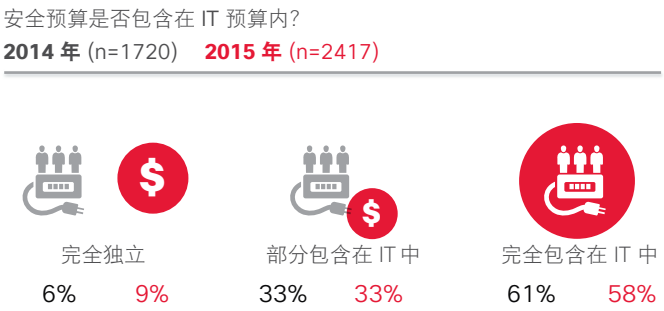
图 43. 预算限制对于低成熟度公司是更大的障碍



来源：思科 2015 年安全功能基准研究

从某些组织制定安全预算的方式可以看出，他们对安全资源考虑得更多。调查结果显示，将安全预算与整体 IT 预算分开的组织数量略有增加。2014 年，6% 的专业人员称其安全预算和 IT 预算完全分立；2015 年，这一数字提高到 9%（请参阅图 44）。

图 44. 采用单独的安全预算的组织略有增加



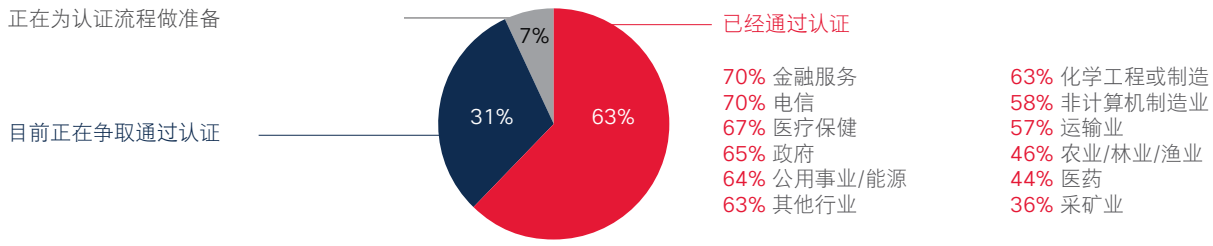
来源：思科 2015 年安全功能基准研究

从组织实施安全策略标准化或参加认证的做法可以看出，他们正致力于提高安全性。近三分之二安全专业人员称其组织已经通过标准化安全策略或实践的认证或正在争取通过认证（图 45）。

这是另一个积极的迹象，表明企业看到了提高安全知识和应对威胁的价值。

图 45. 大多数组织已通过认证或正在申请认证

组织遵循标准化的信息安全策略实践 (**2015 年** n=1265)



来源：思科 2015 年安全功能基准研究

仔细审视安全防御工具的使用可以发现，企业最常用的安全工具是防火墙 (65%)，其次是数据丢失保护工具 (56%) 和身份验证工具（53%；请参阅图 46）。2015 年，企业不太倾向于依赖基于云的工具。尽管安全专业人员表示愿意外包安全服务（请参阅**第 43 页**），但他们可能更倾向于在内部部署工具。（有关完整列表，请参阅**第 71 页**。）

图 46. 防火墙和数据丢失保护是最常用的安全工具

组织使用的安全威胁防御措施	**2014 年** (n=1738)	**2015 年** (n=2432)	通过基于云的服务管理防御措施（使用安全威胁防御措施的安全受访者） **2014 年** (n=1646)	**2015 年** (n=2268)
防火墙*	不适用	65%		31%
数据丢失保护	55%	56%		
身份验证	52%	53%		
加密/隐私/数据保护	53%	53%		
邮件/消息传送安全性	56%	52%	37%	34%
Web 安全	59%	51%	37%	31%
网络安全、防火墙和入侵防御 *	60%	不适用	35%	

* 防火墙和入侵防御在 2014 年是一个代码：“网络安全、防火墙和入侵防御”。

来源：思科 2015 年安全功能基准研究

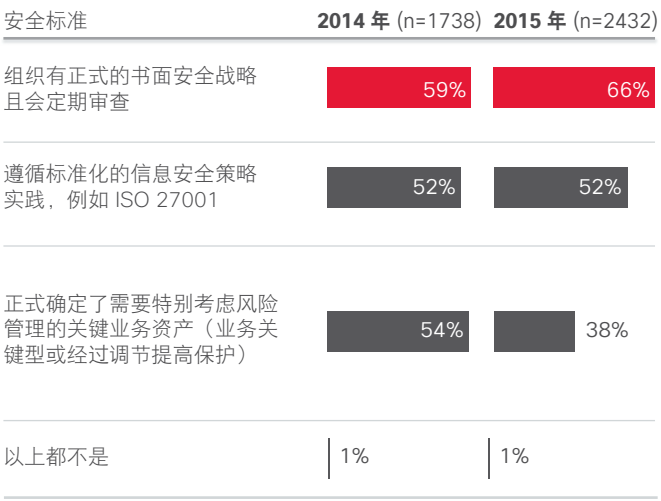
功能：信心下降

2015 年，安全专业人员对其安全基础设施保持最新状态的信心比 2014 年有所下降。毫无疑问，知名度极高的针对各大企业层出不穷的攻击、相应的专用数据盗窃和网络被攻破的公司的公开道歉是出现这种信心下降的原因。

不过，伴随这种信心下降而来的，是对制定更有力的策略日渐高涨的兴趣。如图 47 所示，2015 年制定了正式书面安全战略的公司 (66%) 多于 2014 年 (59%)。

图 47. 制定正式安全策略的组织增加

近三分之二已经通过标准化安全策略或实践的认证。



来源：思科 2015 年安全功能基准研究

分享

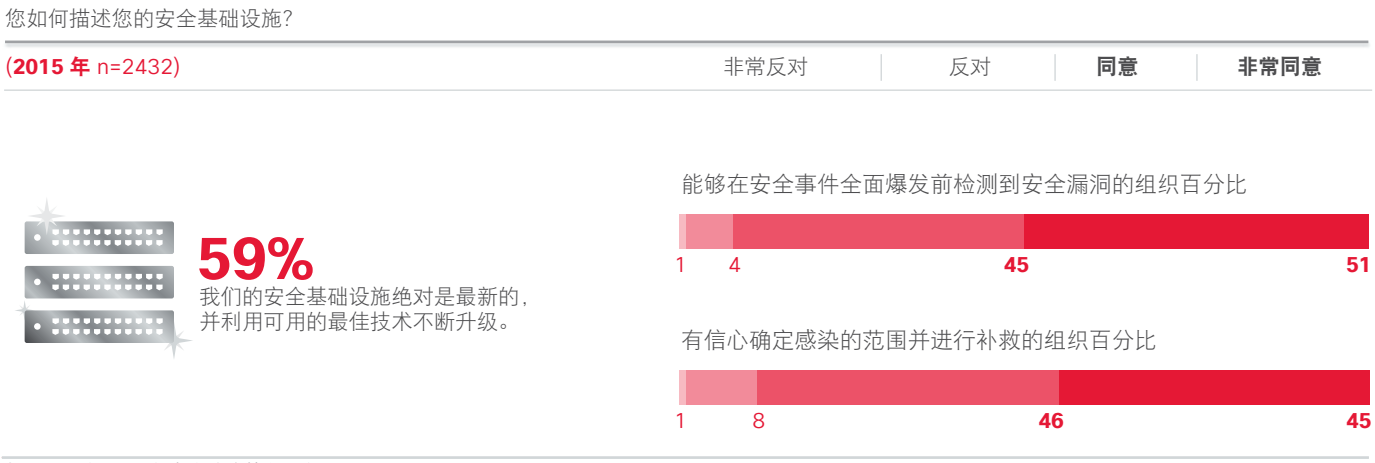
图 48. 2015 年信心下降

来源：思科 2015 年安全功能基准研究

信心下降的一个迹象是安全专业人员对其技术表现出的信心略有下降。2014 年，64% 的受访者表示他们的安全基础设施是最新的并且不断升级。2015 年，这一数字下降至 59%（图 48）。此外，2014 年有 33% 的受访者表示组织未配备最新的安全工具；2015 年，这一数字提高到 37%。

首席安全官的信心更高一点，他们比安全运营经理更乐观：65% 的首席安全官认为他们的安全基础设施是最新的，而安全运营经理中只有 54% 这样认为。安全运营经理的信心受挫可能是因为他们负责应对日常安全事件，致使他们对自身安全防范状况的看法比较消极。

图 49. 对能否检测到漏洞的信心并不相同

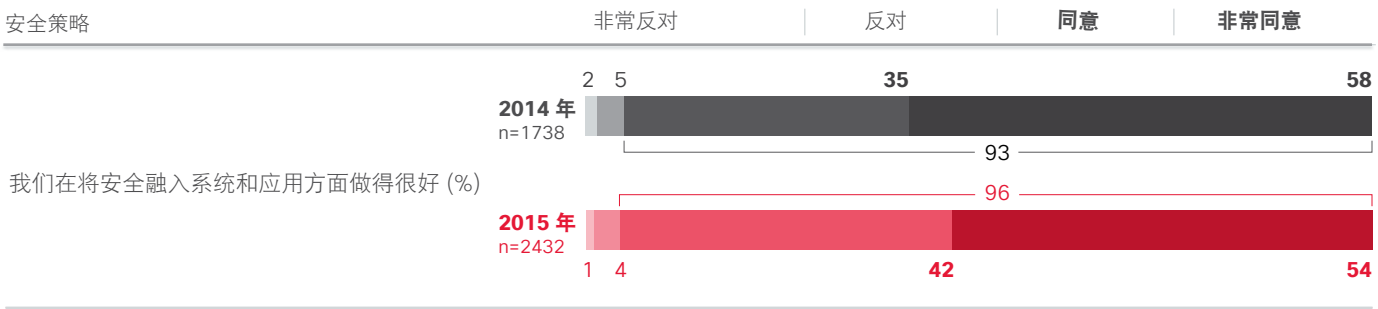


来源：思科 2015 年安全功能基准研究

安全专业人员对自己挫败攻击者的能力也表现出不同程度的信心。51% 的受访者坚信能够在安全事件全面爆发前检测到安全漏洞；只有 45% 的受访者自信能够确定网络感染的范围并对造成的损害进行补救（请参阅图 49）。

安全专业人员对自己防止网络遭受攻击的能力所表现出的信心也有所降低。例如，2015 年坚信自己在将安全融入系统的购买、开发和维护流程方面做得很好的专业人员有所减少（2015 年有 54%，而 2014 年有 58%；请参阅图 50）。（有关完整列表，请参阅**第 76 页**。）

图 50. 对能否将安全融入系统的信心有所下降



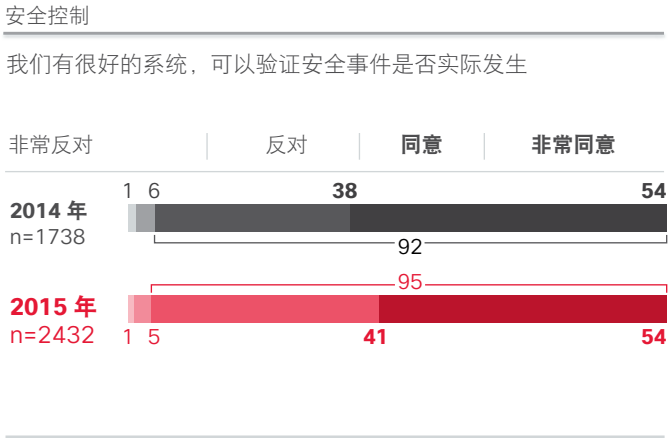
来源：思科 2015 年安全功能基准研究

分享

在某些方面，对安全功能的信心不是非常高。例如，2015 年只有 54% 的受访者表示他们认为自己有很好的系统，可以验证安全事件是否实际发生（请参阅图 51）。（有关完整列表，请参阅**第 77 页**。）

受访者对其系统能否确定这些感染的范围并进行遏制也没有完全的信心。56% 的受访者表示他们会定期、正式、战略性地审查和改进安全实践；52% 的受访者认为他们的各种安全技术很好地融为一体，有效地共同发挥作用（请参阅图 52）。（有关完整列表，请参阅**第 79 页**。）

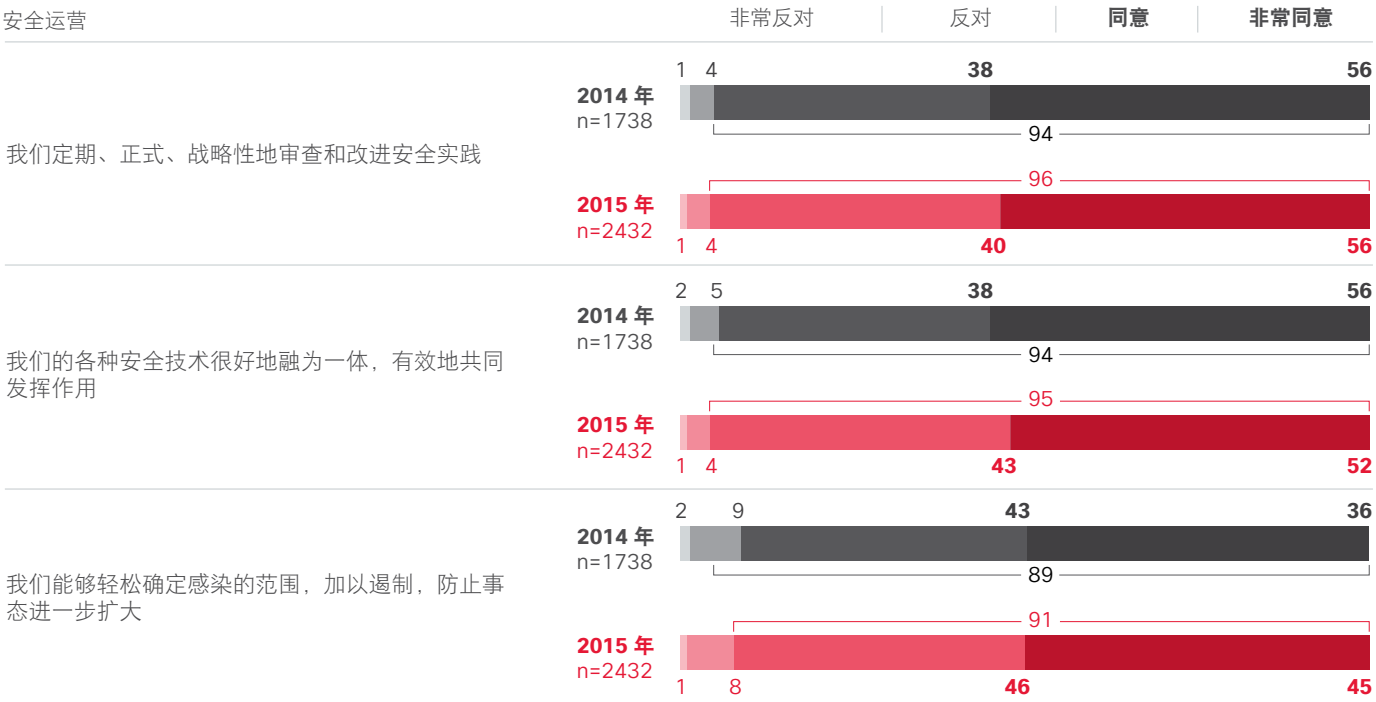
图 51. 企业认为自己拥有良好的安全控制



来源：思科 2015 年安全功能基准研究

分享

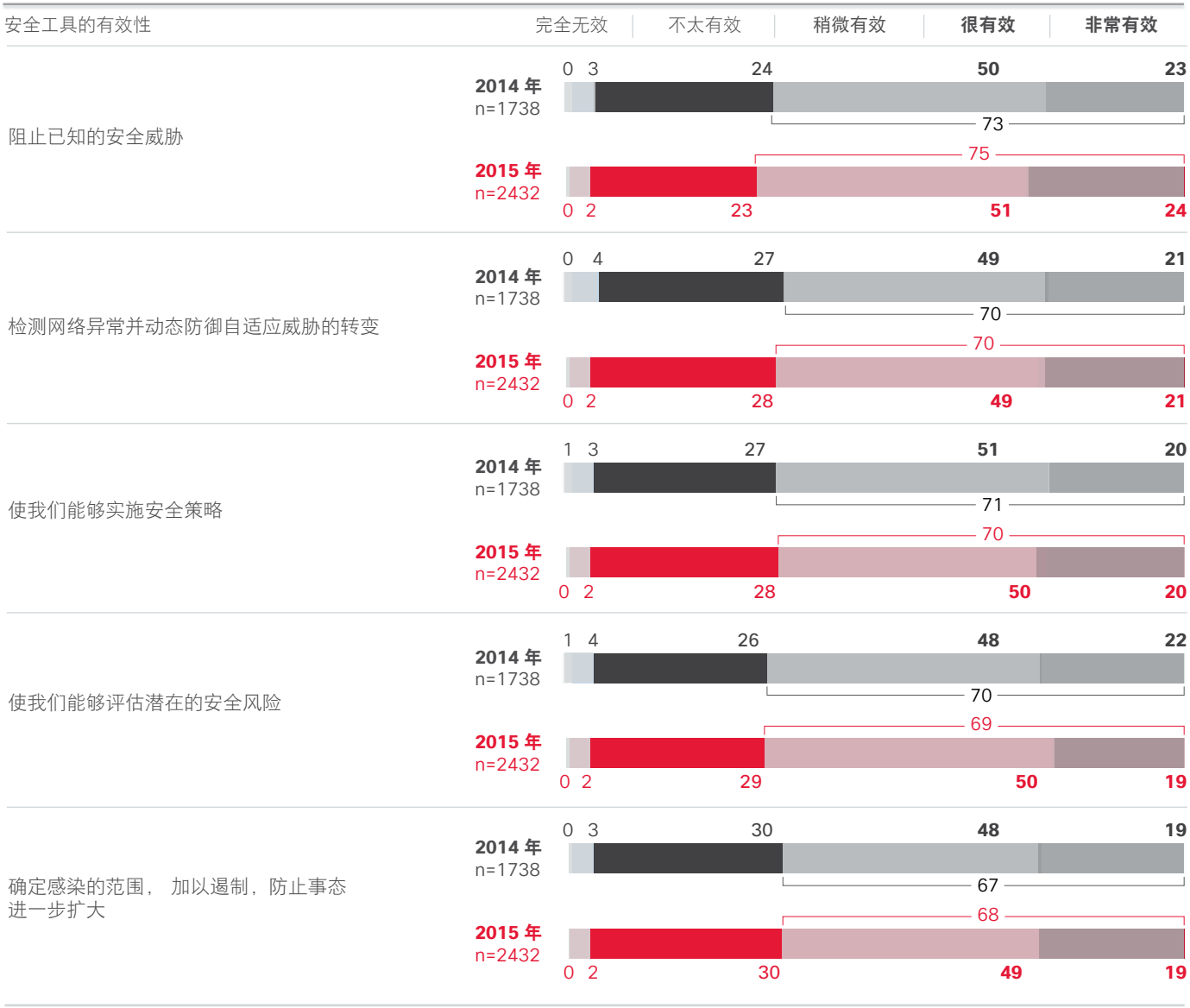
图 52. 企业对能否遏制感染的信心并不相同



来源：思科 2015 年安全功能基准研究

图 53. 四分之一的企业认为安全工具只是稍微有效

与去年类似，超过四分之一的受访者认为他们的安全工具只是“稍微有效”，而不是“很有效”或“非常有效”



来源：思科 2015 年安全功能基准研究

与 2014 年的受访者类似，2015 也有超过四分之一的安全专业人员表示他们认为自己的安全工具只是稍微有效（图 53）。

公开的安全漏洞事件对组织而言往往是决定性时刻。一旦发生这种事件，组织似乎就会更加认识到需要防止未来出现漏洞。但是，2015 年表示组织必须处理公开的安全漏洞事件的安全专业人员有所减少：2014 年这样回答的专业人员占 53%，而 2015 年只占 48%（图 54）。

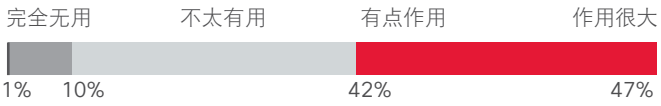
专业人员承认，漏洞具有提醒他们认识到加强安全流程的重要性的价值：47% 的受到公开漏洞影响的安全专业人员表示，漏洞促成了更完善的策略和程序。例如，43% 的受访者表示他们在公开漏洞发生后增加了安全培训，42% 的受访者表示增加了对安全防御技术的投资。

令人欣慰的是，深受公开漏洞之害的组织愈加可能加强其安全流程。2015 年，97% 的安全专业人员称其每年至少会进行一次安全培训，较之 2014 年的 82% 有很大提高（请参阅图 90 [**第 82 页**]）。

图 54. 公开漏洞可提高安全性

贵组织是否曾因安全漏洞而受到公众关注？(n=1701)（n=1347）

漏洞对于推动贵组织改进安全威胁防御策略、 程序或技术的作用有多大？ (n=1134)



来源：思科 2015 年安全功能基准研究

图 55. 进行安全培训的组织有所增加

2015 年，43% 的受访者表示他们在出现公开漏洞后加强了安全培训。

来源：思科 2015 年安全功能基准研究

成熟度：在所有成熟度级别，预算限制都是排名靠前的要因

随着组织部署更加完善的安全实践和策略，他们对自身安全防范状况的看法可能会改变。思科 2015 年安全功能基准研究根据调查受访者有关其安全流程的回答，将受访者及其组织归入五个成熟度类别（图 56）。该研究调查了功能、行业和国家/地区等不同特征对成熟度的影响。

有趣的是，在实施更完善的安全流程和工具方面，不同成熟度的组织似乎面临着一些同样的障碍。虽然具体的百分比可能不尽相同，但是预算限制在各个成熟度级别始终位居挑战排行榜的榜首（图 57）。

图 56. 成熟度模型根据安全流程评定组织

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。

	级别		5 类分割法
优化阶段	1	专注于流程改进	高
量化管理	2	定量度量和控制流程	中高
形成定义	3	体现组织特点的流程；通常为主动式	中
可重复	4	体现项目特点的流程；通常为被动式	中低
初始	5	采用不可预测的临时流程	低

来源：思科 2015 年安全功能基准研究

图 57. 对采用更高级安全的障碍不受成熟度的影响

您认为以下哪些项是采用高级安全流程和技术的最大障碍？

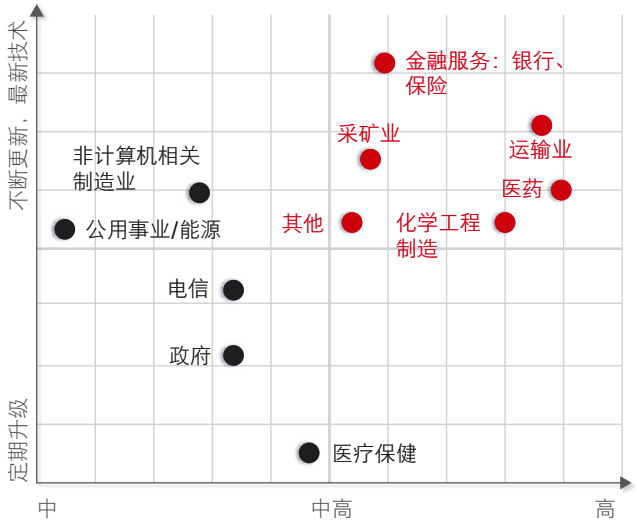
完善程度	低	中低	中	中高	高
预算限制	41%	48%	39%	38%	38%
高级管理层的支持	14%	20%	20%	22%	19%
优先事项冲突	19%	27%	26%	26%	22%
缺少经过培训的人员	21%	27%	22%	19%	23%
缺乏有关高级安全流程和技术的知识	31%	20%	25%	23%	22%
与旧版系统的兼容性问题	21%	28%	29%	34%	33%
优先事项冲突	14%	17%	26%	27%	25%
关于安全的组织文化态度	31%	23%	22%	25%	22%
在其经过市场检验之前不愿购买	12%	25%	24%	25%	19%
当前工作负载太繁重，以致无法承担新的职责	36%	23%	25%	25%	22%

来源：思科 2015 年安全功能基准研究

右图标出了各行业安全基础设施的质量和成熟度。此图根据调查受访者对其安全流程的看法绘制。位于右上象限的行业表现出最高级别的成熟度和基础设施质量。

下图显示了按行业划分的思科成熟度分布情况。2015 年，运输和医药行业近半接受调查的组织归类为高成熟度。与 2014 年相比，2015 年电信和公用事业行业归类为高成熟度的可能性较低。结果基于调查受访者对其安全流程的看法。

图 58. 按基础设施和行业测定安全成熟度

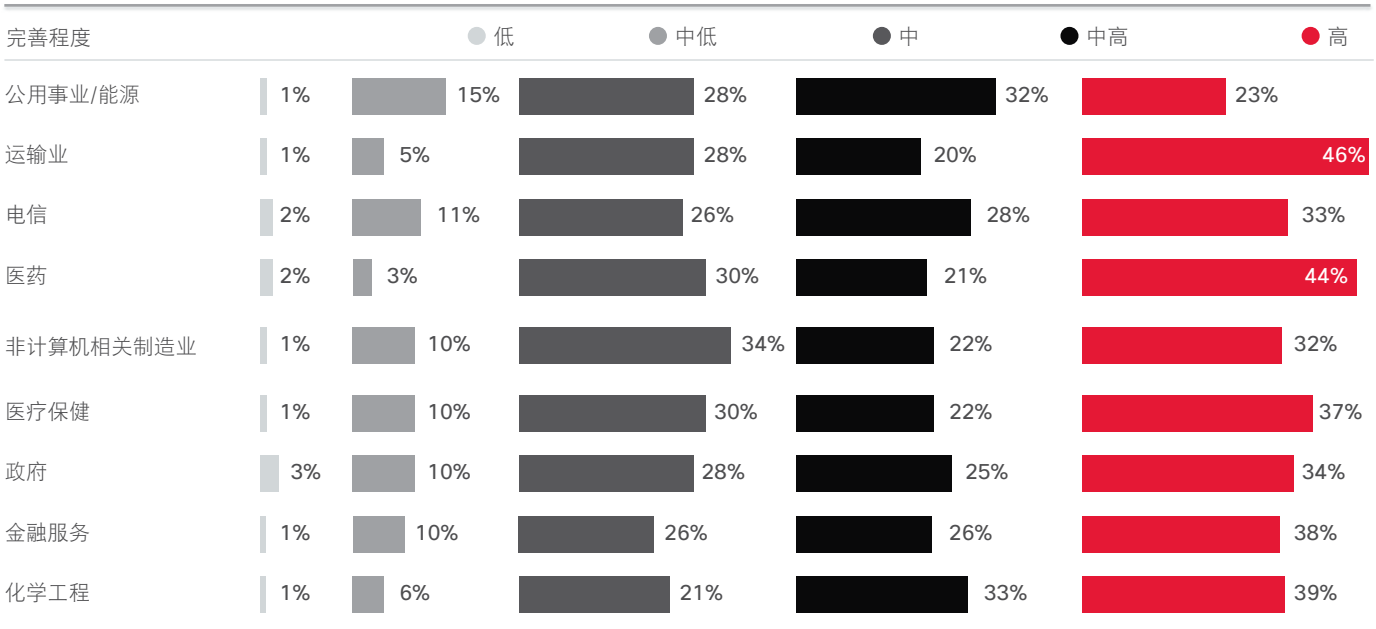


来源：思科 2015 年安全功能基准研究

分享

图 59. 按行业划分的成熟度

类的分布（按行业）

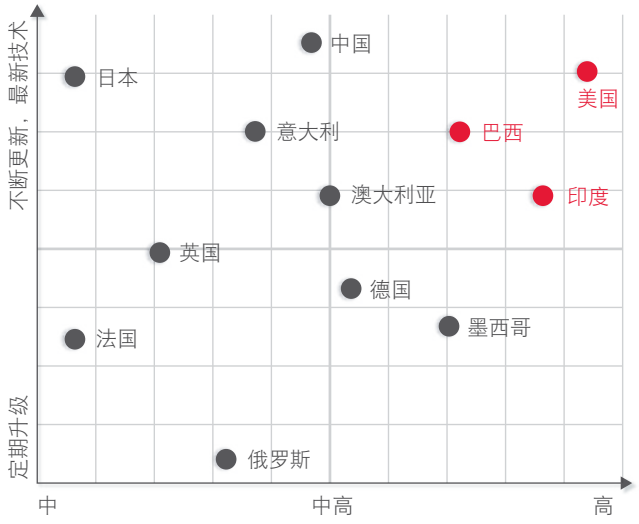


来源：思科 2015 年安全功能基准研究

右图标出了各国家/地区安全基础设施的质量和成熟度。位于右上象限的国家/地区表现出最高级别的成熟度和基础设施质量。请务必注意，这些结果基于安全专业人员对其安全防范状况的看法。

下图显示了按国家/地区划分的思科成熟度分布情况。结果基于调查受访者对其安全流程的看法。

图 60. 按基础设施和国家/地区测定安全成熟度



来源：思科 2015 年安全功能基准研究

图 61. 按国家/地区划分的成熟度

类的分布（按国家/地区）	**2014 年** (n=1637)			**2015 年** (n=2401)	
完善程度	2014	低	中低	中	中高	高
美国	3% / 2%	10% / 4%	27% / 22%	16% / 27%	44% / 45%
巴西	2% / 1%	5% / 9%	24% / 24%	35% / 26%	34% / 40%
德国	1% / 1%	4% / 12%	27% / 24%	25% / 24%	43% / 39%
意大利	1% / 4%	23% / 3%	13% / 36%	25% / 23%	38% / 34%
英国	8% / 0%	8% / 14%	25% / 32%	18% / 22%	41% / 32%
澳大利亚	9% / 1%	7% / 5%	19% / 29%	35% / 36%	30% / 29%
中国	0% / 0%	3% / 6%	32% / 37%	29% / 25%	36% / 32%
印度	7% / 1%	3% / 4%	20% / 21%	16% / 34%	54% / 40%
日本	7% / 2%	15% / 16%	14% / 34%	40% / 16%	32% / 32%
墨西哥	6%	8%	20%	16%	50%
俄罗斯	1%	14%	27%	26%	32%
法国	1%	15%	35%	20%	29%

来源：思科 2015 年安全功能基准研究

建议：对现状核实作出反应

正如思科安全功能基准研究所示，现实已经摆在安全专业人员面前。安全专业人员对于自身安全防范状况能否阻止攻击者的信心在动摇。但是，根据安全培训和正式策略的制定有所增加来判断，通过知名度极高的漏洞攻击来核实现状对于安全行业具有积极的效果。此外，审核和事件响应服务的外包更加频繁也表明防御者在寻求专家的帮助。

企业应继续增强安全防范意识，而安全专业人员则必须支持预算支出增长，从而为技术和人员提供支持。此外，当安全人员部署了适当的工具，不仅可以检测出威胁，而且能遏制其影响并进一步了解预防未来攻击的方式之后，信心就会提高。

展望

展望

本节提供思科地缘政治专家就互联网治理不断变化的格局提出的见解，内容包括数据传输立法方面的变化和关于采用加密的争论。本节还将介绍两项思科研究的重要发现。一项研究是调查高管对网络安全的担忧。另一项研究是关注 IT 决策者对安全风险和可信度的看法。我们还将概述集成式威胁防御架构的价值，并说明思科在减少检测时间 (TTD) 方面的最新进展。

地缘政治视角：互联网治理格局的不确定性

在后斯诺登时代，互联网治理的地缘政治格局已经发生了显著变化。现在，围绕跨境信息的自由流动存在普遍的不确定性。奥地利隐私维权人士 Max Schrems 对社交网络巨头 Facebook 提起诉讼的标志性事件产生了巨大的影响，导致欧洲联盟法院 (CJEU) 于 2015 年 10 月 6 日推翻《美国安全港协定》。[7]

因此在当前形势下，公司在将数据从欧盟向美国传输时不得不依靠安全港之外的机制和法律保障，向欧盟传输时，美国数据也要接受调查。目前，多家数据公司仍在尝试评估这一变化所产生的影响。此外，虽然近两年欧盟和美国官方一直在寻找安全港的替代方案，但人们对预期的新机制仍忧心忡忡。一种担忧是新方案无法在 2016 年 1 月截止日期之前实现；另一种更实际的担忧是，如果新方案无法完全解决 CJEU 的顾虑，并再次被证明可能无效，那么市场信心将无法恢复。[8]

数据保护专家希望 2.0 版安全港不像之前的安全港那样存在争议。它可能依然会重蹈覆辙，在法院受到质疑，然后也被宣告无效。[9]

新的一年中，政府和行业部门之间还将大量讨论端到端加密，包括它能够为消费者和组织带来哪些好处，以及它对执法机构在调查犯罪活动和恐怖活动方面形成何种挑战。2015 年 11 月在巴黎发生的恐怖袭击使得一些政策制定者更加倡导向调查人员提供访问加密通信内容的能力。[10] 这可能会推动 2.0 版安全港的形成，因为相对于安全问题，公民自由问题将退居次要位置。

[7] “欧盟法院宣布欧盟的美国安全港决策无效”，CJEU，2015 年 10 月 6 日：**http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf**。

[8] “随着一月份截止日期临近，2.0 版安全港框架面临失败结局”，作者：Glyn Moody，*Ars Technica*，2015 年 11 月 16 日：**http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/**。

[9] “随着一月份截止日期临近，2.0 版安全港框架面临失败结局”，作者：Glyn Moody，*Ars Technica*，2015 年 11 月 16 日：**http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/**。

[10] “巴黎袭击事件激化加密争论”，作者：Danny Yadron、Alistair Barr 和 Daisuke Wakabayashi，*华尔街日报*，2015 年 11 月 19 日：**http://www.wsj.com/articles/paris-attacks-fan-encryption-debate-1447987407**。

考虑到这样的不确定性，组织应对数据提供商作何要求，才能确保其业务符合数据传输法规要求？ 就短期而言，他们当然应寻求供应商的保证，确保在向欧盟之外传输数据时不仅使用安全港，而且还使用“欧盟标准合同条款”或“企业约束规则”。

组织应密切关注的另一个重要地缘政治问题则与漏洞及漏洞攻击相关。一些政府对未修补漏洞（即所谓的武器化软件）市场的兴起表示强烈担忧。由于安全研究界一直在寻找保护全球网络的方法，这些工具对他们而言至关重要。但是，如果技术旁落到错误的人手中，尤其是那些受压制团体的人手中，则极有可能被用于金融犯罪、窃取国家机密和商业秘密、抑制不同政见或破坏重要基础设施。

如何限制对未修补漏洞的访问，同时不限制执行重要研究的人接触这些漏洞，是未来几个月甚至几年政府明确要努力解决的问题。当尝试解决这个棘手的难题时，政府需要谨慎评估其决策对安全的影响。例如，如果不明确管制未发布漏洞信息传输的法律，则会阻碍安全威胁研究的进展，或纵容在供应商有机会修补漏洞之前公开漏洞。任何用于解决这种不确定性的方法都应在全球范围适用。

网络安全问题重压于高管心头

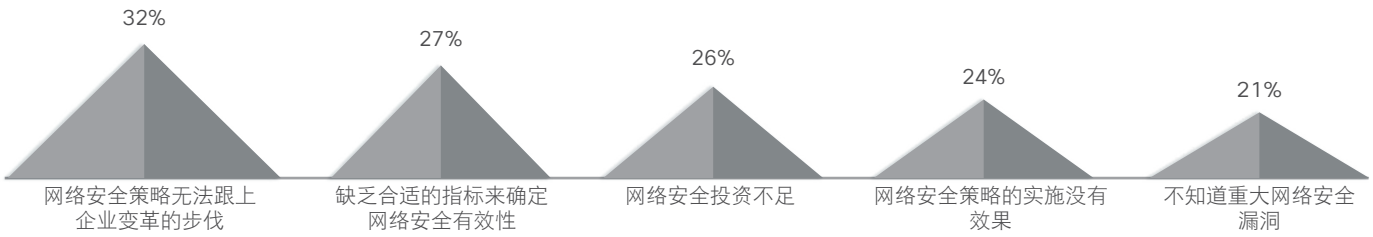
显然，高度安全性可以帮助企业避免灾难性漏洞和攻击。但是，它能否有助于公司取得成功？ 根据 2015 年 10 月思科就网络安全对业务和数字化战略的作用在财务和业务部门高管中执行的一项调查，企业高管理解保护企业免受威胁可能是决定他们能否成功的重要因素。随着组织更加数字化，组织增长将取决于其保护数字平台的能力。

调查显示，高管们越来越关心网络安全：针对网络安全漏洞，48% 的受访高管表示自己非常担心，39% 的受访高管表示他们比较担心。这种担忧与日俱增，41% 的受访者表示与三年前相比，他们对安全漏洞的担忧增加很多，42% 的受访者表示他们的担忧比过去略有增加。

企业领导者也认为投资者和监管者将对安全流程提出更加严格的要求，就像对其他企业职能部门的要求一样。92% 的受访者均同意，监管者和投资者今后将希望公司提供更多有关网络安全风险暴露程度的信息。

企业也似乎已经敏锐地感觉到了所面临的网络安全挑战。根据受访者的回复，最常见的一项挑战是网络安全策略无法跟上商业变化的步伐，其次是缺乏衡量指标来确定安全方案的有效性（图 62）。

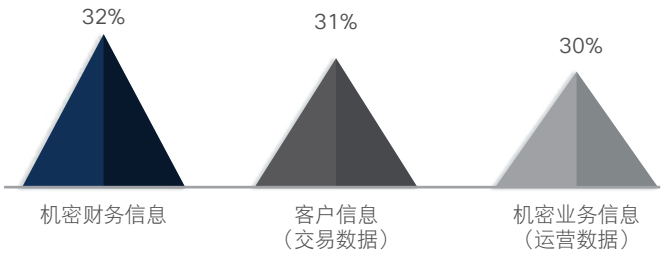
图 62. 企业正面临严峻的网络安全挑战



来源：思科安全研究部门

大约三分之一的高管还担心他们保护重要数据的能力。在被问及最难保护的信息类型时，32% 的受访者选择了“机密财务信息”。受访者将“客户信息”和“机密商业信息”列为其次两个最难保护的数据类型（请参阅图 63）。

图 63. 高管对保护关键数据安全的担忧



来源：思科安全研究部门

可信度研究：为企业面临的风险和挑战带来一线曙光

信息安全漏洞持续增长加强了企业对信任的需求，企业需要相信其系统、数据、业务合作伙伴、客户和公民都是安全的。我们发现信任成为企业选择 IT 和网络基础设施的主要因素。事实上，很多企业都要求在构成其基础设施的全部解决方案整个产品生命周期内都集成安全性和可信度方案。

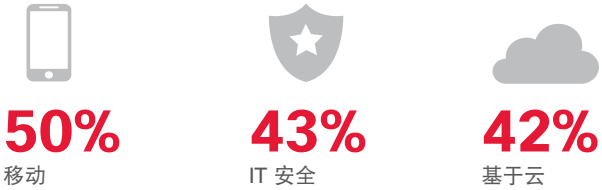
2015 年 10 月，思科执行了一项研究来评估 IT 决策者对所面临安全风险和挑战的看法，从而确定 IT 供应商可信度在 IT 投资中的作用。我们调查了多个国家/地区不同组织中的信息安全和非信息安全决策者。（有关安全风险和可信度研究的更多详细信息，包括我们的方法，请参阅**附录**。）

以下是我们的研究的一些重要发现：

我们发现 65% 的受访者认为自己的组织面临相当大的安全风险，主要包括企业中移动设备的使用、IT 安全性和基于云的解决方案（图 64）。

图 64. 对安全风险的看法

企业认为组织的基础设施在以下方面存在很高的安全漏洞风险：



来源：思科安全风险和可信度研究

分享

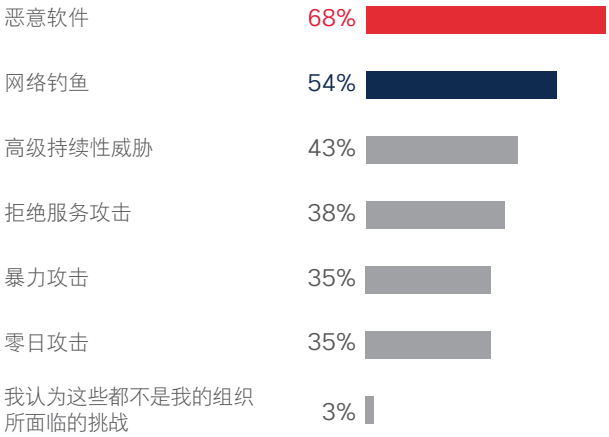
68% 的受访者认为恶意软件是其所在组织面临的头号外部安全挑战。前三大挑战中，另两大挑战为网络钓鱼和高级持续性威胁，分别占 54% 和 43%（请参阅图 65）。

针对内部安全挑战（请参阅图 66），超过一半的受访者 (54%) 认为恶意软件下载是最大威胁，接下来为员工造成的内部安全漏洞 (47%) 和硬件与软件漏洞 (46%)。

我们还发现大多数企业 (92%) 都在组织内部配备了专门的安全团队。88% 的受访者表示他们拥有定期更新的覆盖全组织的正式安全策略。但是，只有 59% 的受访者实行标准化策略和程序来验证 IT 供应商可信度（请参阅图 67）。

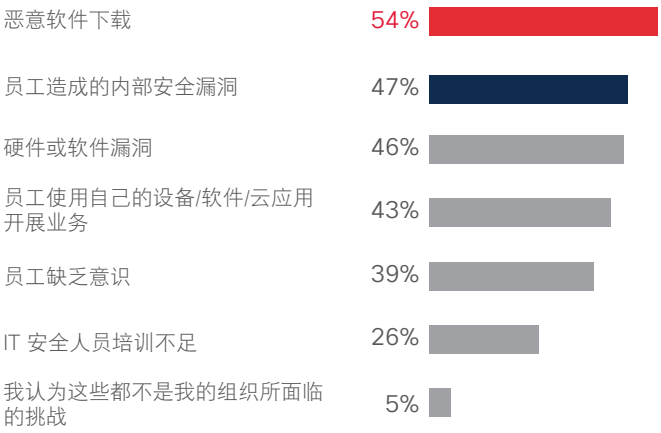
此外，约有一半 (49%) 的大型企业组织采用最新的技术来保持其安全基础设施紧跟时代步伐，而其他大多数组织会定期升级基础设施。根据我们的研究，很少有组织会等到其所采用的技术被淘汰才进行升级。

图 65. （全部受访者）所面临的外部挑战



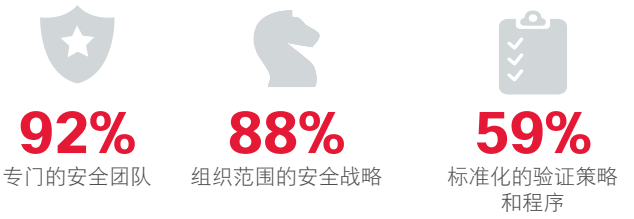
来源：思科安全风险和可信度研究

图 66. （全部受访者）所面临的内部安全挑战



来源：思科安全风险和可信度研究

图 67. 大多数大型企业都有专门的内部安全团队



来源：思科安全风险和可信度研究

分享

供应商可以如何展现可信度

在当今以威胁为中心的格局下，对供应商流程、策略、技术和人员的信任以及对供应商进行验证的能力将是构建供应商与企业之间持续、信任关系的关键。

技术供应商可通过以下方面展现其可信度：

- 从一开始就将安全纳入到其解决方案和价值链中
- 制定并落实降低风险的策略和流程
- 营造注重安全的文化
- 快速和透明地应对漏洞
- 发生安全事件后提供快速补救和保持持续警惕性

当然，升级基础设施是很好的做法。各种规模的组织都需要部署安全、值得信赖的基础设施，确保网络所有方面的安全性。然而，组织也可以通过培养开放、注意安全的文化，缩小受攻击面。

构建这种文化要求组织实施覆盖整个企业的一致的策略和流程，确保安全性落实到企业的各个层面。然后，他们必须向合作伙伴与供应商生态系统传输这种以安全为中心的观念，并且不断向客户、合作伙伴和其他利益相关者展示其透明度与可靠性。

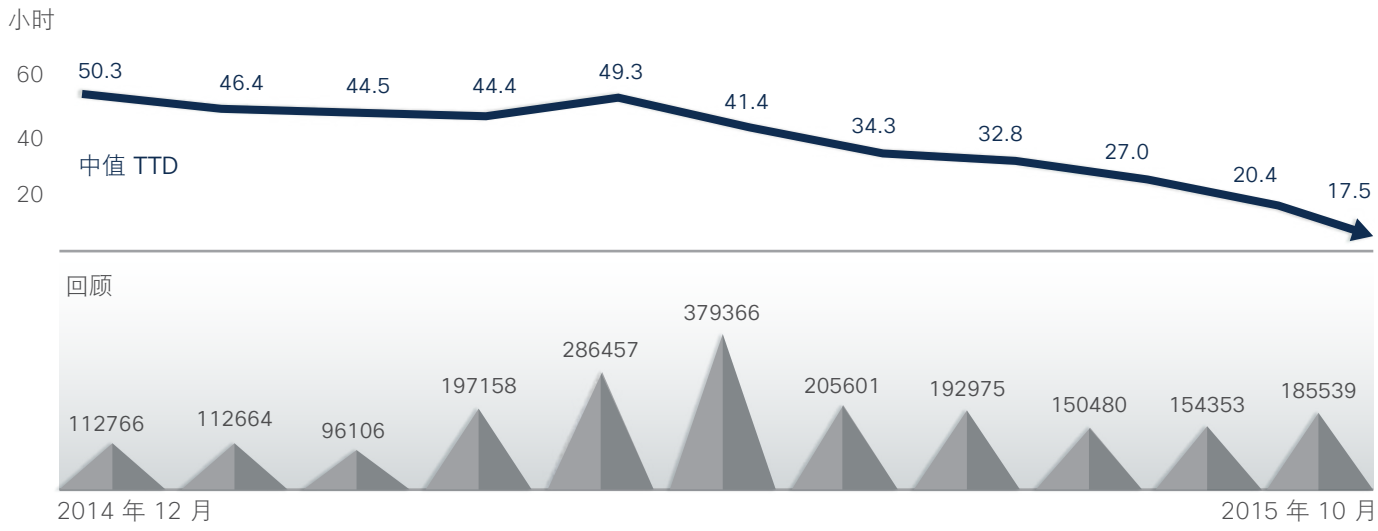
检测时间：不断缩短空档期的竞赛

我们将“检测时间”或“TTD”定义为窗口时间，指第一次观察某文件到检测为威胁之间的这段时间。我们使用从全球部署的思科安全产品收集的选择性安全遥感勘测数据来确定这个窗口时间。

图 68 中的“回顾”类别显示了思科最初将其归为“未知”，之后改为“已知恶意”类别文件的数量。

据《思科 2015 年年中安全报告》所报告，TTD 中值约为两天（50 小时）。

图 68. 2014 年 12 月至 2015 年 10 月的检测时间



来源：思科安全研究部门

从 1 月到 3 月，TTD 中值大致相同，都在 44 至 46 小时之间，并略呈下降的趋势。在 4 月有小幅上升，达到 49 小时。然而，到 5 月底，思科的 TTD 已降至大约 41 小时。

此后，TTD 中值开始快速下降。截至 10 月，思科已将 TTD 中值降低至约 17 小时，低于一天。这远低于 TTD 的当前行业估计值，即 100 至 200 天。这种速度得益于采用了有关如何缓解短期感染的更多细节。

黑客活动的产业化及商业恶意软件的大量使用对我们缩短 TTD 窗口时间的能力发挥了重大作用。随着威胁产业化，威胁传播范围更广，因此也更容易检测。

尽管如此，我们建议将高级威胁防御手段相互结合以及熟练的安全研究人员之间的紧密协作，这对整个 2015 年持续大幅降低 TTD 中值可能更为重要。

图 69. 2014 年 12 月至 2015 年 10 月的检测时间比较

来源：思科安全研究部门

分享

图 69 中的 TTD 比较表明 6 月份多数威胁都是在 35.3 小时左右的时间内被捕获。而到 9 月底，更多威胁都在约 17.5 小时内被终止。同样，我们认为 TTD 中值降低的部分原因是可以更快识别商业恶意软件，例如 Cryptowall 3.0、Upatre 和 Dyre。集成了思科公司 ThreatGRID 等提供的新技术是另一个因素。

但是，即便 TTD 时间窗口缩小，仍有一些威胁比其他威胁更难以检测。针对 Microsoft Word 用户的下载程序通常最容易检测（< 20 小时）。广告软件和浏览器注入属于最难检测的威胁（<200 小时）。

后面这些威胁之所以如此难以检测的一个原因是安全团队通常将其列为低优先级，在抵御攻击者猛烈的零日攻击的斗争中通常会忽略这些威胁（请参阅“浏览器感染：传播广泛而且是数据泄露的一个主要原因”[**第 16 页**]）。

图 70 提供通常在 100 天以内被发现的威胁的类型概览。

图 70. 100 天的标记云

来源：思科安全研究部门

集成式威胁防御的六个原则

在《思科 2015 年年中安全报告》中，思科安全专家提出对自适应集成解决方案的需求将导致未来五年内安全行业发生重大变化。变化的结果，是行业将发生整合，并统一转向可扩展的集成式威胁防御架构。这种架构能够提供跨多个解决方案的可视性、可控性、情报和情景。

这种“检测并响应”的框架将有助于加快对已知威胁或新型威胁的应对速度。此新架构的核心是一个可视性平台，该平台可提供全面的情景感知并会持续更新，从而帮助评估威胁、关联本地和全球情报，以及优化防御。此平台的目的是为所有供应商建立一个可以操作并集合众力的基础。有了可视性，就能实现更高的可控性，从而更有效地抵御各种威胁媒介，并击败更多攻击。

下面，我们列出集成式威胁防御的六个原则，以帮助组织及其安全供应商更好地理解此架构的目的和潜在优势。

1. **要应对日益增多且更加老练的威胁发起者，需要使用功能更丰富的网络和安全架构。**

   在过去的 25 年中，传统的安全模式一直是“发现一个问题，就购买一种设备”。但是，这些解决方案通常是由多家不同安全供应商提供的一系列技术，它们之间无法以任何有意义的方式相互协作。它们产生与安全事件相关的信息和情报，将其集成于事件平台，然后由安全人员执行分析。

   集成式威胁防御架构是一种检测和响应框架，可通过以高效的自动化方式从所部属的基础设施收集更多信息，来提供更多功能并加快威胁应对速度。这种框架会以更智能的方式观察安全环境。它并非仅限于提醒安全团队可疑事件和违反策略的情况，它还能对网络及网络上发生的情况提供更高的可视性，以帮助就安全问题作出更明智的决策。

2. **单凭独立的技术无法应对当前或未来的威胁形势，而只会提高网络环境的复杂性。**

   很多组织都投资于“一流”安全技术，但是他们如何知道这些解决方案是否真的有效？ 过去一年里的各类有关重大安全漏洞的头条新闻，就是很多安全技术并不凑效的例证。不仅如此，这些技术一旦出现问题，往往会带来严重的后果。

   很多提供一流解决方案的安全供应商都无助于安全环境的改善，除非他们提供的解决方案与其竞争对手截然不同，而非大同小异。但是，如今大多数核心安全领域的主要供应商提供的很多产品与服务都不存在显著差异。

3. **鉴于加密流量的增多，集成式威胁防御必须能集中火力击溃加密恶意活动（某些产品已经对加密恶意活动失去效力）。**

   正如此报告中所述，加密网络流量日益增加。当然，使用加密的做法是合理的，但是加密也让安全团队难以跟踪威胁。

   要解决由加密带来的“问题”，途径就是对设备或网络上发生的情况提供更高可视性。集成式安全平台可帮助实现这一点。

4. **开放式 API 对集成式威胁防御架构至关重要。**

   多供应商环境需要一种能够提供更高可视性、情景和可控性的通用平台。构建一个前端集成平台有助于实现更好的自动化，并且使安全产品自身获得更高的感知能力。

5. **集成式威胁防御架构必须减少所要安装和管理的设备和软件数量。**

   安全供应商应努力打造能在单一平台上提供尽可能丰富而广泛的功能的平台。这将有助于降低安全环境的复杂性和分散性，否则会给攻击者提供太多轻松访问和隐藏的机会。

6. **集成式威胁防御在自动化和协作方面的优势可帮助减少检测时间以及控制和补救工作。**

   减少误报有助于让安全团队将重点放在最重要的问题上。情景化支持可对进行中的事件进行一线分析，帮助团队评估这些事件是否需要立即处理，并最终实现自动响应和更深入的分析。

团结就是力量：行业协作的价值

行业协作不仅对将来开发集成式威胁防御架构、实现更快的威胁响应非常重要，面对胆大妄为、挖空心思、不屈不挠的威胁发起者横行的全球形势，行业协作对于紧跟时代步伐也将发挥关键作用。攻击者越来越擅长部属难以检测而且盈利性强的攻击活动。如今，很多攻击者都通过在基础设施中部属合法资产来支持其攻击活动，并且取得了巨大成功。

鉴于这一形势，“思科 2015 年安全功能基准研究”所调查的高管对于自身帮助保障组织安全的能力不再那么自信，也就不足为奇了。我们建议防御者认真考虑积极的持续行业协作在以下方面的有力作用：检测网络犯罪活动、瓦解攻击者获取收入的能力，以及减少攻击者未来发起攻击的机会。

正如本报告前文所述（请参阅“专题报道”[从**第 10 页**开始]），思科合作伙伴计划参与者之间的协作和思科综合安全情报 (CSI) 生态系统内的协作，以及与运营商的合作，是思科之所以能发现、确定和消除涉及 Angler 漏洞攻击包的全球活动以及削弱 SSHPsychos（我们的研究人员曾观察到的最大的 DDoS 僵尸网络之一）的重要原因。

关于思科

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先进的威胁防范解决方案组合，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碎片式的方案，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、一致的可控性和先进的威胁防范。

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，来自思科综合安全智能 (CSI) 生态系统的威胁研究人员将行业领先的威胁智能汇聚到了一起。这相当于每日提取数十亿的 Web 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，帮助机器学习系统和研究人员跟踪跨网络、数据中心、端点、移动设备、虚拟系统、Web、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。

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**。

《思科 2016 年度安全报告》撰稿人

TALOS 安全情报和研究小组

Talos 是思科的威胁情报组织，这个由安全专家组成的精英团队专门为思科客户、产品和服务提供卓越的保护。Talos 由领先的威胁研究人员组成，在成熟系统的支持下，为检测、分析和防御已知和新兴威胁的思科产品创建威胁情报。Talos 维护 Snort.org、ClamAV、SenderBase.org 和 SpamCop 的官方规则集，是向思科 CSI 生态系统提供威胁信息的主要团队。

高级服务云和 IT 转型优化团队

该团队为世界各地最大型的运营商和企业提供建议并优化网络、数据中心与云解决方案。这种咨询服务关注如何最大程度地优化客户关键解决方案的可用性、性能和安全。超过 75% 的财富五百强企业均采用了这项优化服务。

主动威胁分析团队

思科主动威胁分析 (ATA) 团队利用先进的大数据技术，帮助组织抵御已知的入侵、零日漏洞攻击和高级的持续性威胁。这种全面管理服务通过我们的安全专家和我们的全球安全运营中心网络提供。一周七天，一天 24 小时提供不间断的警戒和按需分析功能。

思科思想领袖组织

思科思想领袖组织启发人们发现全球机会、市场转型以及促进组织、行业和体验转变的重要解决方案。该组织就公司在目前快速变化的世界中可以预期获得何种收获以及如何实现最佳竞争力提供敏锐的预测性分析。团队中多位思想领袖均关注通过无缝安全集成物理与虚拟环境，帮助组织实现数字化，加速创新并实现期望的业务成果。

COGNITIVE 威胁分析

思科 Cognitive 威胁分析是通过对网络流量数据的统计分析，发现在受保护网络内运行的漏洞、恶意软件和其他安全威胁的一种基于云的服务。它通过使用行为分析和异常检测，来识别恶意软件感染的症状或数据泄露，从而应对基于外围的防御的漏洞。Cognitive 威胁分析依靠高级统计建模和机器学习来独立识别新威胁，从其所发现的内容中学习，并随着时间推移而适应。

全球政府事务

思科为众多不同级别的政府机构提供支持，帮助其形成支持技术产业并有助于政府实现各项目标的公共政策和法规。全球政府事务团队负责开发和影响支持技术的公共政策和法规。通过与行业利益相关者以及相关合作伙伴合作，该团队与政府领导建立各种关系，对影响思科业务和整体 ICT 采用的政策施加影响，以帮助形成全球、全国和地方级别的政策决策。政府事务团队由前任官员、国会议员、监管者、美国高级政府官员和政府事务专业人员组成，帮助思科提倡及保护技术在全球的使用。

INTELLISHIELD 团队

IntelliShield 团队执行漏洞和威胁研究、分析、整合，以及将来自思科安全研究和运营组织的数据与信息和外部来源关联，提供 IntelliShield 安全智能服务，其支持多种思科产品和服务。

LANCOPE

Lancope 是思科旗下公司，作为网络可视性和安全情报的领先提供商，致力于保护企业抵御当今的主要威胁。通过分析 NetFlow、IPFIX 和其他类型的网络遥感勘测，Lancope 的 StealthWatch® 系统提供情景感知安全分析，以快速检测从 APT 和 DDoS 到零日恶意软件与内部威胁的各种攻击。Lancope 将对整个企业网络的持续单边监控与用户、设备和应用感知相结合，加速事件响应，改善调查分析并有效降低企业风险。

OPENDNS

OpenDNS 是思科旗下公司，作为全球最大的云交付安全平台，为遍及超过 160 个国家/地区的 6,500 多万位日常用户提供服务。OpenDNS 实验室是 OpenDNS 的安全研究团队，为安全平台提供支持。有关详细信息，请访问 **www.opendns.com** 或 **https://labs.opendns.com**。

安全和信任组织

思科安全和信任组织致力于实现思科对董事会和各国领导人最关心的两个最重要问题的承诺。该组织的核心任务包括保护思科的公共和私人客户，在思科的所有产品与服务组合中实现和确保思科的安全部属生命周期以及信任系统工作，并保护思科企业免受不断发展的网络威胁的攻击。思科采用整体方法来全面增强安全与信任，将人员、策略、流程和技术等环节全部包括在内。安全和信任组织重点围绕信息安全、信任工程、数据保护与隐私、云安全、透明与验证，以及高级安全研究与政府等领域，努力推动实现卓越运营。有关更多信息，请访问 **http://trust.cisco.com**。

安全研究和运营组织

安全研究和运营组织 (SR&O) 负责所有思科产品与服务的威胁与漏洞管理，下属成员包括行业领先的产品安全事件响应团队 (PSIRT)。SR&O 通过 Cisco Live 和 Black Hat 等活动以及通过与思科及整个行业的合作伙伴进行协作，帮助客户了解不断发展的威胁形势。此外，SR&O 努力通过创新提供各种新服务。例如，思科定制威胁情报 (CTI) 服务可以识别现有安全基础设施未检出或未缓解的感染指标。

思科合作伙伴撰稿人

LEVEL 3 THREAT RESEARCH LABS

Level 3 Communications 是一家总部位于科罗拉多州布隆菲的著名全球通信服务提供商，致力于为企业、政府和运营商客户提供通信服务。Level 3 的全球服务平台以覆盖三个大陆范围广大的光纤网络为基础，通过海底设施连接，拥有遍及超过 60 个国家/地区 500 多个市场的庞大都市资产。Level 3 的网络能够以广泛的视角判断全球威胁形势。

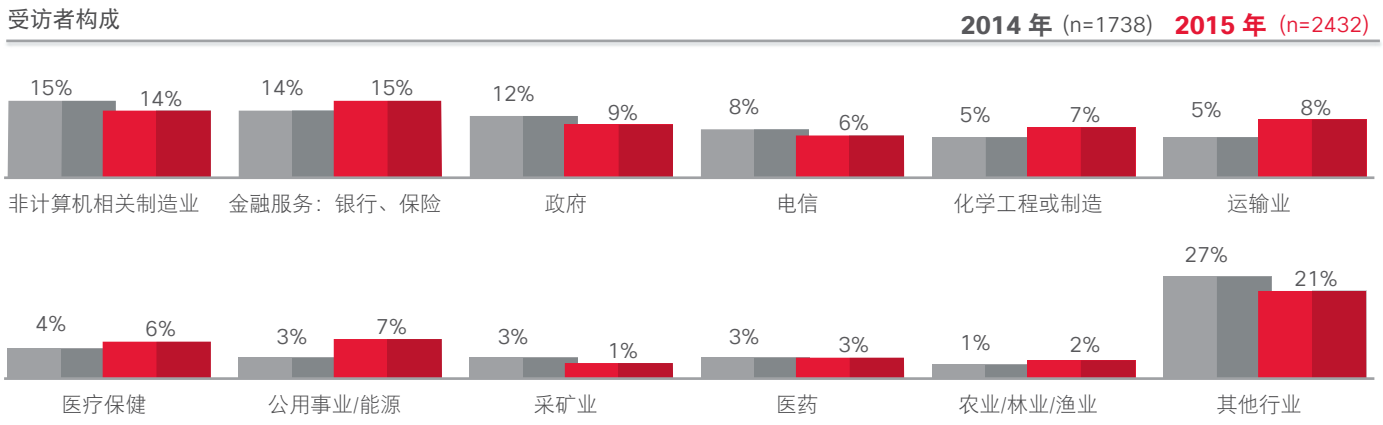
Level 3 Threat Research Labs 是一家安全组织，他们积极分析全球威胁形势并关联内部和外部信息，帮助保护 Level 3 的客户、客户网络和公共互联网。该组织定期与思科 Talos 等行业领导者合作，帮助研究和缓解威胁。

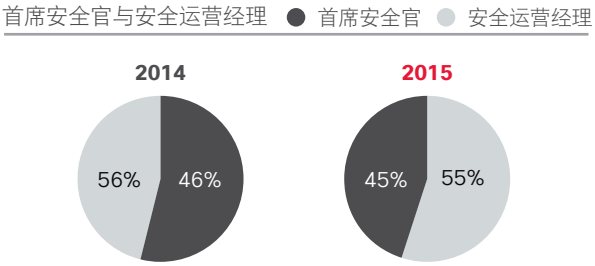
附录

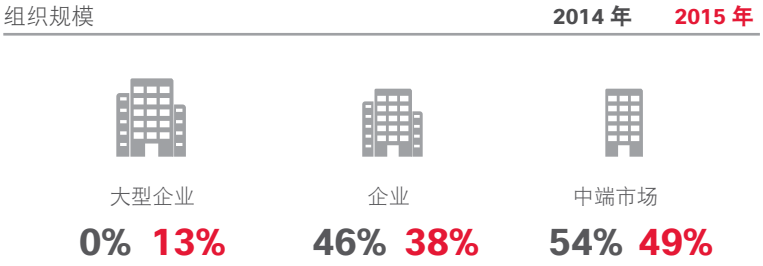
附录

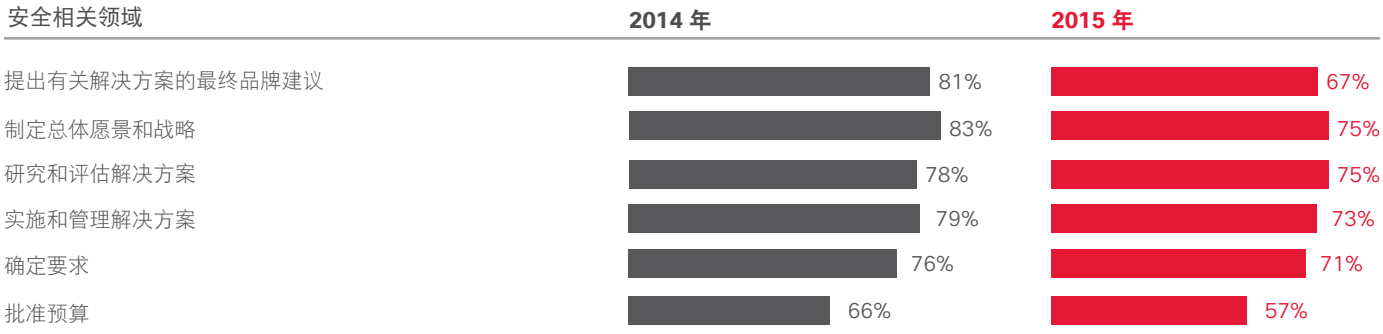
思科 2015 年安全功能基准研究：受访者构成和资源

图 71. 受访者构成





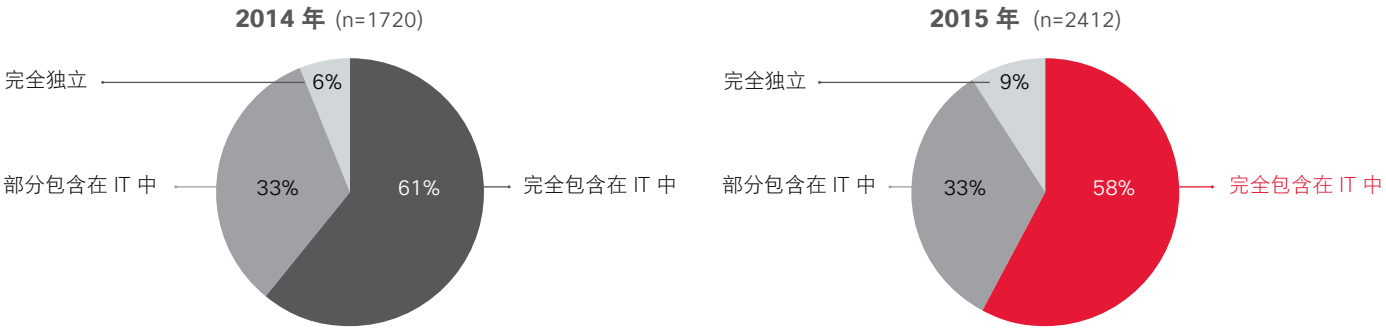




来源：思科 2015 年安全功能基准研究

图 72. 尽管只有 9% 的受访者拥有独立于 IT 预算的安全预算，但这已经比 2014 年有了显著提高

安全预算是否包含在 IT 预算内？（IT 部门成员）



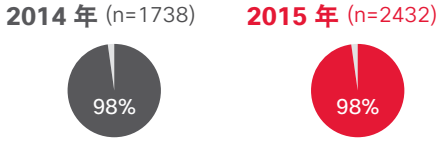
来源：思科 2015 年安全功能基准研究

图 73. 职位：受访者及其管理者

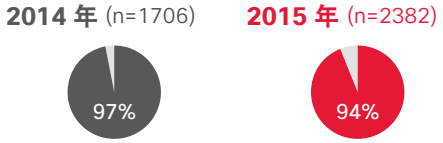
IT 部门的成员

2014 97% 与 2015 98%

专门负责安全的部门或团队



安全团队的成员



职位		经理的职位	
首席安全官	22%	首席执行官	34%
首席技术官	18%	总裁/所有者	18%
IT 总监或经理	16%	首席安全官	6%
首席信息官	13%	首席信息官	6%
安全运营总监	7%	首席技术官	6%
IT 安全副总裁	5%	IT 总监或经理	4%
风险和合规性总监	4%	IT 安全副总裁	4%
安全运营经理	4%	IT 副总裁	2%
安全架构师	4%	执行委员会	2%
IT 副总裁	3%	首席运营官	1%
首席运营官	3%	首席财务官	1%
其他职位	2%	其他职位	0%

来源：思科 2015 年安全功能基准研究

图 74. 防火墙是最常用的安全威胁防御工具；与 2014 年相比，更少的安全威胁防御方式在 2015 年通过基于云的服务进行管理

组织使用的安全威胁防御措施	**2014 年** (n=1738)	**2015 年** (n=2432)	通过基于云的服务管理防御措施（使用安全威胁防御措施的安全受访者） **2014 年** (n=1646)	**2015 年** (n=2268)
防火墙*	不适用	65%		31%
数据丢失保护	55%	56%		
身份验证	52%	53%		
加密/隐私/数据保护	53%	53%		
邮件/消息传送安全性	56%	52%	37%	34%
网络安全	59%	51%	37%	31%
终端保护/防恶意软件	49%	49%	25%	25%
访问控制/授权	53%	48%		
身份管理/用户调配	45%	45%		
入侵防御*	不适用	44%		20%
移动安全性	51%	44%	28%	24%
无线安全	50%	41%	26%	19%
漏洞扫描	48%	41%	25%	21%
VPN	48%	40%	26%	21%
安全信息和事件管理	43%	38%		
DDoS 防御	36%	37%		
渗透测试	38%	34%	20%	17%
补丁和配置	39%	32%		
网络调查分析	42%	31%		
终端设备调查分析	31%	26%		
网络安全、防火墙和入侵防御*	60%	不适用	35%	
以上都不是	1%	1%	13%	11%

* 防火墙和入侵防御在 2014 年是一个代码

* 网络安全、防火墙和入侵防御。

来源：思科 2015 年安全功能基准研究

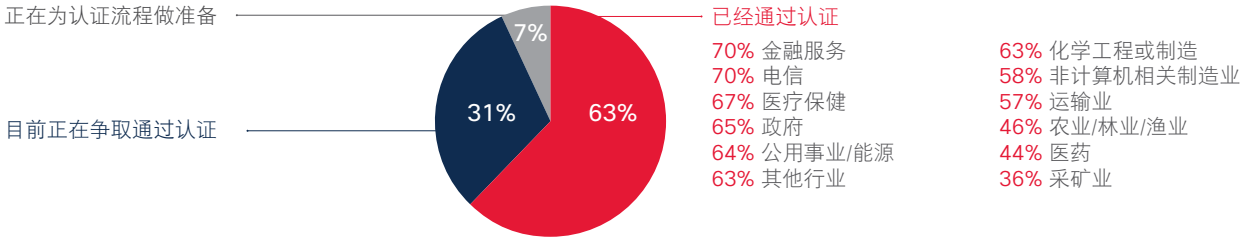
外包

图 75. 建议与咨询仍然是外包最多的安全服务

审核和事件响应的外包显著增加。 认为外包更具成本效益。

半数 (52%) 遵循标准化的安全策略实践（例如 ISO 27001），与去年相同。 其中，绝大多数已经通过认证或正在争取通过认证。

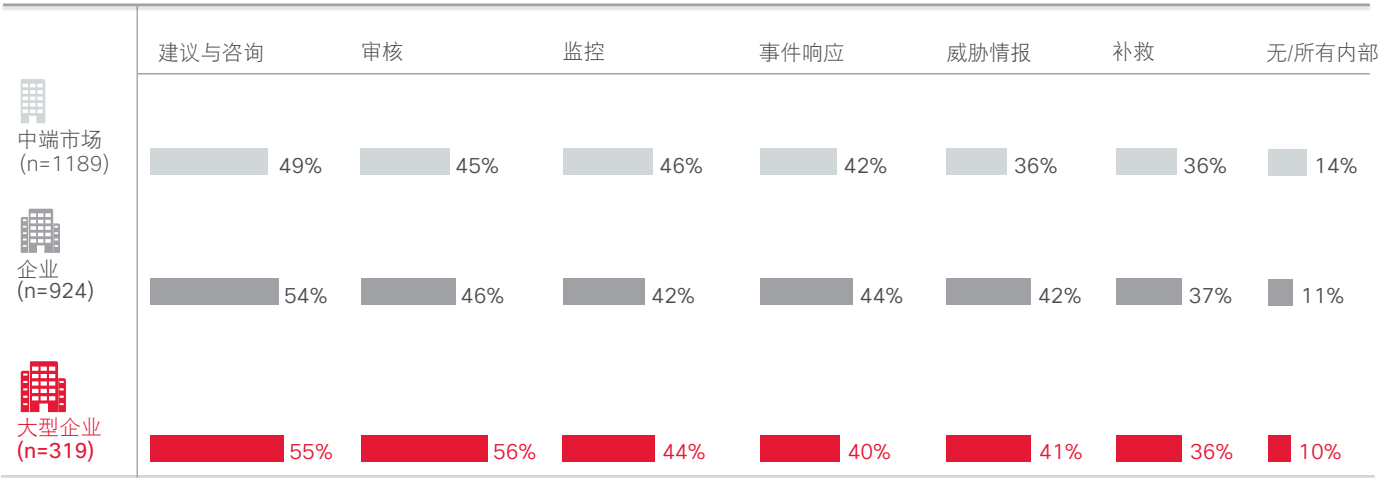
标准化的安全策略实践
组织遵循标准化的信息安全策略实践 (**2015 年:** n=1265)



来源：思科 2015 年安全功能基准研究

图 76. 企业外包概况：大型企业更愿意外包审计服务、建议与咨询服务

哪些安全服务是外包的?



来源：思科 2015 年安全功能基准研究

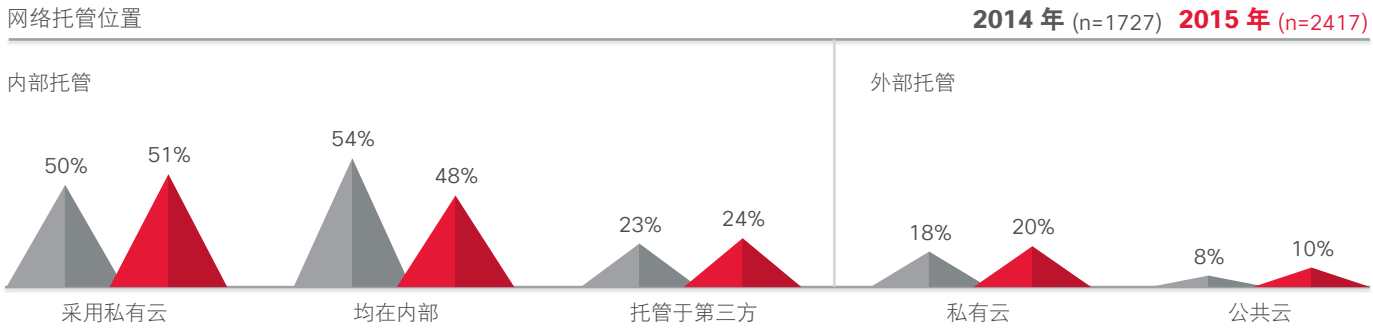
图 77. 国家/地区外包概况：日本更愿意外包建议与咨询服务

哪些安全服务是外包的?

总计	美国	巴西	德国	意大利	英国	澳大利亚	中国	印度	日本	墨西哥	俄罗斯	法国
建议与咨询 52%	52%	51%	19%	51%	44%	54%	52%	54%	64%	58%	41%	55%
审核 47%	50%	55%	38%	48%	50%	36%	33%	51%	41%	63%	40%	59%
监控 44%	48%	49%	32%	39%	41%	52%	31%	51%	51%	49%	37%	50%
事件响应 42%	46%	39%	32%	38%	43%	53%	34%	49%	53%	45%	27%	54%
威胁情报 39%	42%	40%	37%	46%	36%	16%	36%	48%	47%	44%	42%	39%
补救 36%	34%	32%	38%	34%	31%	47%	37%	41%	40%	21%	41%	41%
无/所有内部 12%	18%	9%	18%	13%	19%	4%	19%	12%	10%	3%	16%	4%

来源：思科 2015 年安全功能基准研究

图 78. 网络的内部托管仍然是最常见的；但自去年开始外部托管也有所增加



来源：思科 2015 年安全功能基准研究

公开安全漏洞

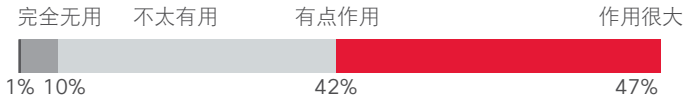
图 79. 在 2015 年，因为安全漏洞而受到公众关注的组织减少

安全入侵事件是推动安全改进的强大动力：

与 **2014 年**相比，在 **2015 年**因为安全入侵事件而受到公众关注的组织减少。

2014 **53%** 对比 2015 **48%**

在您的安全威胁防御策略、程序或技术中，入侵事件能够对改进发挥多大的推动作用？(n=1134)



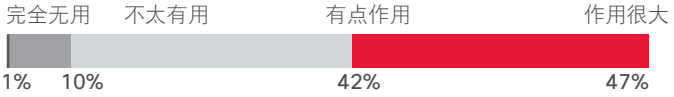
来源：思科 2015 年安全功能基准研究

图 80. 公开漏洞可提高安全性

安全入侵事件是推动安全改进的强大动力：
参与安全调查的受访者。**2014 年** (n=1701) **2015 年** (n=1347)

2014 **53%** 肯定回答 对比 2015 **48%** 肯定回答

在您的安全威胁防御策略、程序或技术中，入侵事件能够对改进发挥多大的推动作用？(n=1134)



在出现安全入侵事件之后，首席安全官比安全运营经理更多地提到改进。

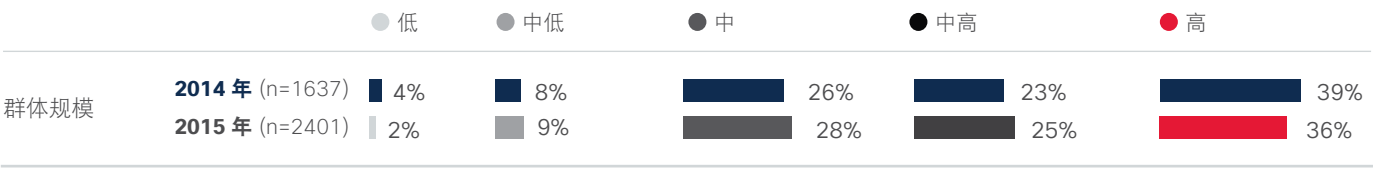
来源：思科 2015 年安全功能基准研究

领先地位与成熟度

图 81. 五类分割法密切跟踪安全功能成熟度模型 (CMM)

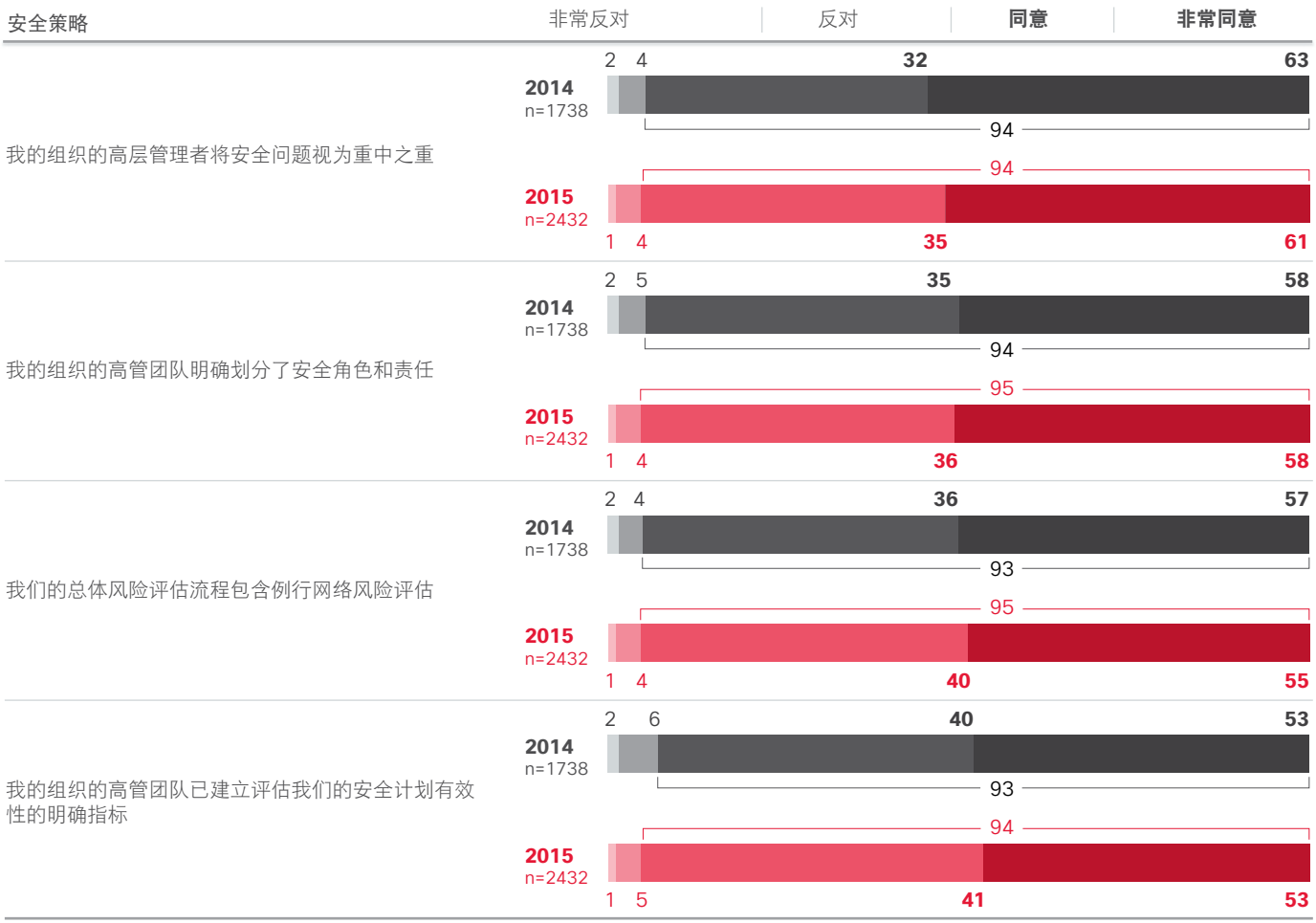
在安全性优先级的成熟度及其如何转化为流程和程序方面，细分市场反映出与去年的研究相似的情况。

60% 或以上的企业达到了更高的安全成熟度要求。这对于大多数国家/地区和行业而言均如此。



来源：思科 2015 年安全功能基准研究

图 82. 在 2014 年，几乎所有受访者都同意或强烈同意高层领导将安全视为头等大事



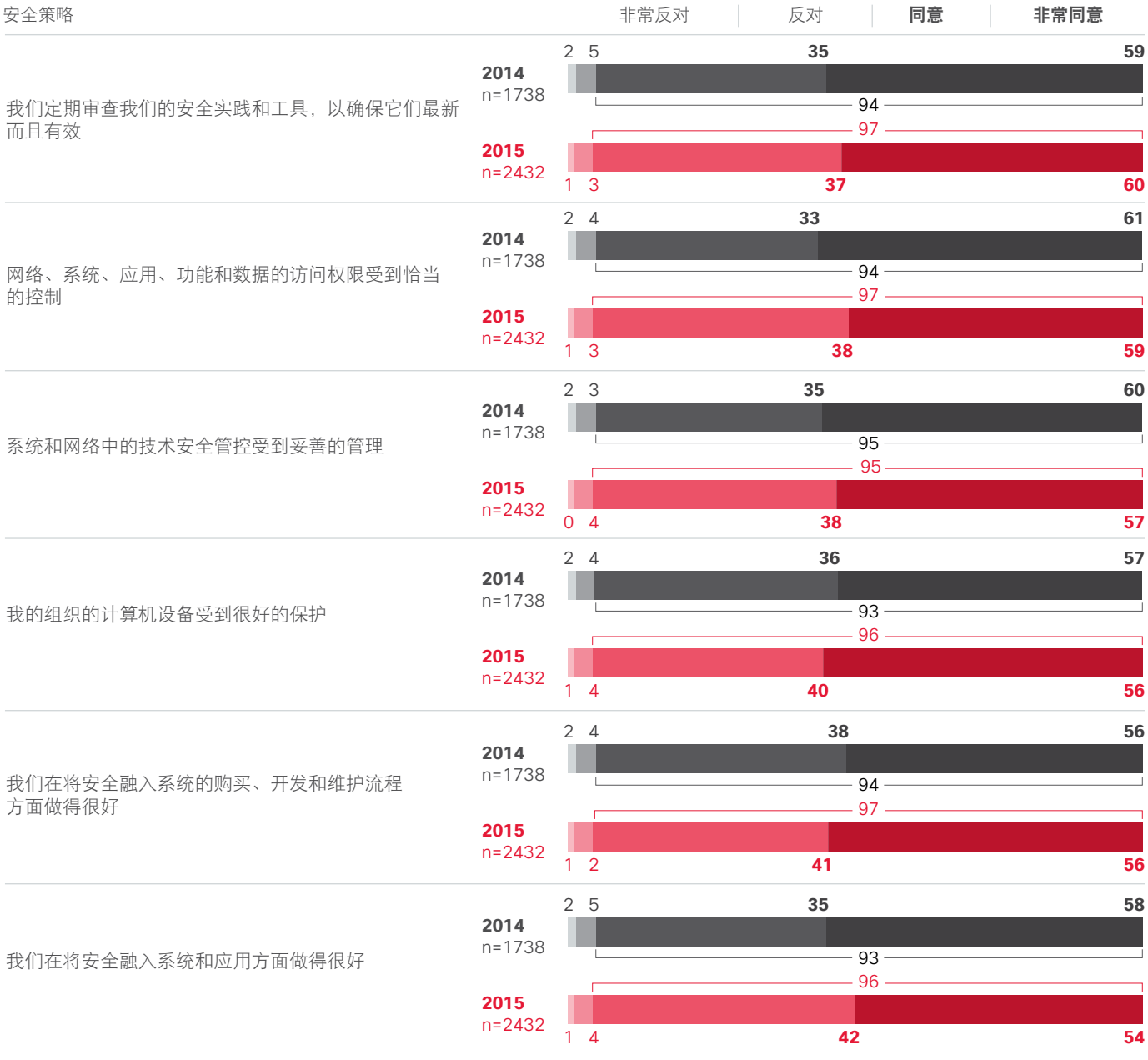
很明显，更多制药行业的受访者比大多数其他行业的专业人员更强烈地同意“我的组织的高管团队已建立评估我们的安全计划有效性的明确指标”的陈述。

很明显，更多的首席安全官比安全运营经理同意关于高管参与度的所有陈述。

来源：思科 2015 年安全功能基准研究

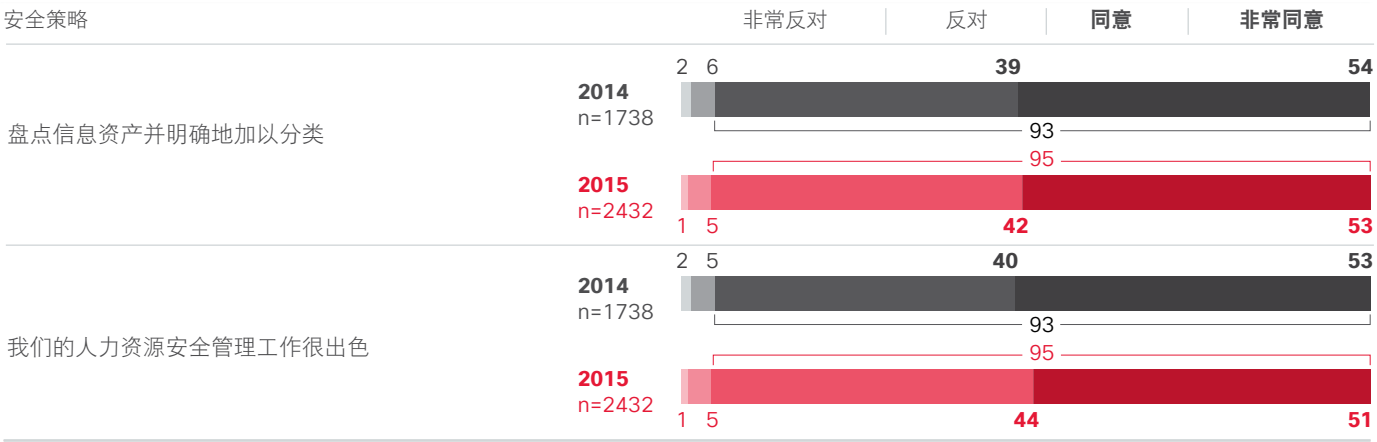
流程

图 83. 对在系统内构建安全性的能力信心不一



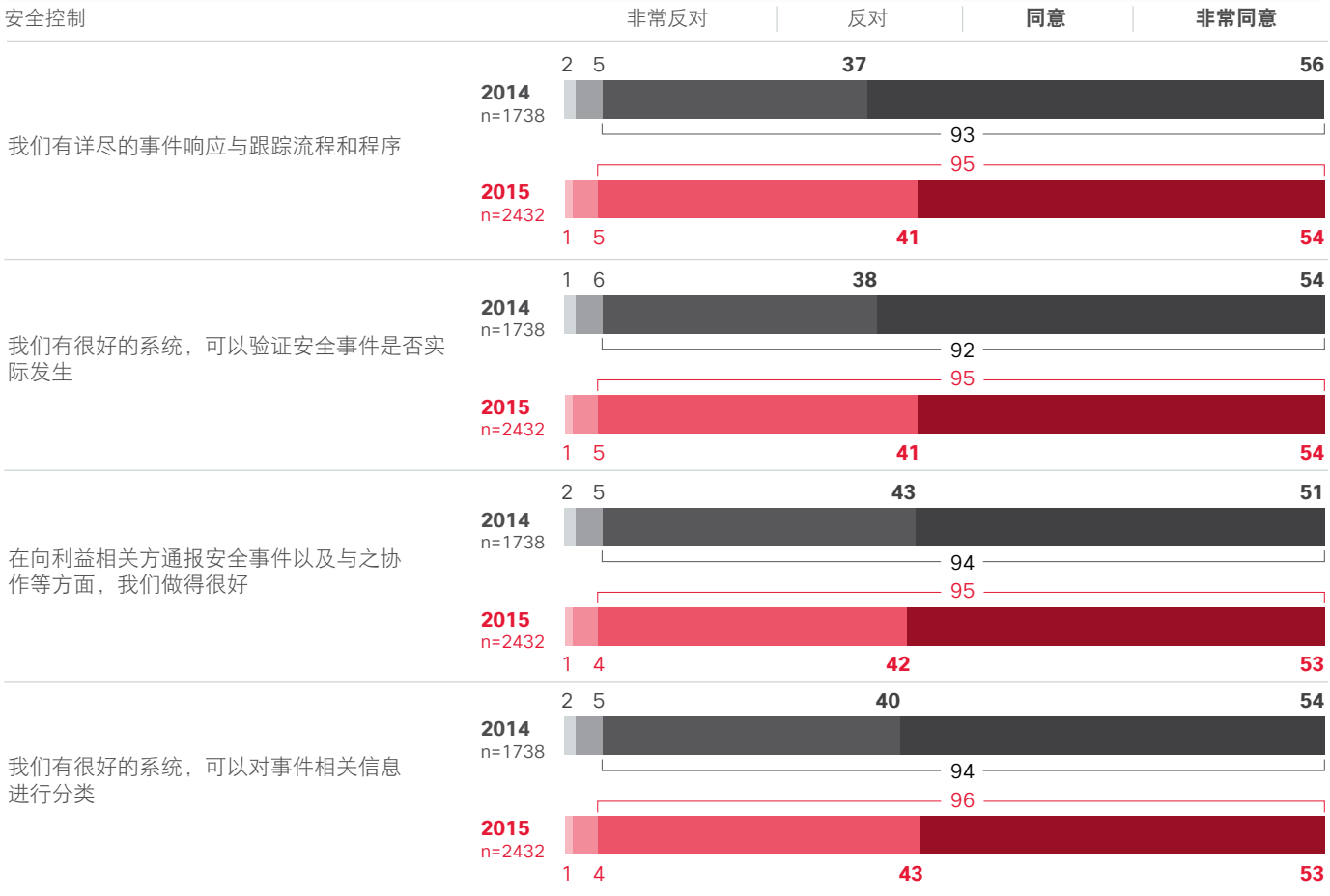
来源：思科 2015 年安全功能基准研究

图 83. 对在系统内构建安全性的能力信心不一（续）



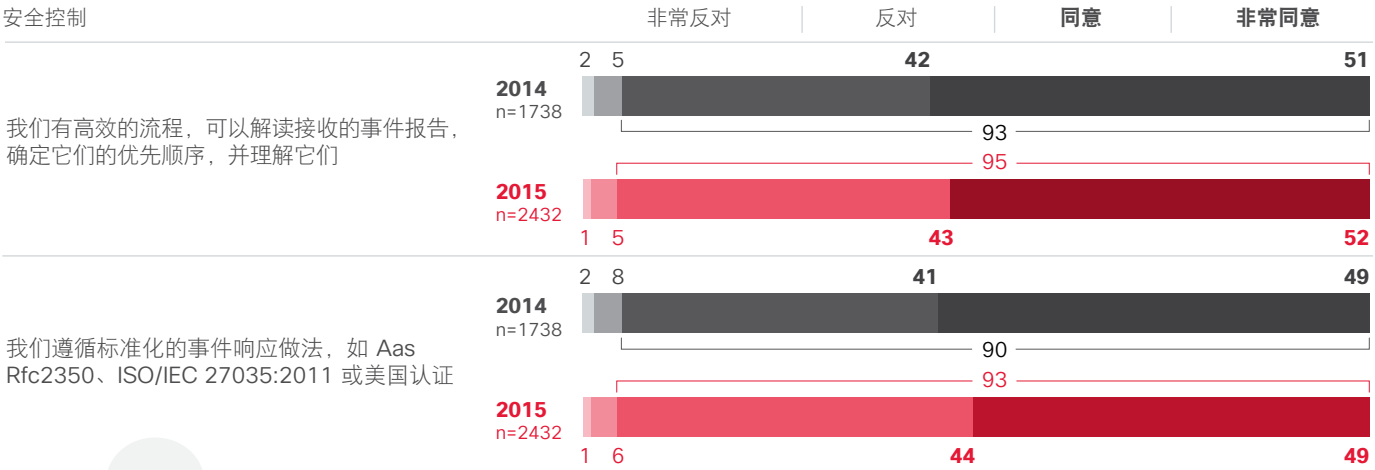
来源：思科 2015 年安全功能基准研究

图 84. 企业认为自己拥有良好的安全控制



来源：思科 2015 年安全功能基准研究

图 84. 企业认为自己拥有良好的安全控制（续）



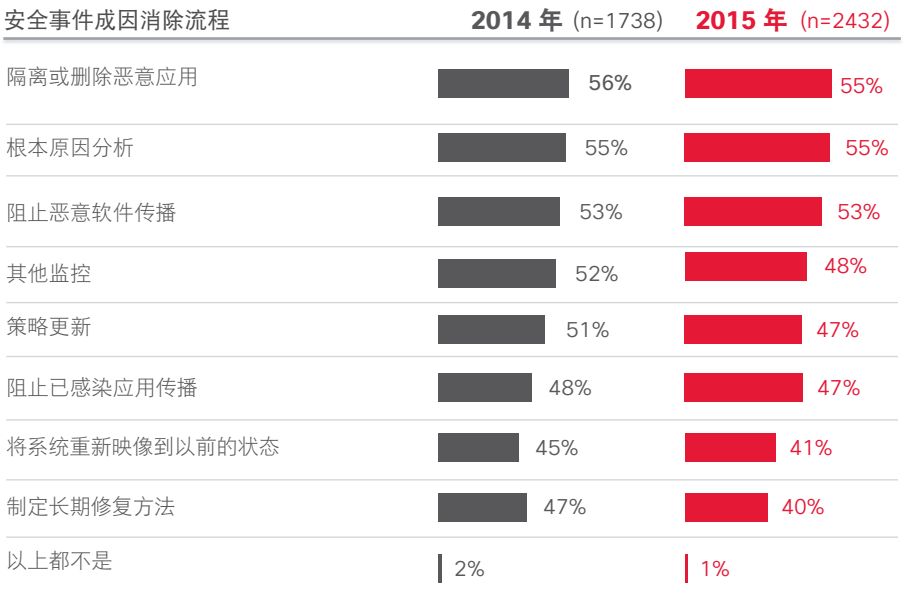
金融服务业的受访者比大多数其他行业的专业人士更可能强烈同意“我们有很好的系统，可以对事件相关信息进行分类”的陈述。

除了“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”的陈述，首席安全官比安全运营经理对围绕安全控制的特点方面更乐观。

来源：思科 2015 年安全功能基准研究

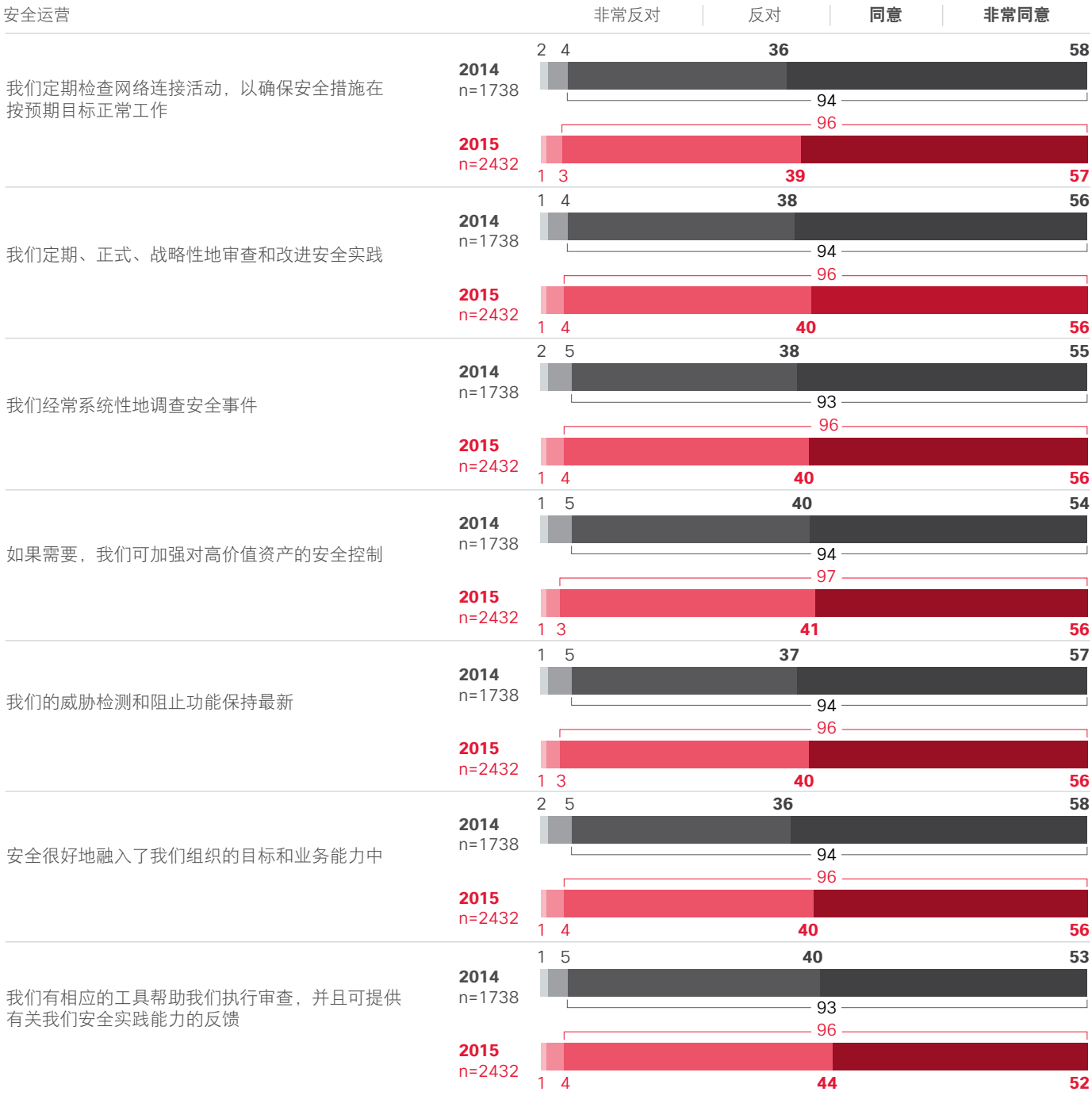
图 85. 隔离/删除恶意应用以及根源分析仍然是最常用的流程

与大多数其他国家/地区的受访者相比，在被问及关于安全事件成因消除流程时，很明显有更多的美国受访者选择“以上都不是”。



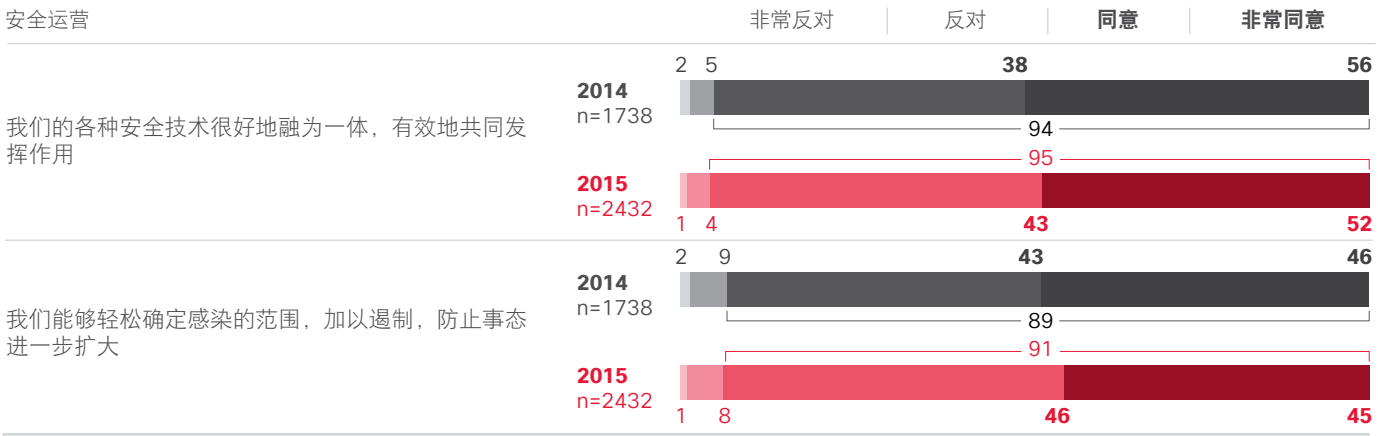
来源：思科 2015 年安全功能基准研究

图 86. 企业对控制威胁的能力信心不一



来源：思科 2015 年安全功能基准研究

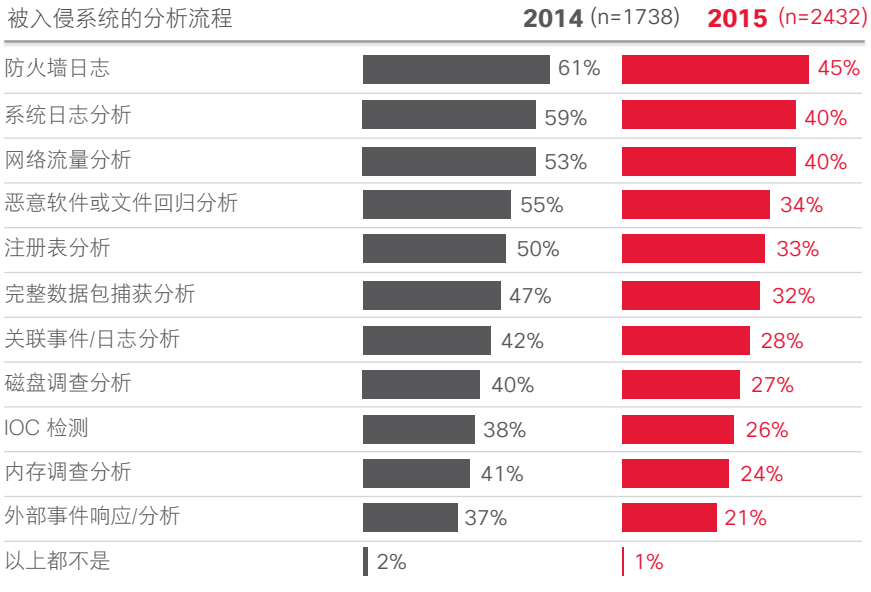
图 86. 企业对控制威胁的能力信心不一（续）



来源：思科 2015 年安全功能基准研究

图 87. 防火墙日志和系统日志分析仍然是分析受威胁系统最常用的流程

与其他发展中公司相比，企业和大型企业公司报告使用更多流程来分析被入侵系统。



来源：思科 2015 年安全功能基准研究

图 88. 在 2015 年，利用事故前备份进行恢复是恢复受影响系统最常用的流程

根据调查，中国的受访者与所调查的其他国家/地区的受访者相比，在“修补和更新被视为有漏洞的应用”方面执行得更频繁。

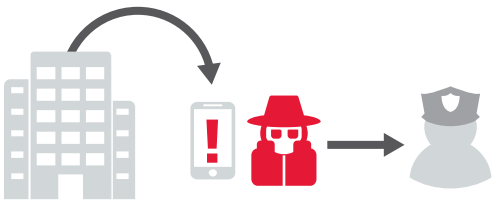
受影响系统的恢复流程	2014 (n=1738)	2015 (n=2432)
用事件前的备份进行恢复	57%	59%
根据事件后查明的漏洞，实施其他或全新检测和控制措施	60%	56%
修补和更新视为有漏洞的应用	60%	55%
差异恢复（删除事件引起的变更）	56%	51%
黄金映像恢复	35%	35%
以上都不是	2%	1%

来源：思科 2015 年安全功能基准研究

图 89. 首席执行官或总裁最可能收到安全事故通知，其次为运营和财务部门

与来自中端市场企业和企业公司的受访者相比，很明显更多的大型企业受访者提及在发生事件时通知外部机构。

大型企业



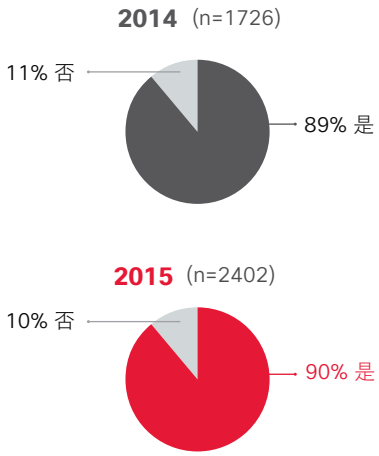
发生事件时通知的群体	2014 (n=1738)	2015 (n=2432)
首席执行官	不适用	45%
Operations	46%	40%
财务部门	不适用	40%
技术合作伙伴	45%	34%
工程	38%	33%
人力资源	36%	32%
法务	36%	28%
制造业	33%	27%
全体员工	35%	26%
公共关系	28%	24%
外部机构	32%	21%
保险公司	22%	18%
发生事件时通知的群体	不适用	15%

来源：思科 2015 年安全功能基准研究

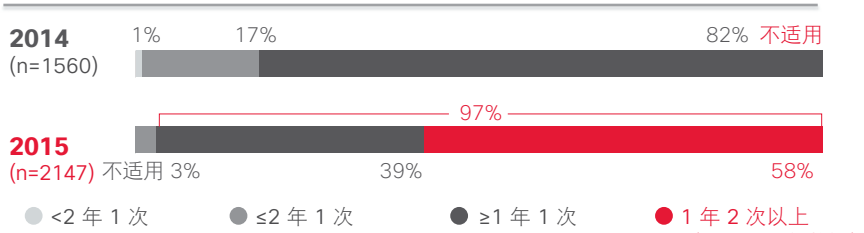
培训

图 90. 几乎所有公司 (97%) 每年都至少进行一次安全培训

是否定期向安全检查站传达安全意识和/或提供培训计划？（专门负责安全的受访者）



多久举办一次安全培训？
（安全团队接受培训的受访者）



与未曾遭受入侵的公司 (83%) 相比，更多遭受过入侵攻击的公司会定期执行安全意识和/或培训计划 (96%)。

肯定回答 96% 对比 否定回答 83%

与中端市场企业 (88%) 和企业公司 (89%) 相比，更多大型企业 (93%) 表示他们会定期执行安全意识和/或培训计划。

大型企业 93% 中端市场 88% 企业 89%

来源：思科 2015 年安全功能基准研究

图 91. 安全意识培训的频率和正式安全策略的影响自 2014 年以来有所上升 – 行动证明

经历过安全入侵事件影响的受访者（提及最多的前 5 项内容）(**2015 年** n=1109)

提高员工的安全意识培训

2015 年，43% 的受访者表示他们在出现公开入侵事件后增强了安全培训。

43%

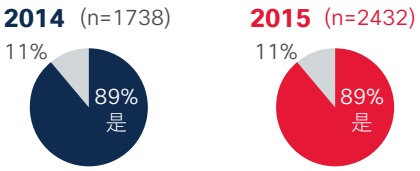
2015 年，41% 的受访者表示他们建立了一套正式的安全策略和程序。

41%

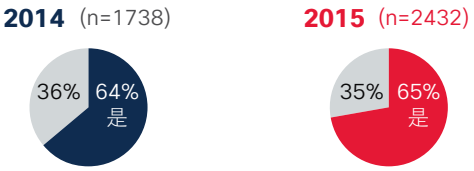
来源：思科 2015 年安全功能基准研究

图 92. 与 2014 年相同，近九成受访者表示他们的安全人员会参加以安全为主题的会议或培训

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）



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）



来源：思科 2015 年安全功能基准研究

安全风险和可信度研究

图 93. 背景和方法

思科希望深入了解企业和运营商 IT 决策者对其组织安全风险和挑战的看法，以及 IT 供应商可信度在其 IT 解决方案购买中所发挥的作用。

具体目标包括：

- 衡量内外部威胁和漏洞构成的风险级别
- 了解当前为缓解安全风险实施的策略、政策和解决方案
- 确定 IT 解决方案采购流程以及 IT 供应商可信度在该流程中所发挥的作用
- 衡量对接收关于如何验证 IT 供应商可信度相关信息的兴趣
- 确定不同行业和受众是否对安全风险观点或缓解风险的方法存在不同理解

方法：定量和定性方法

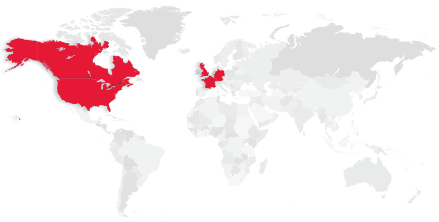
我们利用了两种方法来提供对这各项研究目标的见解：

（参与制定 IT 采购决策的所有受访者）

针对
1050 家企业 ITDM 展开的基于网络的定量调查
（402 家位于美国，282 家位于英国，197 家位于德国，169 家位于法国）

针对
20 家运营商展开定性深入访谈
（7 家位于美国，3 家位于加拿大，3 家位于英国，4 家位于德国，3 家位于法国）

在美国、英国、法国、德国和加拿大执行了研究



从 2015 年 8 月至 9 月收集数据

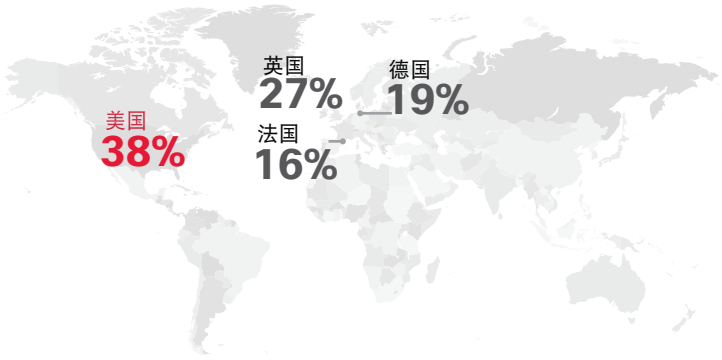
20
基于网络的简短调查

45
简短的深入访谈

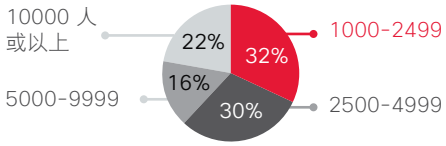
来源：思科安全风险和可信度研究

图 94. 企业受访者构成（定量）

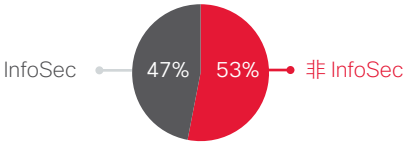
国家/地区



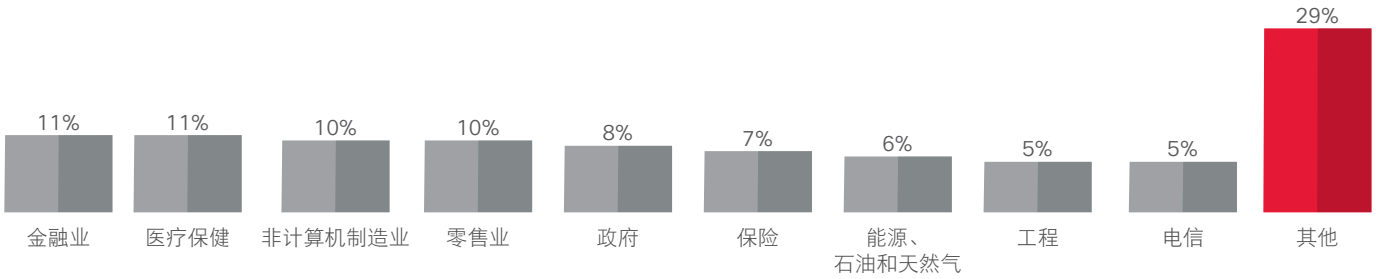
公司规模



InfoSec 分类



行业（报告超过 5% 的行业）



职位

高管（首席信息官、首席安全官、首席技术管等）	25%
副总裁	9%
主管	30%
高级工程师/架构师	6%
工程师	3%
经理	26%
法务	2%

参与购买

设定愿景/战略	69%
确保合规性	71%
审批大型采购	69%
研究/评估解决方案	77%
提供信息或制定最终品牌决策	80%
实施/管理解决方案	77%
授权提供资金/审批预算	53%

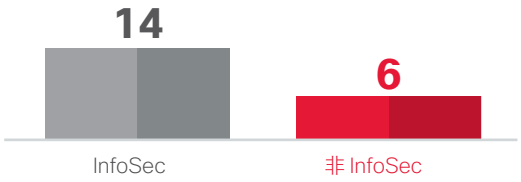
来源：思科安全风险和可信度研究

图 95. 运营商受访者构成（定性）

国家/地区

公司规模

InfoSec 分类



服务提供商类型

应用服务	11%
技术服务	11%
移动电信	6%
媒体服务	4%
有线电信	3%

职位

首席信息官/首席技术官/首席安全官	7%
IT 副总裁	1%
IT 总监	8%
高级经理	1%
高级工程师/架构师	2%
经理	1%

参与购买

设定愿景/战略	80%
确保合规性	100%
审批大型采购	70%
研究/评估解决方案	95%
制定最终品牌决策	85%
实施/管理解决方案	75%
授权提供资金/批准	60%

来源：思科安全风险和可信度研究

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。

2016 年 1 月发布