思科
2017 年年度网络安全报告

cisco

目录

执行摘要

随着受攻击面的扩大，防御者必须把重点放在一个最重要的目标上：减少攻击者的行动空间。

如今，攻击者可以肆意利用的工具多于以往。而且，他们还会狡猾地适时选用各种工具，牟取最大利益。移动终端和在线流量激增，让攻击者如虎添翼。他们不仅有更大的行动空间，所能利用的攻击目标和攻击手段也更加广泛。

面对日益扩大的威胁形势，防御者可采用大量的策略来应对这些挑战。一方面，他们可以购买各种独立工作的同类最佳 (BoB) 解决方案，来获得信息和保护。另一方面，他们可以在人才短缺、预算紧张的市场上争夺人才。

要完全阻止所有攻击是不现实的。但是，您可以通过限制攻击者的行动空间，来抑制其对您资产的危害，从而最大限度降低风险和威胁的影响。作为一种可行的措施，您可以将您的所有安全工具简化为一套互联的集成安全架构。

在自动化的架构中配合使用集成安全工具，可简化检测和缓解威胁的过程。这样，您就可以将时间用于解决更为复杂和顽固的问题。许多组织至少使用六种来自不同供应商的解决方案（第 53 页）。很多时候，他们的安全团队只能调查他们在一天中收到的安全警告中的一半。

思科安全研究部门通过总结研究、洞察和分析成果，发布了《思科 2017 年年度网络安全报告》。这份报告着重介绍了攻击者与防御者之间不断上演且没有休止的拉锯战：攻击者试图获得更多行动时间；防御者则奋力消除攻击者试图利用的机会。报告中还将仔细审视思科威胁研究人员和其他专家整理的数据。我们的研究和见解旨在帮助组织有效应对当今快速变化的复杂威胁。

本报告分为以下部分：

攻击者行为

在此部分中，我们将分析攻击者如何侦测易受攻击的网络以及传输恶意软件，并阐述邮件、第三方云应用和广告软件等工具如何成为攻击者的攻击手段。此外，我们还将说明网络犯罪分子在攻击的安装阶段使用的方法。此部分还将介绍我们的“演进时间”(TTE) 研究，该研究揭露了攻击者如何不断更新策略并成功躲避检测。您可以在此部分了解我们在缩短平均检测时间中值 (TTD) 方面的最新工作进展。此外，我们还将介绍思科面向各种行业和地理区域执行的恶意软件风险最新研究。

防御者行为

此部分介绍漏洞的最新发展趋势，主要探讨的内容之一是中间件库中的新型漏洞。通过这些漏洞，攻击者可以利用相同的工具感染多种应用，从而降低危害用户所需的时间和成本。我们还将分享思科关于补丁趋势的研究。我们还将谈到通过定期向用户提供更新，鼓励他们采用安全性更高的常见 Web 浏览器和生产解决方案版本所带来的优势。

思科 2017 年安全能力基准研究

此部分介绍我们的第三次安全能力基准研究的结果，此项研究旨在了解安全专业人员对其组织内安全状态的看法。今年，安全专业人员似乎对他们手上的工具信心十足，但他们并不确定这些资源能否帮助自己缩小攻击者行动空间。该研究还表明，公共安全漏洞对商机、收入和客户具有十分重要的影响。同时，安全漏洞也在推动组织改进技术和流程。有关组织安全状态相关的更多深入分析，请转至第 49 页。

行业

此部分说明确保价值链安全的重要性。我们将分析政府隐瞒供应商产品中零日攻击和漏洞相关信息的潜在危害。此外，我们还将讨论在高速环境中使用快速加密解决方案保护数据的情况。最后，我们将概述随着全球互联网流量增加以及潜在受攻击面扩大，组织安全将面临的诸多挑战。

结论

在结论中，我们建议防御者调整其安全实践，以便能够更好地应对来自攻击链的典型安全挑战并减少攻击者行动空间。此部分还将具体指导如何建立一种简化的集成安全方法，将高级领导层、策略、协议和工具联系在一起，以预防、检测和缓解各种威胁。

主要研究结果

- 2016 年，漏洞攻击包“三巨头”（Angler、Nuclear 和 Neutrino）突然从威胁领域消失，其他规模较小的漏洞攻击包和新型漏洞攻击包开始活跃起来。
- 根据思科 2017 年安全能力基准研究，大多数公司都在其环境中使用超过五家安全供应商和五种以上的安全产品。安全专业人员中，55% 的人使用至少六家供应商；45% 的人使用一到五个不等的供应商；65% 的人使用六种或更多的产品。
- 根据该基准研究，限制组织采用高级安全产品和解决方案的主要因素包括：预算（占受访者的 35%）、产品兼容性 (28%)、认证 (25%) 和人才 (25%)。
- 思科 2017 年安全能力基准研究发现，由于种种限制，组织仅可调查其在一天当中收到的安全警报中的 56%。在受到调查的警报中，有一半 (28%) 被视为有效警报；而只有不到一半 (46%) 的有效警报得到补救。此外，44% 的安全运营经理每天会收到 5000 多条安全警报。
- 2016 年，员工向企业环境中引入的联网型第三方云应用中有 27% 造成了高安全风险。开放式身份验证 (OAuth) 连接涌入企业基础设施，在被用户授予访问权限后，可以自由地与企业云和软件即服务 (SaaS) 平台通信。
- 在思科对垂直行业的 130 个组织进行的一项调查中，有 75% 的组织受到广告软件感染的影响。攻击者可能会使用这些感染来促进其他恶意软件攻击。
- 恶意广告活动背后的操作者越来越多地使用代理（也称为“攻击入口”）。通过代理，他们可以更快速实施行动，维护其行动空间并避开检测。攻击者可以通过这些中间链路，在不改变初始重定向的情况下，从一台恶意服务器快速切换到另一台恶意服务器。
- 垃圾邮件占邮件总量的近三分之二 (65%)，而且我们的研究表明，由于存在大量发送垃圾邮件的活跃僵尸网络，全球垃圾邮件量日益增长。据思科威胁研究人员称，他们在 2016 年观察到的全球垃圾邮件中，大约有 8% 到 10% 的邮件可归为恶意邮件。此外，带恶意邮件附件的垃圾邮件的百分比正在不断攀升，而攻击者也似乎在尝试各种文件类型，以帮助他们从活动中牟利。
- 根据安全能力基准研究，尚未遭受安全漏洞攻击的组织可能认为其网络是安全的。但调查中有 49% 的安全专业人员称其组织曾因安全漏洞而受到公众关注，因此这种自信可能有点盲目。

- 思科 2017 年安全能力基准研究还发现，遭受攻击的组织中有近四分之一失去了商机。四成受访者表示损失巨大。五分之一的组织由于遭受攻击而失去客户，近 30% 的组织收入受损。
- 根据基准研究的受访者称，出现漏洞时，最有可能受到影响的是运营和财务（分别占 36% 和 30%），其次是品牌声誉和客户保留率（二者均占 26%）。
- 安全漏洞引起的网络中断通常会产生长期的影响。根据该基准研究，45% 的中断持续了 1 至 8小时；15% 持续了 9 至 16 小时，11% 持续了 17 至 24 小时。这些中断中，41%（请参阅第 55 页）影响了 11% 到 30% 的系统。
- 中间件（用作平台或应用间网桥或连接器的软件）中的漏洞愈发明显，让人愈发担心中间件会成为普遍的威胁媒介。许多企业都依靠中间件，因此这种威胁可能会影响每个行业。在某个思科®项目过程中，我们的威胁研究人员发现所分析的大多数新漏洞都可归因于使用中间件。
- 软件更新的速度可能会影响用户安装补丁和升级的行为。据我们的研究人员称，定期和可预测的更新计划会让用户较早升级其软件，从而能减少攻击者可以利用漏洞的时间。
- 2017 年安全能力基准研究发现，大多数组织都依赖第三方供应商来提供至少 20% 的安全资源，而且这些极为依赖此类资源的组织很可能在未来扩大对这些资源的使用。

简介

简介

攻击者拥有广泛多样的技术组合，用以获取组织资源的访问权限以及无限制的行动时间。他们的策略涵盖所有的基本手段，包括：

- 利用补丁和更新中的缺陷
- 引诱用户进入社交工程陷阱
- 将恶意软件注入广告等看似合法的在线内容

他们还具有很多其他能力，从利用中间件漏洞，到投放恶意垃圾邮件，不胜枚举。而且他们在达到目标后，便会迅速且不被察觉地停止活动。

攻击者夜以继日地开发威胁，加快行动速度，以及寻找扩大其行动空间的方法。互联网流量的爆炸性增长（主要是由于移动速度加快和在线设备激增）给攻击者提供了可乘之机，他们可以利用更大的攻击面肆意展开攻击。在此情况下，企业面临的风险也随之增加。思科 2017 年安全能力基准研究发现，曾经受到攻击的组织中，有三分之一以上损失了 20% 或更多的收入。49% 的受访者表示，其组织曾因安全漏洞而受到公众关注。

有多少企业能够承受这样的利润损失并保持活力？防御者必须将其资源集中用于减少攻击者的行动空间。这样，攻击者就会发现，获得企业宝贵资源的访问权限以及在未被检测到的情况下开展活动难如登天。

自动化对于实现此目标至关重要。它可以帮助您了解网络环境中的正常活动，让您将少而宝贵的资源集中用于调查和解决真正的威胁。简化安全操作还有助于您更有效地消除攻击者可以无限制进行活动的空间。但是，该基准研究表明，大多数组织使用的解决方案都在五个以上，而且供应商也在五个以上（第 53 页）。

如此复杂的技术组合以及铺天盖地的安全警报，正说明我们不能再一味增加保护措施，而是需要简化保护。当然，吸收更多安全人才是一个好主意。这是因为，组织拥有越多在职专家，就越能更好地落实技术管理，并实现更好的成果。但是，由于安全人才稀缺和安全预算有限，组织不太可能大量雇佣安全人才。所以，大多数组织必须充分利用其现有人才。他们依靠外包服务为其安全团队加强实力，同时节省预算支出。

正如我们稍后将在本报告中论述的那样，应对这些挑战的有效方法是以集成的方式将人员、流程和技术融入组织的运营。要将安全融入运营，就需要真正了解企业需要保护的内容，以及保护这些重要资产所应采取的措施。

《思科 2017 年年度网络安全报告》展示了我们安全行业取得的最新进展，旨在帮助组织和用户抵御攻击。我们还分析了攻击者突破这些防线所用的技术和战略。本报告还着重讲述了思科 2017 年安全能力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。

受攻击面的扩大

受攻击面的扩大

移动设备、*公共云*、*云基础设施*、*用户行为*。参与思科第三次安全能力基准研究的安全专业人员在考虑其组织遭受网络攻击的风险时，将上述所有因素视为风险的主要来源（图 1）。这不难理解：移动设备的激增使需要保护的终端也随之增加。云正在推动安全边界不断向外延伸。而且，用户是并且永远都是安全链中的薄弱环节。

随着企业实行全数字化，以及万物互联 (IoE)[1] 开始酝酿成形，防御者需要担心的问题也越来越多。受攻击面只会逐渐扩大，给攻击者提供更多行动空间。

十多年来，思科®可视化网络指数 (VNI) 坚持提供全球 IP 流量预测，并对促进网络发展的动态因素做出分析。来看看最近的报告《*皆字节时代 - 趋势和分析*》中的以下统计数据：[2]

- 到 2016 年底，年度全球 IP 流量将突破皆字节 (ZB) 大关，到 2020 年将达到每年 2.3 ZB。（1 皆字节等于 1000 艾字节，或 10 亿太字节。）这意味着未来 5 年全球 IP 流量将增长三倍。
- 到 2020 年，无线和移动设备的流量将占总 IP 流量的三分之二 (66%)。有线设备仅占 34%。
- 从 2015 年到 2020 年，平均宽带速度几乎将翻一番。
- 到 2020 年，全球消费者互联网流量的 82% 将来自 IP 视频流量，较之 2015 年的 70% 有所上升。

图 1 让安全专业人员担心受到网络攻击的最主要的威胁来源

移动设备	公共云中的数据	云基础设施	用户行为（例如，点击邮件或网站中的恶意链接）
58%	57%	57%	57%

安全专业人员中认为这些类别非常或极具挑战性的人数百分比

来源：思科 2017 年安全能力基准研究

在以下网站下载 2017 年图表：**www.cisco.com/go/acr2017graphics**

[1] “万物互联常见问题解答”，思科：http://ioeassessment.cisco.com/learn/ioe-faq。
[2] 皆字节时代 - 趋势和分析，思科 VNI，2016 年：http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html。

此外，思科《*VNI™ 预测和方法（2015-2020 年）*》白皮书[3]预测，2020 年全球互联网流量将达到 2005 年的 95 倍。

当然，伺机行动的网络犯罪分子也密切关注着这些趋势。我们已经看到，影子经济中的运营商正在采取各种措施，使自己能够在当前不断变化的环境中越来越敏捷。他们正在创建目标高度明确、形式更为多样的攻击，从而在整个扩大的受攻击面上取得成功。同时，安全团队一直在忙于解决此起彼伏的安全事件，面对铺天盖地的警报不知所措。他们不得不依赖于在网络环境中部署大量安全产品，而这只能使其工作更为复杂，甚至可能会增加组织遭受威胁的风险。

组织必须：

- 整合安全技术
- 简化安全操作
- 增强自动化

这些措施可以帮助组织降低运营成本，减轻安全人员的负担，并提高安全措施的成效。最重要的是，这将为防御者节省出更多时间，集中精力消除攻击者当前可以利用的不受限制的行动空间。

[3] *思科 VNI 预测和方法，2015-2020 年*，思科 VNI，2016 年：
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html。

攻击者行为

攻击者行为

侦测 | 武器化 | 交付 | 安装

攻击者研究、确定和选择他们的目标。

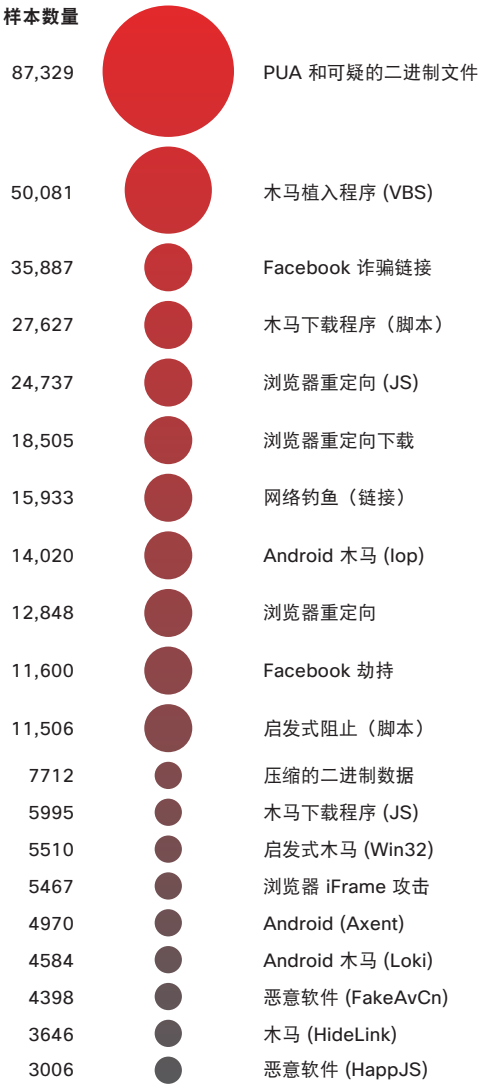
Web 攻击方法：“短尾”威胁帮助攻击者为攻击活动奠定基础

当然，侦测是发起网络攻击的基本步骤。在此阶段，攻击者寻找易受攻击的互联网基础设施或网络漏洞，借以获取访问用户计算机的权限并最终潜入组织。

可疑的 Windows 二进制文件和可能有害的应用 (PUA) 在 2016 年的 Web 攻击方法列表中遥遥领先（请参阅图 2）。可疑的 Windows 二进制文件可传输间谍软件和广告软件等威胁。恶意浏览器扩展程序就是一种 PUA 示例。

Facebook 诈骗（包括虚假产品与服务和媒体内容，以及调查诈骗）在我们的列表中排名第三。在我们观察的最常见恶意软件的年度列表和年中列表中，Facebook 诈骗居高不下，突出说明了社交工程在许多网络攻击中的基本作用。Facebook 每月在全球拥有近 18 亿活动用户，[4]理所当然成为了一个网络犯罪分子和其他攻击者争相欺诈用户的领域。一项积极性进展是，Facebook 公司最近宣布，他们正在采取措施消除假新闻和诈骗。评论家指出，此类内容可能对 2016 年美国总统大选的选民产生了影响。[5]

图 2 观察到最常用的恶意软件



来源：思科安全研究部门

[4] Facebook 统计数据，2016 年 9 月：http://newsroom.fb.com/company-info/。

[5] “扎克伯格宣布要解决 Facebook 的‘虚假新闻’问题，《今日美国》的 Jessica Guynn 和 Kevin McCoy，2016 年 11 月 14 日：http://www.usatoday.com/story/tech/2016/11/13/zuckerberg-vows-weed-out-facebook-fake-news/93770512/。

浏览器重定向恶意软件在 2016 年观察到的最常见恶意软件类型列表中位居第五。正如《*思科 2016 年年中网络安全报告*》[6] 中所述，浏览器感染可能会使用户面临遭受恶意广告攻击的风险，攻击者可以利用恶意广告安装勒索软件和进行其他恶意软件攻击活动。思科威胁研究人员提醒，广告注入器、浏览器设置劫持程序、实用程序和下载程序等恶意广告软件是一个日益严重的问题。事实上，最近我们在研究广告软件问题的过程中调查了一些公司中，结果发现其中 75% 的公司感染了广告软件。（有关该主题的更多信息，请参阅第 23 页“调查发现 75% 的组织受到广告软件感染影响”。）

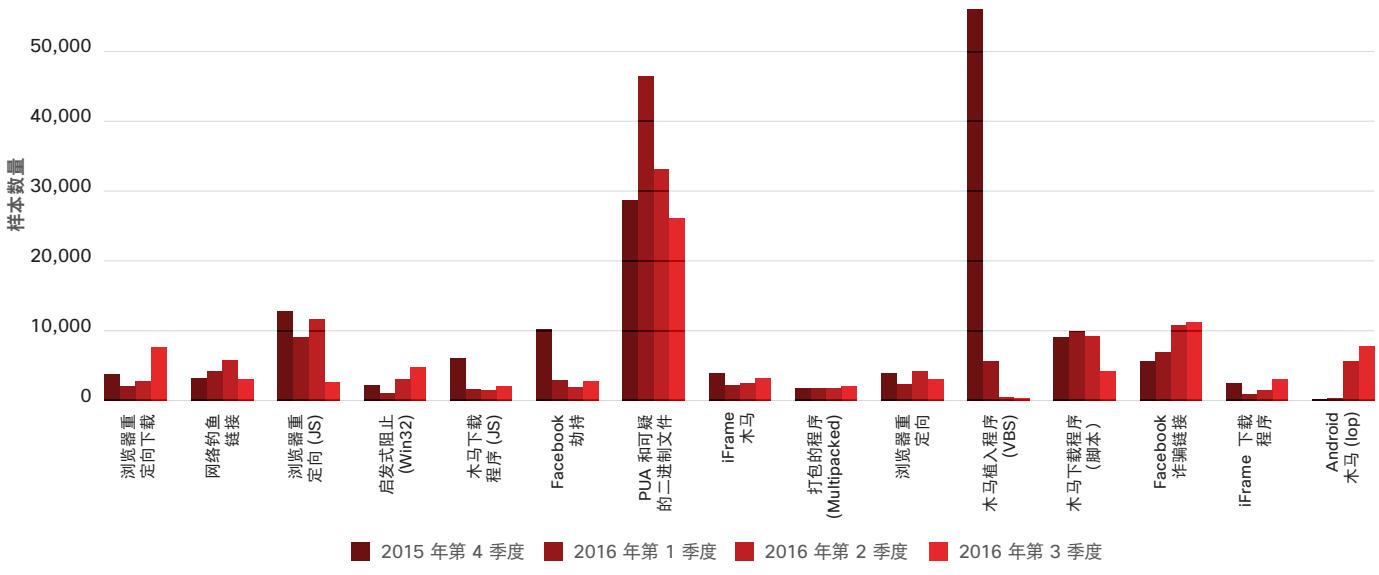
图 3 中列出的其他恶意软件类型（如浏览器 JavaScript 滥用恶意软件和浏览器 iFrame 滥用恶意软件）也旨在感染浏览器。特洛伊木马（植入程序和下载程序）也在观察到的前五种最常见恶意软件类型之列，这表明它们仍然是用于获取用户计算机和组织网络初始访问权限的常用工具。

值得注意的另一趋势是：攻击者持续频繁使用针对 Android 操作平台用户的恶意软件。在过去的 2 年中，Android 木马在短尾威胁列表中一直呈稳步上升状态，在 2016 年观察到的最常见恶意软件中排名第 10。图 2（请参阅上一页）中短尾威胁列表上排名非常靠后的 Loki 恶意软件相当棘手，因为它可以复制和感染其他文件和程序。

图 3 有助于说明思科威胁研究人员自 2015 年年末以来观察到的恶意软件趋势。图中显示攻击者在基于 Web 的攻击的侦测阶段已做出明确转变。现在越来越多的威胁专门寻找易受攻击的浏览器和插件。这种转变反映出攻击者对恶意广告的依赖程度增加，通过传统的 Web 攻击媒介攻击大量用户将会变得更加困难。（请参阅下一部分第 15 页“Flash 面临逐步淘汰，但用户必须保持警惕”。）

对于个人用户、安全专业人员和企业而言，这清楚地表明他们必须确保浏览器安全，并且禁用或删除不必要的浏览器插件，这样可以有效地帮助防止恶意软件感染。这些感染可能导致更多造成重大损失的严重破坏性攻击，例如勒索软件攻击活动。上述简单的措施，即可大大降低您遭遇基于 Web 的常见威胁的风险，并防止攻击者找到执行攻击链的下一个阶段：武器化的行动空间。

图 3 观察到最常用的恶意软件（2015 年第 4 季度 - 2016 年第 3 季度）



来源：思科安全研究部门

[6] *思科 2016 年年中网络安全报告*：http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html。

侦测 | **武器化** | 交付 | 安装

攻击者将远程访问恶意软件与交付内容负载中的漏洞攻击包搭配使用。

Web 攻击媒介：Flash 面临逐步淘汰，但用户必须保持警惕

Adobe Flash 长期以来一直都是一种对试图攻击和危害系统的攻击者极具吸引力的 Web 攻击媒介。然而，随着 Web 上 Adobe Flash 内容量持续下降，以及用户对 Flash 漏洞的认识提高，网络犯罪分子很难再像以前一样大规模攻击用户。

Adobe 公司本身正在逐渐退出对此软件平台的全面开发和支持，并且鼓励开发人员采用 HTML5 等较新的标准。[7] 同时，常用 Web 浏览器的运营商也对 Flash 采取强硬措施。例如，谷歌在 2016 年宣布将在 Chrome 浏览器上逐步停止对 Adobe Flash 的全面支持。[8] Firefox 继续支持旧版 Flash 内容，但它阻止了“对用户体验不太必要的某些 Flash 内容。”[9]

Flash 面临逐步淘汰，但漏洞攻击包开发人员仍在将其继续用作攻击媒介。然而，有迹象表明这种局面可能正在发生变化。自 2016 年三大领先的漏洞攻击包（Angler、Nuclear 和 Neutrino）突然从威胁领域消失后，我们的威胁研究人员发现 Flash 相关互联网流量已有明显下降。（请参阅第 20 页“漏洞攻击包巨头的消失为其他规模较小的漏洞攻击包和新型漏洞攻击包提供了机会”。）Angler 漏洞攻击包背后的攻击者高度有针对性地利用 Flash 漏洞来危害用户。Nuclear 漏洞攻击包也同样注重以 Flash 作为目标。Neutrino 依赖 Flash 文件来传输漏洞攻击包。

用户必须保持谨慎，并应卸载 Flash，除非出于业务原因需要使用 Flash。如果必须使用 Flash，则应及时更新，使之保持最新状态。使用具有自动补丁功能的 Web 浏览器会有帮助。正如第 13 页“Web 攻击方法：‘短尾’威胁帮助攻击者为攻击活动奠定基础”中所述，使用安全的浏览器（禁用或删除不必要的浏览器插件）将帮助您显著降低遭受基于 Web 的威胁的风险。

Java、PDF 和 Silverlight

Java 和 PDF 互联网流量 2016 年均出现显著下降。Silverlight 流量已降至不值得威胁研究人员定期跟踪的级别。

Java 是曾经占主导地位的 Web 攻击媒介，近年来其安全状态已有显著改善。在 2016 年年初，Oracle 决定淘汰 Java 浏览器插件，这有助于降低 Java 成为网络攻击媒介的吸引力。PDF 攻击也日益减少，因此更容易检测出，这就是当前许多攻击者较少采用此策略的原因。

然而，如同 Flash，网络犯罪分子仍在使用 Java、PDF 和 Silverlight 来攻击用户。个人用户、企业和安全专业人员必须了解这些潜在的危害手段。要降低遭遇这些威胁的风险，他们必须：

- 下载补丁
- 使用最新网络技术
- 避免可能存在风险的 Web 内容

[7] “Flash、HTML5 和开放式网络标准”，Adobe 新闻，2015 年 11 月：https://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html。
[8] “Flash 和 Chrome”，Anthony LaForge，The Keyword 博客，Google，2016 年 8 月 9 日：https://blog.google/products/chrome/flash-and-chrome/。
[9] “减少 Adobe Flash 在 Firefox 中的使用”，Benjamin Smedberg，Future Release 博客，Mozilla，2016 年 7 月 20 日：https://blog.mozilla.org/futurereleases/2016/07/20/reducing-adobe-flash-usage-in-firefox/。

应用安全性：在应用呈爆炸性增长的情况下，解决开放式身份验证连接带来的风险

在企业迁移到云的同时，其安全边界也扩展到虚拟领域。但是，随着员工将各种联网型第三方云应用引入企业环境并建立连接，这种安全边界开始迅速消失。

虽然员工的初衷是提高工作效率并在工作时保持连接，但是这些影子 IT 应用却会给企业带来风险。它们可以接触到企业基础架构，并在用户通过开放式身份验证 (OAuth) 授予访问权限后自由地与企业云和软件即服务 (SaaS) 平台进行通信。这些应用可以获得广泛的（有时甚至是过度的）权限范围，其中包括查看、删除、向外传输和存储企业数据，甚至代表用户执行操作。因此，这些应用必须得到妥善的管理。

云安全提供商 CloudLock（现为思科旗下公司）抽选了 900 个来自各行各业、具有代表性的组织，并持续跟踪其联网型第三方云应用的增长情况。如图 4 所示，在 2016 年年初已发现约 129,000 种不同应用。到十月底，这一数字已增长到 222,000 个。

应用的数量自 2014 年以来已增长约 11 倍。（请参阅图 5。）

最危险应用的分类

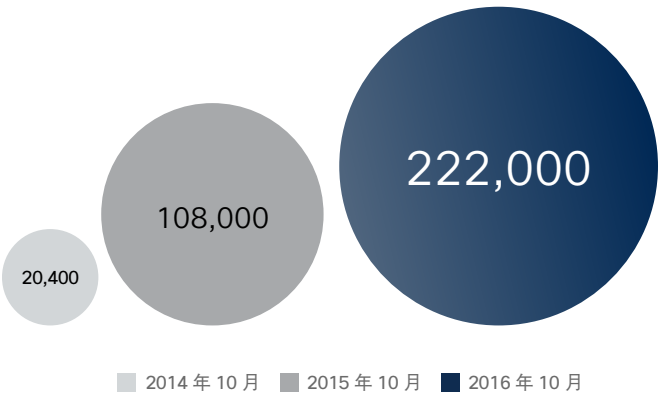
为了帮助安全团队了解其环境中哪些联网型第三方云应用对网络安全性构成的风险最大，CloudLock 制定了云应用风险指数 (CARI) 评估过程。此过程包括多项评估：

- **数据访问要求：**组织回答以下问题，例如：授权应用需要什么权限？授予数据访问权限是否意味着，应用可通过开放式身份验证连接取得企业 SaaS 平台的编程 (API) 访问权限？应用（以及相应的供应商）能否代表用户并对企业数据执行操作，例如查看和删除数据？
- **社区信任评级：**社区信任评级：此评估根据同行驱动的评估和大众评估进行。
- **应用威胁情报：**由网络安全专家根据应用的各种安全属性（如安全认证、漏洞历史记录和分析师评论）进行的一项全面背景检查。

图 4 2016 年联网型第三方云应用呈现爆炸性增长

来源：思科 CloudLock

图 5 第三方云应用与上一年同期相比实现的增长



来源：思科 CloudLock

在以下网站下载 2017 年图表：**www.cisco.com/go/acr2017graphics**

风险评分和示例

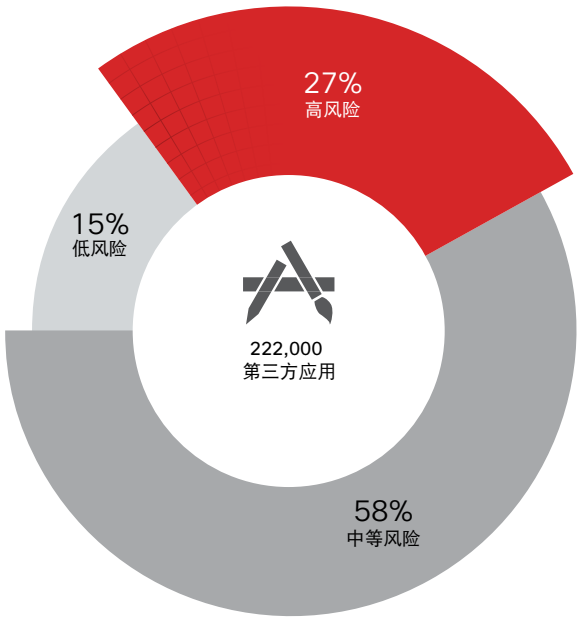
在使用 CARI 对第三方云应用进行分类之后，CloudLock 为每个应用指定风险评分，分值为 1（风险最低）至 5（风险最高）。

例如，在最小访问范围（只可以查看邮件）、100% 社区信任评级和无漏洞历史记录情况下，应用将获得分数为 1 的评分。

具有完全帐户访问权（可查看所有邮件、文档、导航历史记录、日历等）、8% 的信任评级（即表示仅 8% 的管理员信任它）以及无安全认证的情况下，应用将获得分数为 5 的评分。

CloudLock 使用 CARI 对其在抽选的 900 个组织中发现的 222,000 个应用进行分类。在所有这些应用中，有 27% 被认为是高风险，而大多数归为中等风险。（请参阅图 6。）其中一半的组织存在与 2016 年夏季发布的热门游戏应用相关的 OAuth 连接。

图 6 分类为高风险的第三方应用

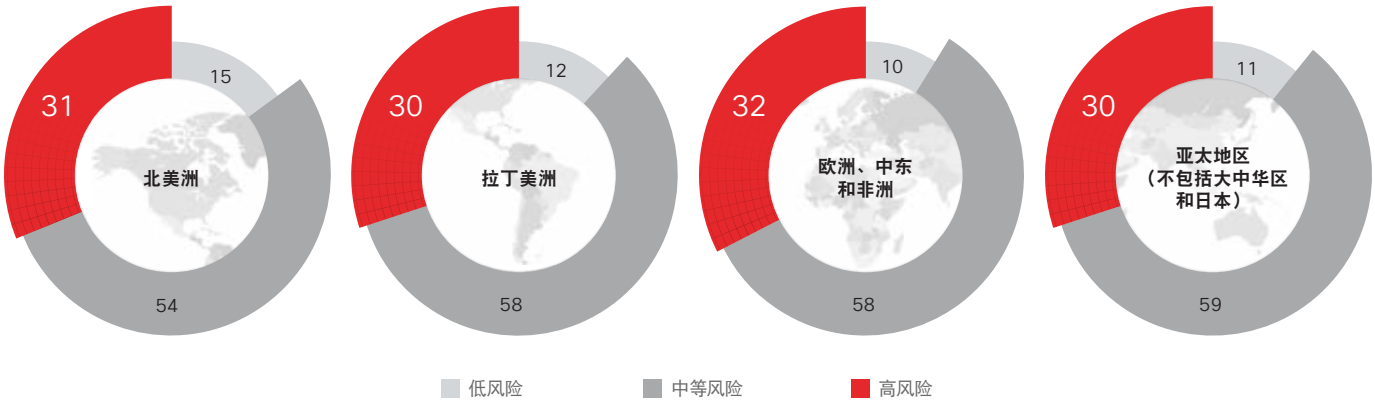


来源：思科 CloudLock

分享

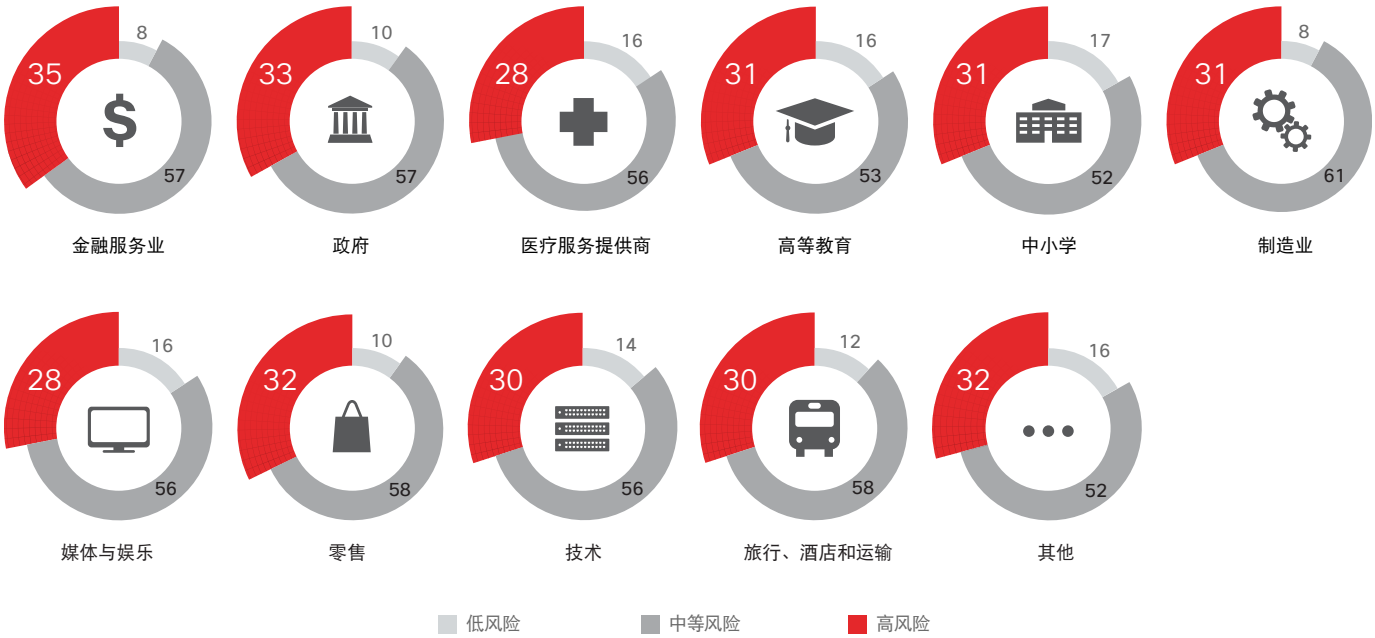
通过我们的分析，我们发现所有组织（无论其规模、行业或地区如何）的低、中、高风险应用分布都相对均匀（图 7 和 8）。

图 7 低、中和高风险应用的分布（按地区）



来源：思科 CloudLock

图 8 低、中和高风险应用的分布（按行业）



来源：思科 CloudLock

在以下网站下载 2017 年图表：**www.cisco.com/go/acr2017graphics**

排除干扰

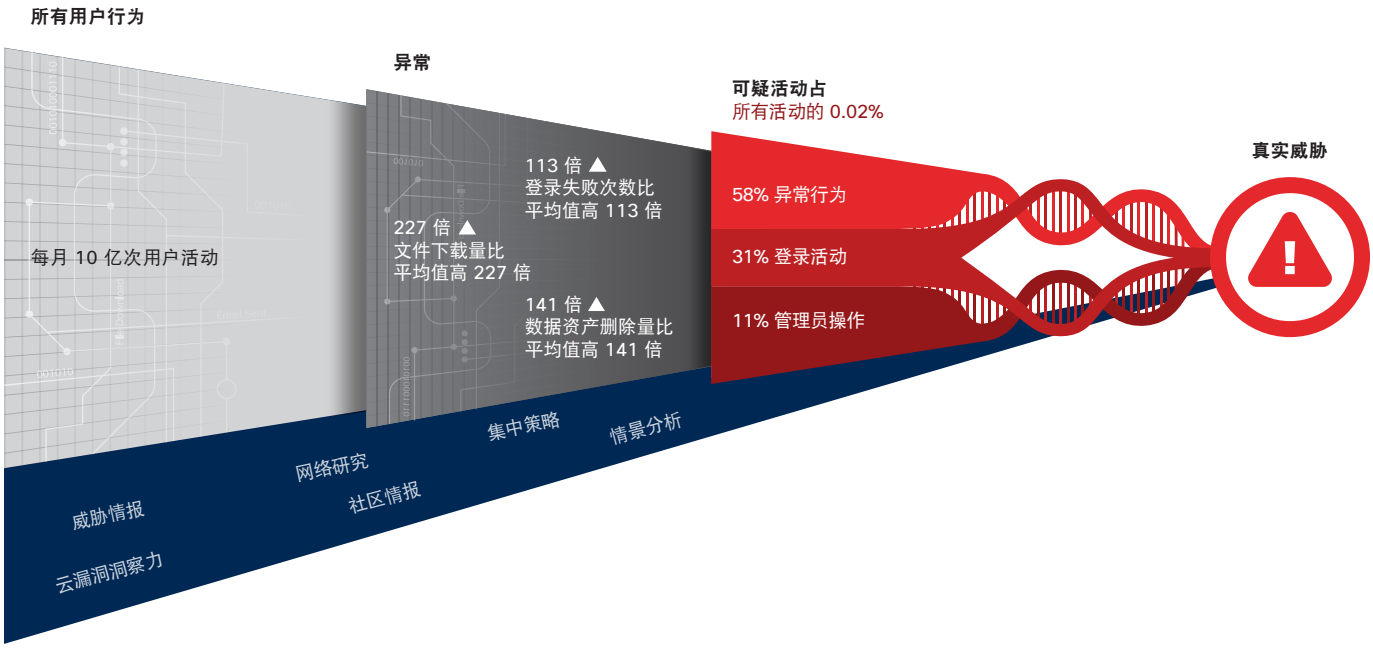
为了识别包括第三方云应用在内的企业 SaaS 平台中的可疑用户和实体行为，安全团队必须对数十亿用户活动进行筛选，确定其组织环境中用户行为的正常模式。他们必须找出这些预期模式之外的异常情况，然后关联各个可疑活动，以确定可能需要调查的真正威胁。

例如，短期内几个国家/地区出现异常频繁的登录活动，这就很可疑。假设某个组织的正常用户行为是，员工每周从一两个国家/地区登录特定应用。如果某个用户在一周内开始从 68 个国家/地区登录该应用，安全团队就需调查该活动是否合法。

根据我们的分析，在联网型第三方云应用相关的 5000 个用户活动中，仅有 1 个活动（占 0.02%）是可疑的。当然，安全团队面临的挑战是查明这一个可疑活动。

只有通过自动化，安全团队才能排除安全警报中的“干扰”，将资源集中在调查真正的威胁上。上述识别正常和潜在可疑用户活动的多阶段过程（如图 9 所示），便可以依赖自动化（每个阶段采用相应的算法）。

图 9 利用自动化（流程）识别用户行为模式



来源：思科 CloudLock

侦测 | 武器化 | **交付** | 安装

攻击者通过恶意使用邮件、文件附件、网站和其他工具，将其网络武器传送到目标。

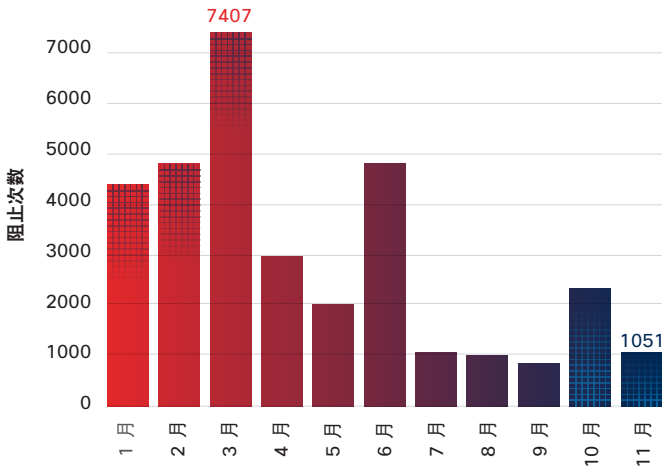
主要漏洞攻击包的消失为小型攻击者和新入行者提供了机会

2016 年，漏洞攻击包环境经历了巨大的变化。年初，Angler、Nuclear、Neutrino 和 RIG 显然还占据漏洞攻击包领导地位。到 11 月，其中就只剩 RIG 唯一一个仍然保持活跃。如图 10 所示，漏洞攻击包活动在 6 月前后明显下降。

首先消失的是 Nuclear，它在 5 月突然停止运营。其制作者为何要放弃它依然是一个迷。依赖 Flash 文件实现攻击的 Neutrino 漏洞攻击包在 2016 年也退出了历史舞台。（有关 2016 年已知漏洞攻击包中的主要漏洞列表，请参阅下一页中的图 11。）

Flash 仍然是攻击者眼中有吸引力的 Web 攻击媒介，但随着时间的推移，这种吸引力可能会渐渐消退。较少的网站和浏览器完全支持 Flash，有的甚至完全不支持，而且人们普遍提高了对于 Flash 漏洞的认识。（有关该主题的更多信息，请参阅第 15 页“Web 攻击媒介：Flash 面临逐步淘汰，但用户必须保持警惕”。）

图 10 漏洞攻击包登录页面阻止情况（2016 年 1 月 - 11 月）



来源：思科安全研究部门

在以下网站下载 2017 年图表：**www.cisco.com/go/acr2017graphics**

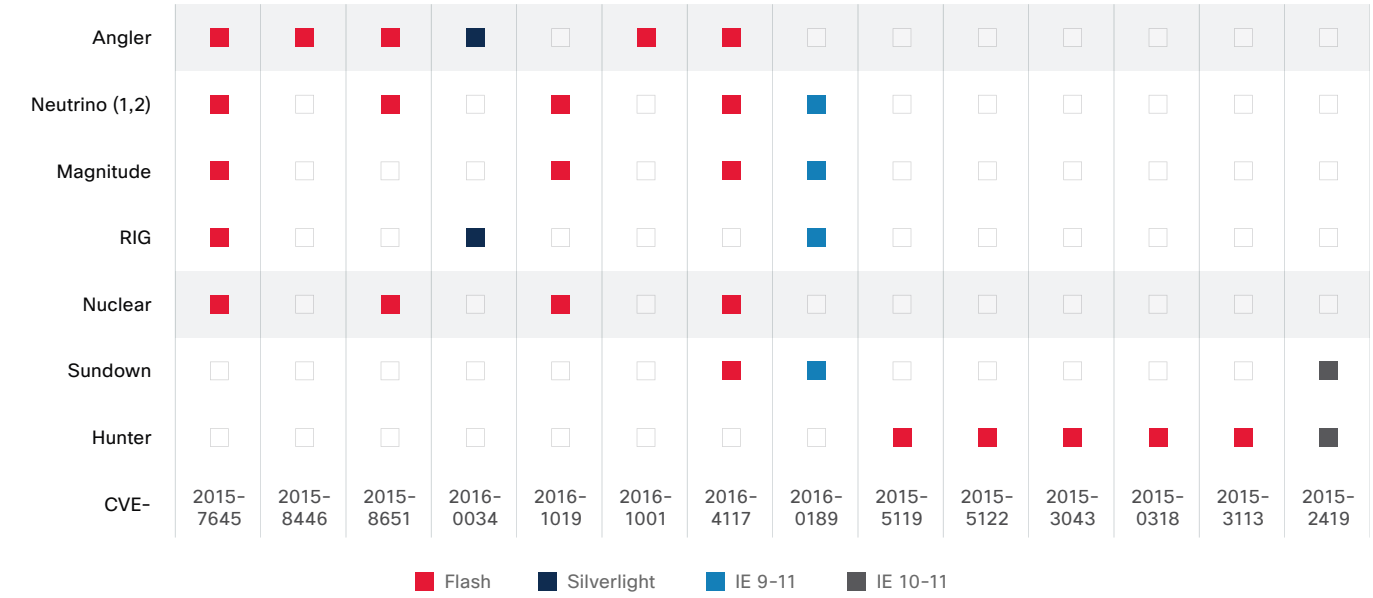
巨头时代的终结

Angler 是已知漏洞攻击包中使用量最大而且最高级的漏洞攻击包，它以 Flash 漏洞为目标，与许多臭名昭著的恶意广告和勒索软件攻击活动有关。不过，与神秘消失的 Nuclear 和 Neutrino 不同，Angler 在 2016 年的退出并不难理解。

当年春末，约 50 名黑客和网络犯罪分子在俄罗斯被捕；该团伙涉嫌利用 Lurk 恶意软件专门针对俄罗斯银行发动银行木马攻击。[10] 思科威胁研究人员发现了 Lurk 和 Angler 二者之间的直接关系，包括主要通过 Angler 向俄罗斯境内受害者传送 Lurk 病毒的确凿证据。该犯罪团伙被捕后，Angler 的时代也随之终结。[11]

现在，漏洞攻击工具的“三巨头”均已退出市场，规模较小的漏洞攻击包和新型漏洞攻击包开始争抢更多市场份额。而且，它们正在变得更加复杂和敏捷。在 2016 年年末，Sundown、Sweet Orange 和 Magnitude 漏洞攻击包呈现稳定增长的态势。已知的是，连同 RIG 在内，这些漏洞攻击包均以 Flash、Silverlight 和 Microsoft Internet Explorer 漏洞为目标。（请参阅图 11。）卸载 Flash 并禁用或删除不必要的浏览器插件将有助于降低用户受到这些威胁危害的风险。

图 11 排名靠前的漏洞攻击包漏洞



来源：思科安全研究部门

分享

[10] “俄罗斯黑客团伙因盗窃 2500 万美元而被捕”，BBC 新闻，2016 年 6 月 2 日：http://www.bbc.com/news/technology-36434104。
[11] 有关此主题的更多信息，请参阅 2016 年 7 月的思科 Talos 博文，通过联系分散的线索揭示犯罪软件格局剧变。

恶意广告：攻击者使用代理来提高速度和敏捷性

用户被定向至漏洞攻击包有两种主要方式：受感染网站和恶意广告。攻击者会将一个指向漏洞攻击包登录页面的链接置入恶意广告或已感染的网站中，或者使用被称为代理的中间链接。（这些链接位于受感染网站和漏洞攻击包服务器之间，也称为“攻击入口”。）代理充当初始重定向和将恶意软件负载传送给用户的实际漏洞攻击包之间的中间人。

随着攻击者发现他们必须加快行动以维护其活动空间和逃避检测，这种战术变得越来越受欢迎。攻击者可通过代理从一个恶意服务器快速切换到另一个服务器，而无需更改初始重定向。由于他们不需要不断修改网站或恶意广告来启动感染链，漏洞攻击包操作者可以执行更长时间的攻击活动。

ShadowGate：一种具成本效益的攻击活动

随着单独通过传统网络攻击媒介来感染大量用户变得更加困难（参见第 15 页），攻击者越来越多地依赖恶意广告来让用户接触漏洞攻击包。我们的威胁研究人员将最近的一种全球恶意广告活动命名为“ShadowGate”。该活动说明了恶意广告如何为攻击者提供更大的灵活性和机会，向大规模地理区域的用户发起攻击。

ShadowGate 涉及流行文化、零售、色情和新闻等不同类别的网站。它可能影响了北美、欧洲、亚太地区和中东的数百万用户。值得注意的是，该活动实现了全球覆盖并使用许多种语言。

ShadowGate 第一次使用域名阴影是在 2015 年年初。它会不定期停止活动一段时间，然后再次开始活动，并继续将流量定向至漏洞攻击包登录页面。最初，ShadowGate 仅用于将用户定向到 Angler 漏洞攻击包。但在 Angler 于 2016 年夏天消失后，用户被定向到 Neutrino 漏洞攻击包，直至 Neutrino 也在几个月后消失。（有关此报道的更多信息，请参阅第 20 页上的“漏洞攻击包巨头的消失为其他规模较小的漏洞攻击包和新型漏洞攻击包提供了机会”。）

虽然 ShadowGate 观察到了大量 Web 流量，但只有极少部分交互会使用户被定向到漏洞攻击包。恶意广告主要采取展示形式，也就是它们只呈现在页面上，而无需用户交互。此在线广告模式让参与 ShadowGate 活动的攻击者可更有效地开展其活动。

我们对 ShadowGate 的研究促使我们与一家大型 Web 托管公司携手合作。我们通过收回用于托管此活动的注册人帐户，缓解了此威胁。然后我们取消了所有相关子域。

有关 ShadowGate 活动的更多详细信息，请参阅 2016 年 9 月的思科 Talos 博文，Talos 挫败 ShadowGate：重创全球恶意广告活动。

调查发现 75% 的组织受到广告软件感染影响

合法用途的广告软件通过重定向、弹出窗口和广告注入来下载或显示广告，并为其制作者创收。但是，网络犯罪分子也将广告软件用作提高收入来源的工具。他们不仅使用恶意广告软件从注入广告获利，而且将其作为促进其他恶意软件（如 DNSChanger 恶意软件）攻击活动的跳板。恶意广告软件通过软件捆绑包传输；发布者创建一个带一个合法应用以及数十个恶意广告软件应用的安装程序。

恶意攻击者使用广告软件执行以下操作：

- 注入广告，这可能导致进一步感染或遭受漏洞攻击包攻击
- 更改浏览器和操作系统的设置以消弱安全性
- 破坏防病毒产品或其他安全产品
- 获取对主机的完全控制权，以便能够安装其他恶意软件
- 根据位置、身份、所用的服务以及经常访问的站点跟踪用户
- 窃取个人数据、凭证和基础设施信息等信息（例如，公司的内部销售页面）

为了评估企业的广告软件问题范围，思科威胁研究人员分析了 80 种不同的广告软件变体。我们在 2015 年 11 月至 2016 年 11 月期间执行的调查中，对整个垂直行业大约 130 个组织进行了调查。

我们根据各组件的主要行为将广告软件分为四组：

- **广告注入器：**此广告软件通常驻留在浏览器中，并可能影响所有操作系统。
- **浏览器设置劫持程序：**此广告软件组件可以更改计算机设置，使浏览器更不安全。
- **实用程序：**这是一种大型且不断增长的广告软件类别。实用程序是为用户提供有用服务（如 PC 优化）的 Web 应用。这些应用可以注入广告，但其主要目的是说服用户购买服务。然而，在很多时候，所谓的服务只不过是一场骗局，并不会为客户提供任何好处。
- **下载程序：**此广告软件可传输其他软件，例如工具栏。

我们得出的结论是，在我们的研究中有 75% 的组织受到广告软件感染影响。

图 12 受到广告软件感染的组织所占百分比

来源：思科安全研究部门

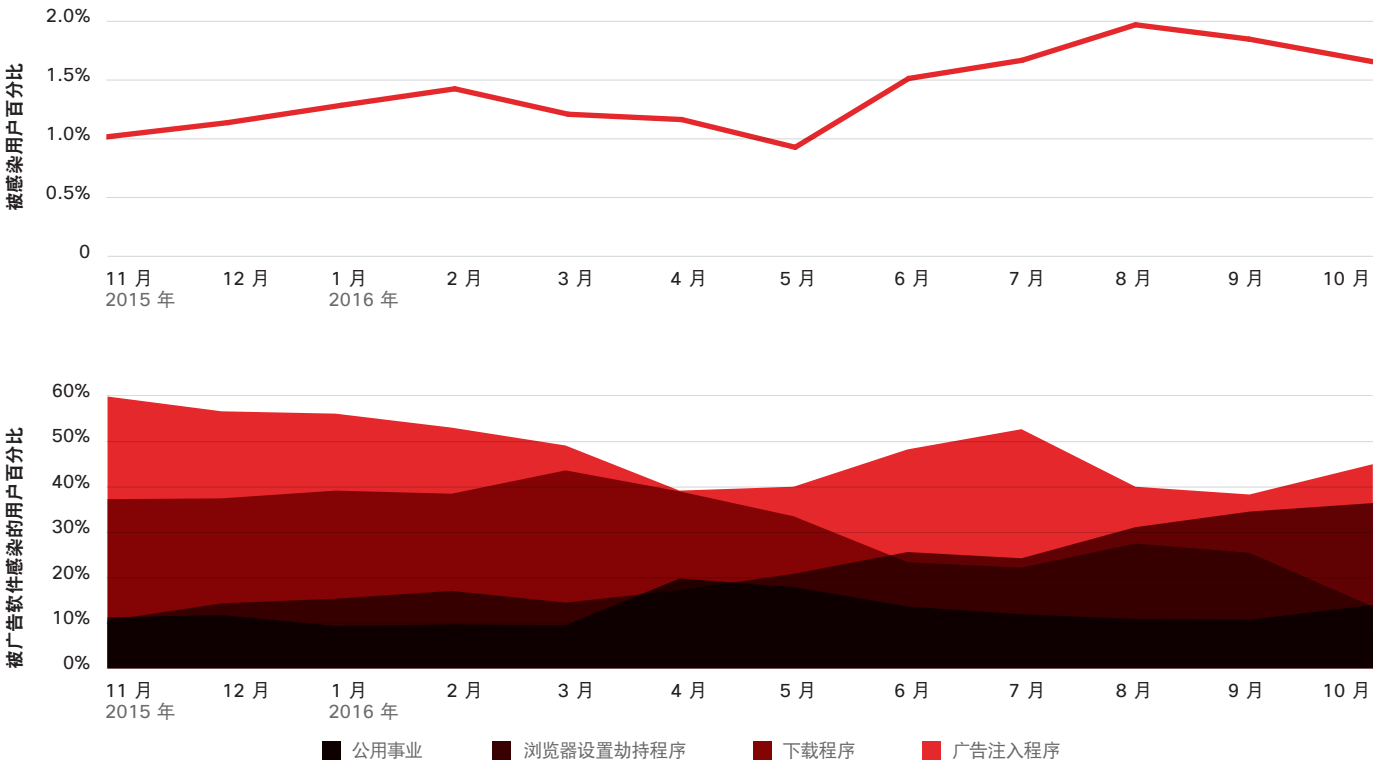
分享

图 13 显示在我们调查的组织中观察到的事件类型。广告注入器是主要的感染来源。此结果表明，大多数有害应用都以 Web 浏览器为目标。近年来，我们还发现基于浏览器的感染呈上升趋势，这表明攻击者一直在尝试使用此策略攻击用户以牟取利益。

我们在调查中确定的所有广告软件组件均可能使用户和组织面临恶意活动的风险。安全团队必须认识到广告软件感染带来的威胁，并确保组织中的用户完全了解风险。

有关此主题的更多信息，请参阅 2016 年 2 月思科安全博文：《与所安装广告软件相关的 DNSChanger 爆发》。

图 13 广告软件组件引起的总事件明细



来源：思科安全研究部门

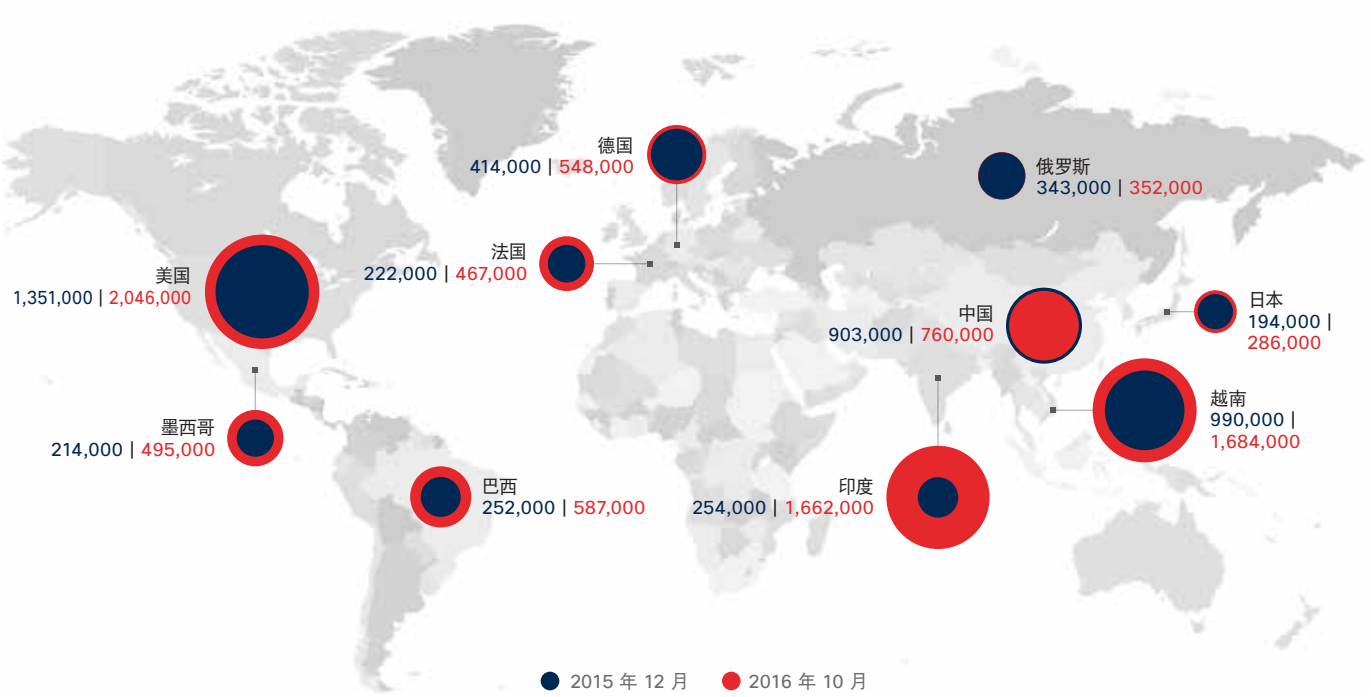
在以下网站下载 2017 年图表：**www.cisco.com/go/acr2017graphics**

全球垃圾邮件日益剧增，恶意附件的比例也越来越高

2016 年，思科威胁研究人员使用选择性客户遥感勘测进行了两项研究，以评估总邮件数量中垃圾邮件的百分比。我们发现垃圾邮件占邮件总量的近三分之二 (65%)。我们的研究还表明，由于 Necurs 等大量垃圾邮件发送僵尸网络活动猖獗，全球垃圾邮件数量仍在增长。此外，通过我们的分析可确定，在 2016 年观察到的全球垃圾邮件中，约有 8% 到 10% 的邮件可以归为恶意邮件。

从 2016 年 8 月到 10 月期间，IP 连接阻止数量显著增加（图 14）。[12] 之所以出现这种趋势，是因为垃圾邮件数量整体上升，而且信誉系统也更多地结合了关于垃圾邮件发送者的信息。

图 14 按国家/地区划分的 IP 阻止，2015 年 12 月 – 2016 年 11 月



来源：思科安全研究部门

分享

[12] IP 连接阻止是垃圾邮件因发件人信誉分值较低而被垃圾邮件检测技术即刻阻止。示例包括来自已知垃圾邮件发送僵尸网络或已知参与了垃圾邮件攻击的受感染网络的邮件。

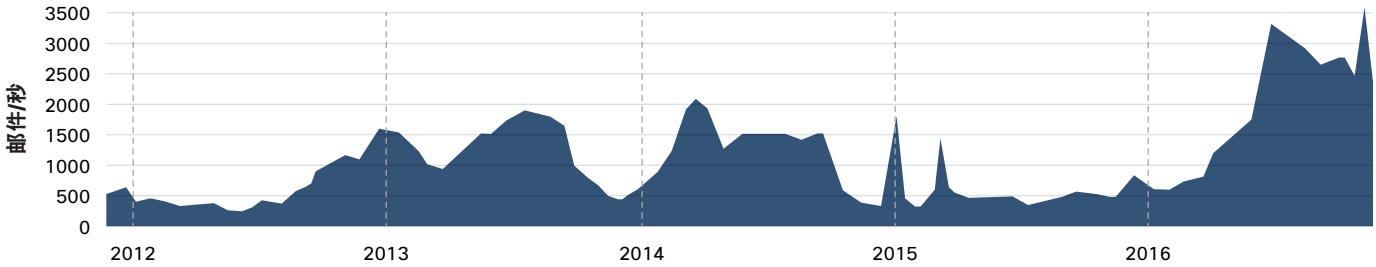
IP 位置封锁名单（Composite Blocking List，简称 CBL，此名单基于 DNS，是一种关于可疑垃圾邮件发送计算机感染的黑洞名单）的五年图表，[13] 也表明在 2016 垃圾邮件总量显著增加（图 15）。

根据 CBL 的 10 年数据分析（未列出），2016 年垃圾邮件数量接近 2010 年的历史最高水平。近年来，得益于新的反垃圾邮件技术以及对垃圾邮件相关僵尸网络的严厉打击，垃圾邮件数量有所下降。我们的威胁研究人员认为，近期全球垃圾邮件数量的增长是 Necurs 僵尸网络导致的。Necurs 是 Locky 勒索软件的主要媒介。它还可以传播 Dridex 银行木马等威胁。

图 16 是思科 SpamCop 服务团队制作的内部图，说明在 2016 年观察到的垃圾邮件量的变化。此图显示 SpamCop 阻止列表 (SCBL) 从 2015 年 11 月到 2016 年 11 月的整体大小。SCBL 中的每一行代表一个不同的 IP 地址。

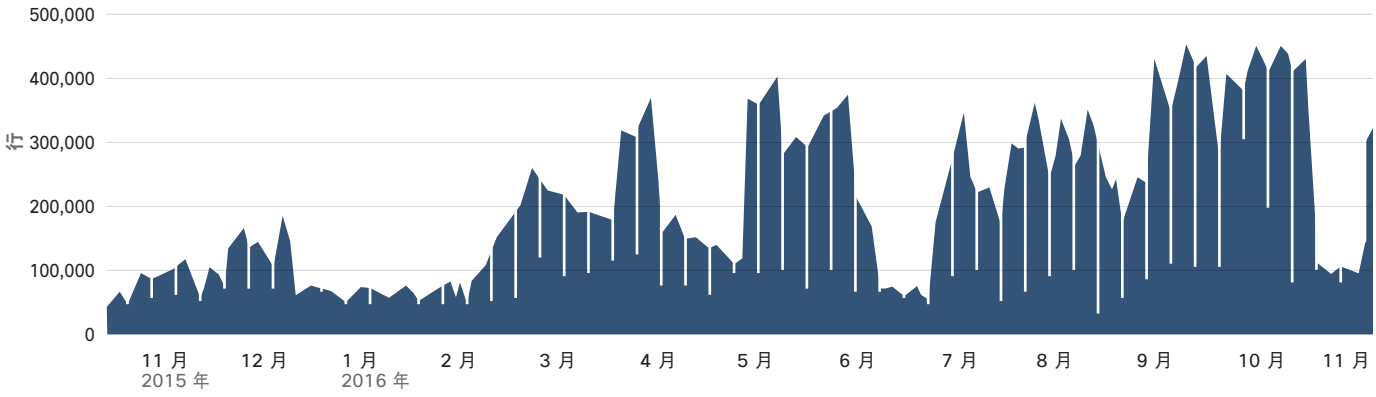
在 2015 年 11 月到 2016 年 2 月之间，SCBL 大小停留在 200,000 个 IP 地址以下。在 9 月和 10 月期间，SCBL 大小超过 400,000 个 IP 地址，然后在 10 月份有所下降，我们的威胁研究人员认为这种下降是因为 Necurs 操作者暂停了攻击。另请注意，6 月份也出现了显著下降情况。在 5 月底，与 Lurk 银行木马有关的犯罪分子在俄罗斯落网（请参阅第 21 页）。随后，包括 Necurs 在内的几大威胁纷纷销声匿迹。但是，3 周后，Necurs 重回人们视野，在不到 2 小时内，其 200,000 多个 IP 地址就出现在 SCBL 列表中。

图 15 垃圾邮件总量



来源：CBL

图 16 SCBL 的总规模



来源：SpamCop

分享

[13] 有关 CBL 的更多信息，请访问 http://www.abuseat.org/。

发送 Necurs 垃圾邮件的许多主机 IP 都已感染 2 年多。为帮助充分掩蔽此僵尸网络，Necurs 仅从部分已感染主机发送垃圾邮件。受感染主机可能使用 2 至 3 天，有时候会间隔 2 至 3 个星期都不再使用。此行为使应对垃圾邮件攻击的安全人员更难以开展工作。他们可能认为自己已经找到并成功清理受感染的主机，但事实上 Necurs 背后的操作者只是在等待机会发起另一轮攻击。

2016 年 10 月发现的垃圾邮件中，有 75% 包含恶意附件。其中大部分垃圾邮件发自 Necurs 僵尸网络。（请参阅图 17。）Necurs 可发送恶意 .zip 附件，其中包含 JavaScript、.hta、.wsf 和 VBScript 下载程序等嵌入式可执行文件。在计算包含恶意附件的垃圾邮件总数的百分比时，我们将“容器”文件 (.zip) 和其中的“子”文件（如 JavaScript 文件）计为单个恶意附件。

攻击者尝试多种附件类型，使恶意垃圾邮件活动花样百出

我们的威胁研究人员分析了攻击者如何使用不同类型的文件附件来防止恶意垃圾邮件被检测出来。我们发现，他们不断地调整策略，尝试各种各样的文件类型，并且一旦失利就会立即迅速转换战术。

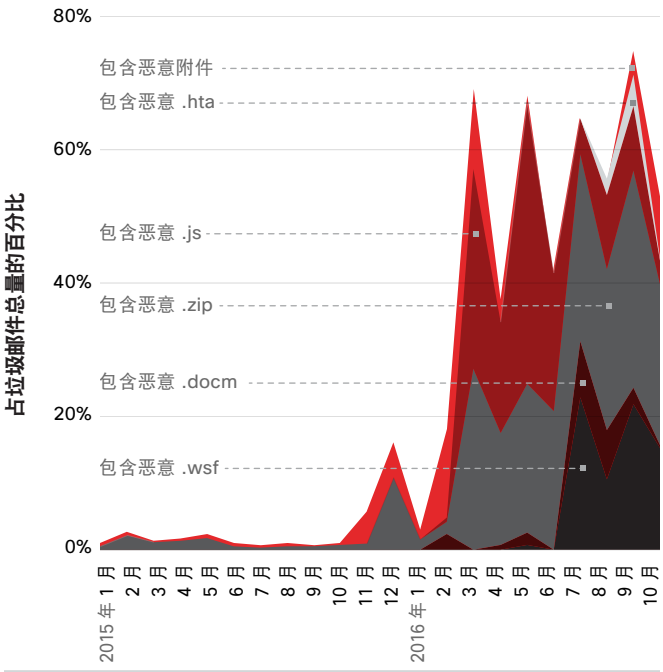
图 17 显示在观察期间，恶意垃圾邮件操作者尝试了使用 .docm、JavaScript、.wsf 和.hta 文件。如前所述，这其中许可文件类型都与 Necurs 僵尸网络发送的垃圾邮件相关。（有关我们分析的其他文件类型的研究信息，请参阅第 78 页中的附录。）

特定月份中不同文件类型的具体百分比，通过当月所观察到的包含恶意附件的垃圾邮件总数百分比推导得出。例如，2016 年 7 月，.docm 文件占所观察到的恶意附件总百分比的 8%。

2016 年 .wsf 文件的模式（请参阅图 17）提供了一个示例，可以说明攻击者如何不断发展其恶意垃圾邮件战术。在 2016 年 2 月份之前，此文件类型很少用作恶意附件。随后，由于 Necurs 僵尸网络越来越活跃，此类文件类型开始蔓延。截至 7 月，.wsf 文件的数量已占恶意垃圾邮件附件总量的 22%。与此同时，全球垃圾邮件活动也显著增多（请参阅上一部分），其中增加的大部分垃圾邮件都来自 Necurs 僵尸网络。

通过 8、9 和 10 月份的数据，我们可看出 .wsf 文件百分比的波动情况。这种情况表明，如果文件类型频繁被检测出来，攻击者会暂停活动。

图 17 包含恶意附件的垃圾邮件总量所占百分比



来源：思科安全研究部门

Hailstorm 和 Snowshoe

有两种类型的恶意垃圾邮令防御者感到异常棘手：Hailstorm 攻击和 Snowshoe 攻击。两者均行动迅速、目标明确，而且极具攻击性。

Hailstorm 以反垃圾邮件系统为攻击目标。这些攻击背后的操作者利用非常短暂的时间窗口，即自其发起垃圾邮件活动至反垃圾邮件系统发现它并向反垃圾邮件扫描器发出防御警报的这一段时间。在系统检测并阻止攻击者的活动前，他们通常仅有数秒或数分钟的行动时间。

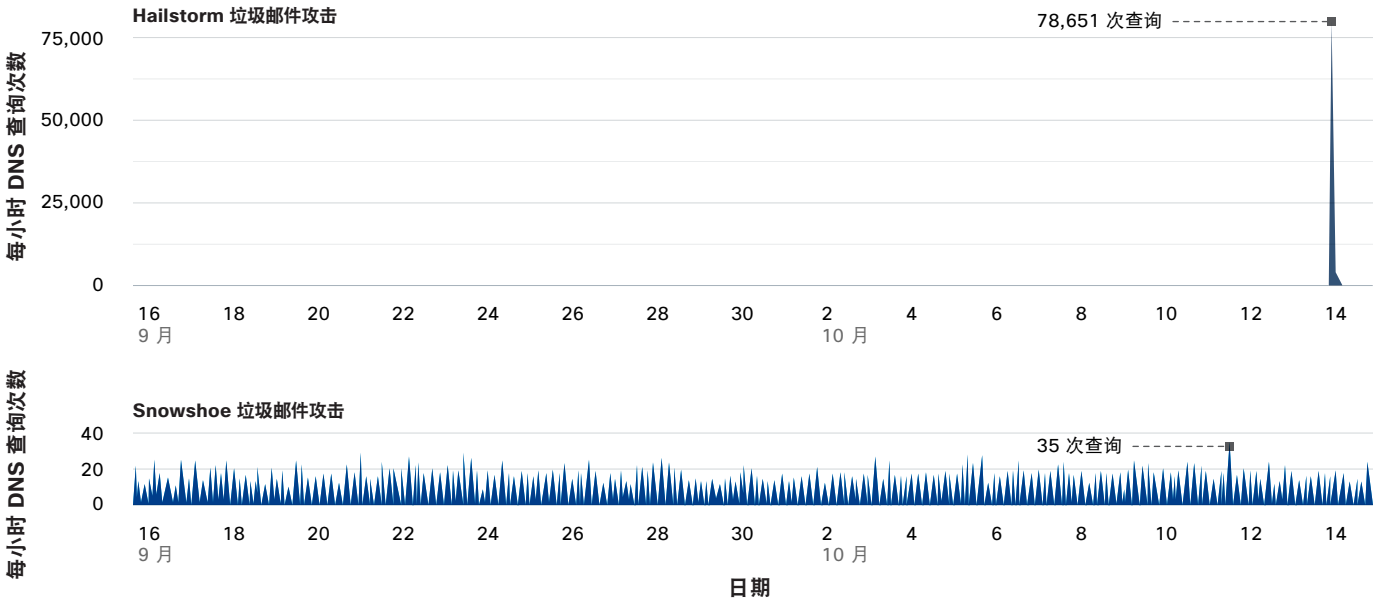
图 18 中的尖峰是 Hailstorm 攻击。此活动在“思科调查”界面有显示。在攻击之前，没有任何人解析该 IP 地址。随后，DNS 中解析该域的计算机数量飙升到 78,000 台以上，然后回落到零。

图 18 还对比显示了 Hailstorm 攻击和 Snowshoe 垃圾邮件活动，其中可以看出，攻击者企图躲避基于垃圾邮件数量的检测解决方案。DNS 查找数量稳定，但每小时大约仅有 25 个查询。攻击者可通过这些数量较少的攻击，悄然从大量的 IP 地址分发垃圾邮件。

尽管这两种垃圾邮件攻击方式迥异，但它们也有许多共同之处。通过这两种不同的方法，攻击者都可以：

- 通过从合法的 IP 和域发送垃圾邮件来避免列入信誉黑名单
- 模仿包含专业内容和订阅管理的营销邮件
- 使用配置良好的邮件系统，而非粗制滥造的脚本或垃圾邮件僵尸网络
- 正确设置前向确认的反向 DNS 和发件人策略框架 (SPF) 记录

图 18 Hailstorm 和 Snowshoe 垃圾邮件攻击的比较



来源：思科 Investigate

分享

攻击者还可通过转变文本和循环使用文件类型来削弱内容检测。（有关网络犯罪分子如何发展其威胁以逃避防御者检测的更多信息，请参阅第 34 页“演进时间”部分。）有关攻击者如何尝试在垃圾邮件中使用各种恶意文件附件的更多信息，请参阅上一部分内容。

图 19 显示排名靠前的威胁爆发警报，介绍了相关垃圾邮件和网络钓鱼邮件的概况，我们在 2016 年观察到攻击者频繁更新这些邮件以企图绕过邮件安全检查和规则。了解当前最常见的邮件威胁类型至关重要，您可以因此而避免遭受此类恶意邮件的欺诈。

图 19 排名靠前的威胁爆发报警

版本	发布号	发布名称和 URL	消息摘要	附件文件类型	语言	上次发布日期
96	35656	RuleID4626	发票，付款	.zip	德语、英语	2016/4/25
87	34577	RuleID10277	采购订单	.zip	德语、英语	2016/6/2
82	36916	RuleID4400KVR	采购订单	.zip	英语	2016/2/1
74	38971	RuleID15448	采购订单，付款，收据	.zip, .gz	英语	2016/8/8
72	41513	RuleID18688	订单，付款，研讨会	.zip	英语	2016/9/1
70	40056	RuleID6396	采购订单，付款，收据	.rar	英语	2016/6/7
66	34796	RuleID5118	产品订单，付款	.zip	德语、英语	2016/9/29
64	39317	RuleID4626（续）	发票，付款，发货	.zip	英语、德语、西班牙语	2016/1/28
64	36917	RuleID4961KVR	确认，付款/转帐，订单，发货	.zip	英语	2016/7/8
63	37179	RuleID13288	交货通知，出庭，票据发票	.zip	英语、西班牙语	2016/7/21
61	38095	RuleID858KVR	发货，报价，付款	.zip	英语	2016/8/1
58	39150	RuleID4961KVR	报价请求，产品订单	.zip	英语、德语、多种语言	2016/1/25
47	41886	RuleID4961	转帐，发货，发票	.zip	英语、德语、西班牙语	2016/2/22

来源：思科安全研究部门

在以下网站下载 2017 年图表：**www.cisco.com/go/acr2017graphics**

侦测 | 武器化 | 交付 | **安装**

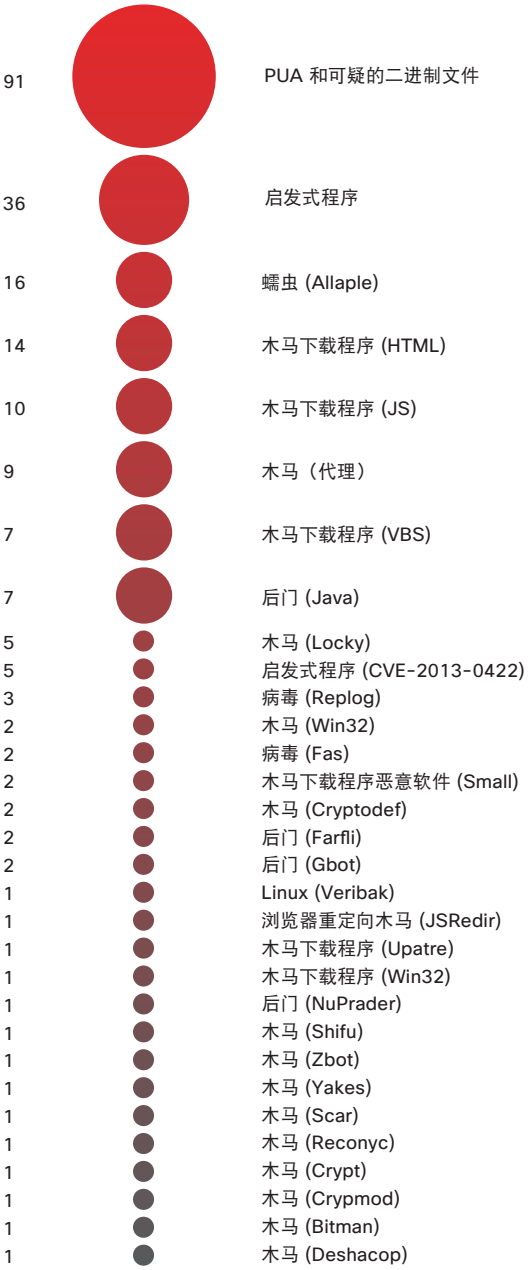
一旦威胁潜入，就会在目标系统上安装一个后门，让网络攻击者能够持续访问。

Web 攻击方法：“长尾”快照揭示用户可轻松避免的威胁

所谓 Web 攻击方法的长尾范围（图 20），涵盖一系列用于攻击链尾阶段（安装）的少量使用的恶意软件类型。在此阶段，已传输的威胁（银行木马、病毒、下载程序或一些其他漏洞攻击包）将在目标系统中安装后门，为攻击者提供相应机会和持久访问权限，以窃取数据、启动勒索软件攻击和实施其他恶意行为。

图 20 列出的威胁是恶意软件签名的示例，不在前 50 个被观察到最常用的恶意软件类型之列。Web 攻击方法的长尾，本质上讲是一种威胁快照，可在成功攻击后秘密的在机器或系统上进行活动。在这些感染中，许多都是因为遭遇了恶意广告软件攻击，或是陷入了精心设计的网络钓鱼诈骗之中。通常，用户都可以轻易避免或迅速补救这些情况。

图 20 观察到的少量使用恶意软件的示例



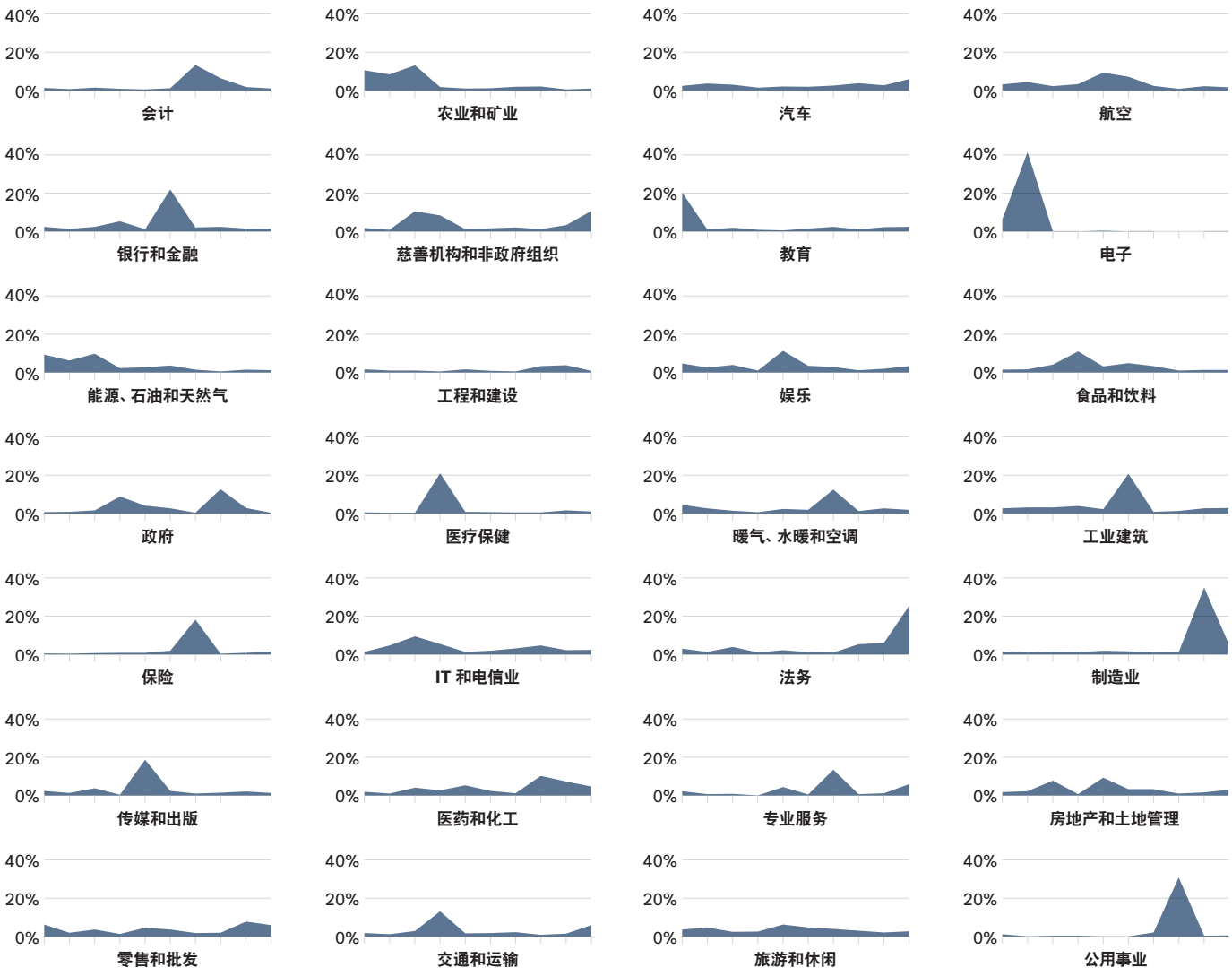
来源：思科安全研究部门

垂直行业遭受恶意软件攻击的风险：攻击者无孔不入，牟取利益

在《*思科 2016 年年中网络安全报告*》中，关于恶意软件风险的一条关键信息是，“没有哪个垂直行业是安全的”。从我们的研究人员对攻击流量（“阻止率”）、“正常”流量或行业预期流量的定期分析来看，报告中传递的这一信息在下半年得到了印证。

通过对垂直行业及其阻止率进行一段时间的观察（图 21），我们发现，在这几个月的某个时间点，每个行业都出现了不同程度的攻击流量。很明显，随着攻击的此起彼伏，不同的垂直行业都会在某个时间内受到一定程度的影响，无一幸免。

图 21 每月垂直行业阻止率百分比



来源：思科安全研究部门

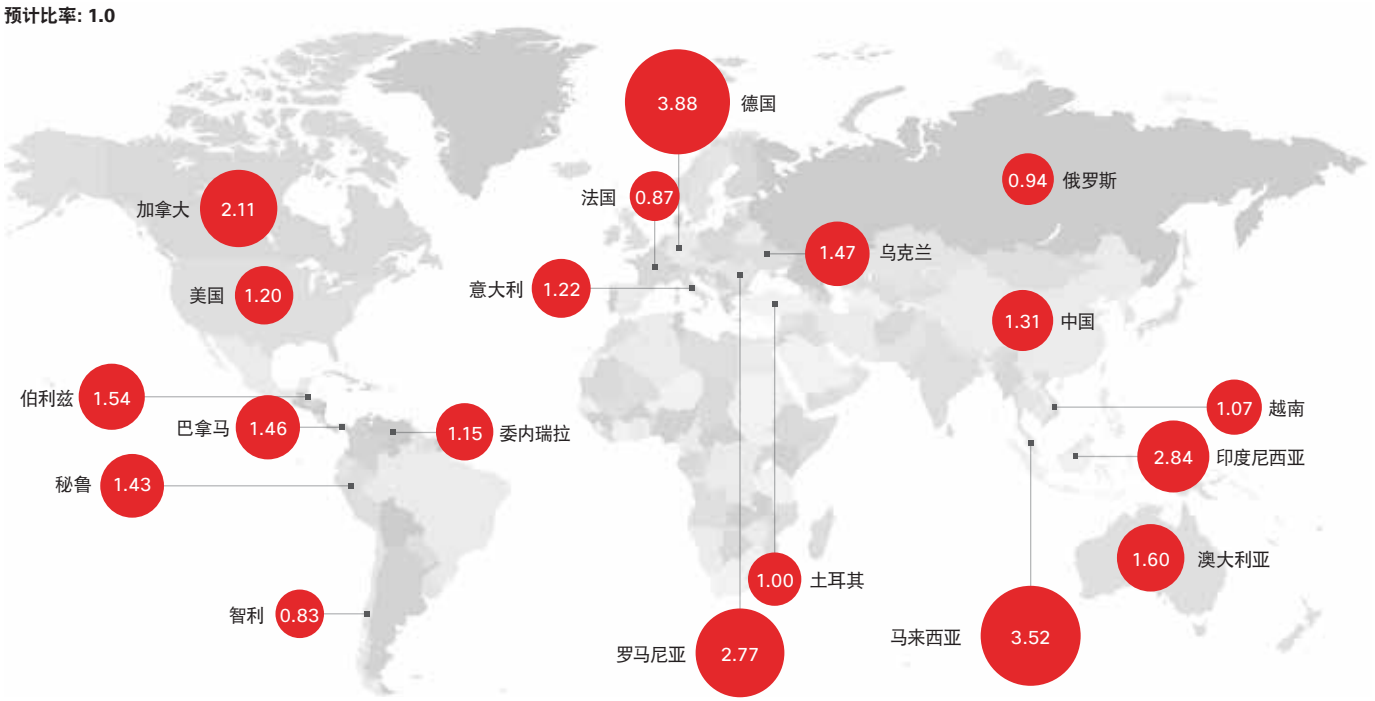
Web 阻止活动的地区概况

攻击者经常更换其行动根据地，寻找可从中发起攻击活动的薄弱基础设施。通过研究总体互联网流量和阻止活动，思科威胁研究人员得以洞悉恶意软件的来源。

如图 22 所示，相比《*思科 2016 年年中网络安全报告*》中的阻止率，来自美国的流量略微上升。美国占的阻止活动比例较高，但应考虑到，这种情况与美国在线流量比例较高有关。此外，美国是恶意软件攻击的全球最大目标之一。

对安全专业人员的启示：如同垂直 Web 阻止活动，区域性 Web 阻止活动表明恶意软件流量是一个全球性的问题。

图 22 按国家或地区划分的网络威胁阻止情况



来源：思科安全研究部门

分享

检测时间：一个衡量防御者进展的基本指标

思科一直不断改进其测量 TTD 的方法，让我们能够确保跟踪和报告最准确的 TTD 中值评估值。我们最近对方法所做的调整是，增强对以下文件的可视性：最初观察归类为“未知”，然后在经过继续分析和全球观察后被确定为“已知恶意”的文件。通过更全面的数据可视性，我们可以更准确地确定威胁首次出现的时间，以及安全团队确定此威胁所需的确切时间。

这种新的洞察力可帮助我们分析出，我们在 2015 年 11 月的 TTD 中值为 39 小时。（请参阅图 23。）截至 2016 年 1 月，我们已将 TTD 中值降低到 6.9 小时。在收集和分析 2016 年 10 月的数据后，我们的威胁研究人员确定，思科产品在 2015 年 11 月至 2016 年 10 月期间实现的 TTD 中值为 14 小时。（注：2016 年的 TTD 中值数字为观察期间的平均值）。

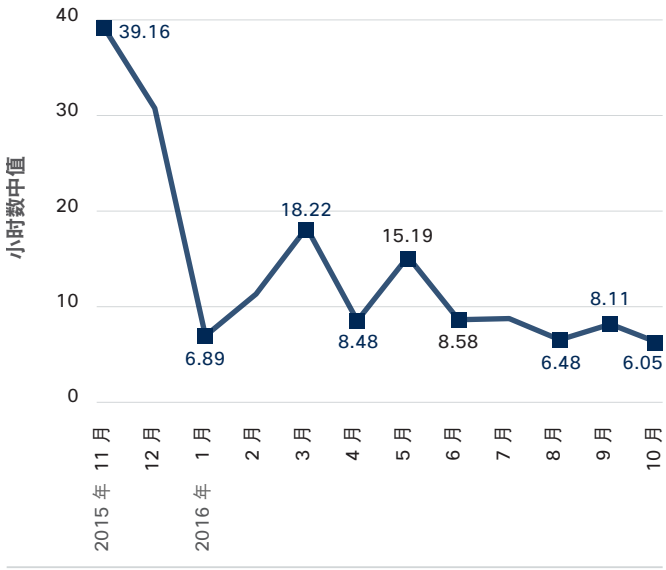
TTD 中值在整个 2016 年有所波动，但整体呈下降趋势。TTD 中值增加，表明攻击者在此期间发起了新的一轮威胁。随后中值有所下降，反映出防御者在此期间占据有利地位，并可以迅速识别出已知威胁。

从图 23 也可看出，到 2016 年 4 月底，TTD 中值约为 15 小时，大于我们在《*思科 2016 年年中网络安全报告*》中报告的数字 - 13 小时。[14] 15 小时这个数字是基于从 2015 年 11 月到 2016 年 4 月期间收集的数据。该数字不是用我们改进后的方法得出的，未分析关于文件的更多详尽回顾性信息。使用新的年中 TTD 数字，我们可以发现，从 2016 年 5 月至 10 月期间 TTD 下降到了约 9 小时。

查看回顾性数据不仅对于确定更为准确的 TTD 中值测量值至关重要，而且对于研究威胁如何随时间变化同样有着举足轻重的作用。当前形势下，许多威胁具有较强的躲避检测的能力，即使安全社区已知其存在，也仍需花费较长的时间去识别。

攻击者将改进某些恶意软件系列，以躲避检测并延长其行动时间。这种策略将阻碍防御者在检测许多已知类型的威胁方面获得优势并继续保持该优势。（有关该主题的更多信息，请参阅第 34 页“演进时间：对于某些威胁，变化持续不断”）。然而，实际上网络犯罪分子经常迅速地改进其威胁，这表明他们正面临着持续和强大的压力，力求保持其威胁凑效并带来收入。

图 23 按月显示的 TTD 中值



来源：思科安全研究部门

思科将“检测时间”或 TTD 定义为从发生入侵到发现威胁之间的这段时间窗。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时间窗口。利用我们的全球可视性和持续分析模型，对于在发现时没有分类的所有恶意代码，我们都能够测出从恶意代码开始在终端上运行到它被确定为威胁之间的时间。

[14] *思科 2016 年年中网络安全报告*：**http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html**。

演进时间：对于某些威胁，变化持续不断

网络犯罪分子使用各种混淆技术，使恶意软件保持强大和有利可图。他们常用的两种方法是，改进负载传送类型并快速生成新文件（成功躲避仅散列检测方法）。我们的研究人员仔细分析了攻击者如何使用这两种策略来帮助六个臭名昭著的恶意软件系列（Locky、Cerber、Nemucod、Adwind RAT、Kryptik 和 Dridex）避开检测并继续危害用户和系统。

通过我们的分析，我们尝试测量了“演进时间”(TTE)：攻击者更改特定恶意软件传送方式所花的时间以及每次更改策略的间隔时间。我们分析了不同思科来源的 Web 攻击数据，特别是 Web 代理数据、云和终端高级恶意软件产品，以及复合反恶意软件引擎。

我们的研究人员调查传送恶意软件的文件扩展名变化，以及用户系统定义的文件内容（或 MIME）类型变化。我们确定每个恶意软件系列都具有独特的演进模式。对于每个系列，我们分析了 Web 和邮件传送方法的模式。我们还跟踪了与每个恶意软件系列相关联的独特散列时间，以确定攻击者创建新文件（以及新散列）的速度。

通过我们的研究，我们了解到：

- 勒索软件系列似乎也有类似的新二进制文件循环。但是，Locky 使用更多的文件扩展名和 MIME 组合来传送负载。
- 一些恶意软件系列仅使用少量的文件传送方法。其他软件使用 10 种或更多方法。攻击者倾向于长期使用有效的二进制文件。在某些情况下，文件突然出现然后便迅速消失，表明恶意软件开发者面临压力，需要转换战术。
- Adwind RAT 和 Kryptik 恶意软件系列具有较高的 TTD 中值。（有关 TTD 的更多信息，请参阅第 33 页。）我们还发现这些系列包括存活期跨度更大的文件。这表明攻击者会重新使用他们发现难以被检测出的有效二进制文件。
- 观察 Dridex 恶意软件系列的文件存活期，看似这种影子经济可能正在放弃使用此一度风行的银行木马。在 2016 年下半年，Dridex 的检测量下降，开发用来传送此恶意软件的新二进制文件也有所下降。该趋势表明，恶意软件的开发者认为继续改进该威胁没有多少价值，或者他们已经找到一种新的方式来封装恶意软件，使其更难以检测。

TTE 和 TTD

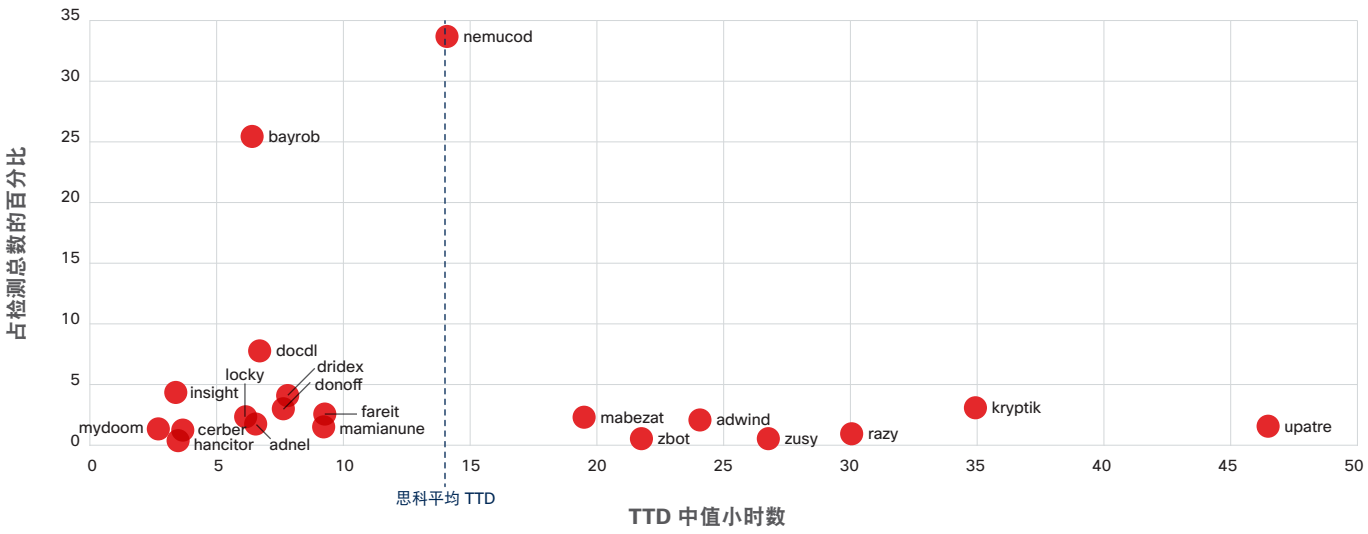
图 24 中列出了我们在 TTE 研究中分析的六大恶意软件系列。该图表描述了我们研究人员从 2015 年 11 月至 2016 年 11 月观察到的恶意软件系列中，按检测数量排名前 20 的恶意软件系列的 TTD 中值。该期间的平均 TTD 中值约为 14 小时。（有关如何计算 TTD 的详细信息，请参阅第 33 页。）

思科产品在 TTD 中值内检测到的许多恶意软件系列都是工业化威胁，由于其传播迅速，因此更为普遍。Cerber 和 Locky 这两种勒索软件均为此类威胁。

对于攻击者不愿过多改进或完全不考虑继续改进的普遍性旧威胁，思科产品通常也会在低于该 TTD 中值的时间内检测出来。此类恶意软件系列包括 Bayrob（僵尸网络恶意软件）、Mydoom（影响 Microsoft Windows 的计算机蠕虫）和 Dridex（银行木马）。

在以下几部分中，我们将分别介绍对 Locky、Nemucod、Adwind RAT 和 Kryptik 恶意软件系列的 TTE 和 TTD 研究重点。有关 Cerber 和 Dridex 的详细研究结果，请参阅第 78 页的附录。

图 24 排名靠前的恶意软件系列的 TTD 中值（检测数量排名前 20 的系列）



来源：思科安全研究部门

分享

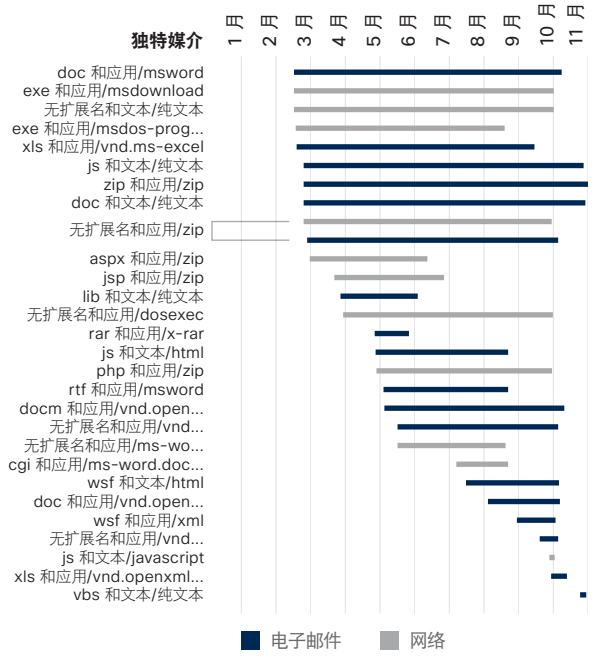
TTE 分析：Locky

通过我们的 TTE 研究，我们了解到 Locky 和 Cerber 使用有限数量的文件扩展名和 MIME 组合通过 Web 或邮件传送恶意软件。（请参阅图 25。）我们观察到有几个组合，包含与 Microsoft Word（msdownload、ms-word）相关的文件内容类型。但是，关联的文件扩展名（.exe 和 .cgi）并没有返回 Word 文件。我们还发现了指向恶意 .zip 文件的内容类型。

Locky 和 Cerber 看似也经常使用新的二进制文件，作为尝试回避基于文件的检测的手段。Locky 恶意软件系列的文件存活期见图 26。图表的上半部分显示在特定月份观察到的文件的存活期。图表的下半部分显示与 Locky 相关的散列量的月度变化，包括新文件和以前观察到的文件。

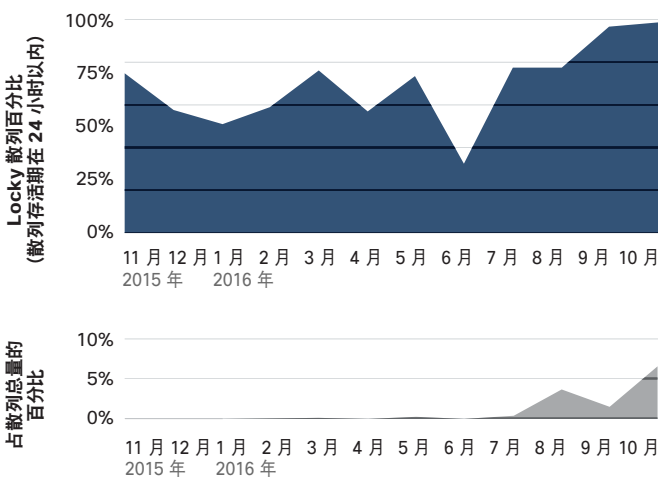
另请注意，在图 26 中，6 月份散列数量的下降，以及文件存活期的分布情况。已知传送 Locky 的 Necurs 僵尸网络于 6 月份被关闭。这可能让该恶意软件的开发者受挫，当月该恶意软件萎靡不振。然后，很明显，他们又迅速恢复了元气。到 7 月份，该恶意软件已经恢复到其更加标准的文件存活期组合，其中大多数 (74%) 文件在首次检出时存活期尚不足一天。

图 25 造成和包括 Locky 负载（Web 和邮件媒介）的威胁和指标系列的文件扩展名和 MIME 组合



来源：思科安全研究部门

图 26 Locky 恶意软件系列的散列存活期和每月观察到的散列总量百分比



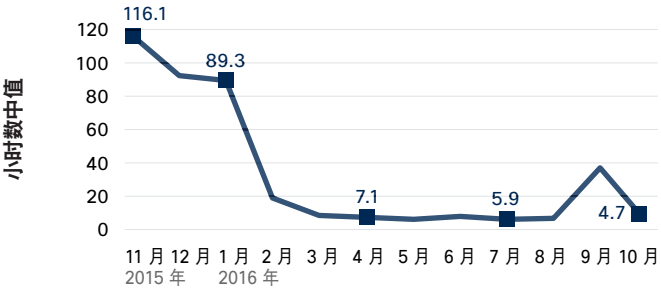
来源：思科安全研究部门

分享

此勒索软件二进制文件的快速循环并不足为奇。Locky 和 Cerber 实例通常在引入当天或之后一两天内即被检测到，因此，要想保持这些勒索软件的活力和效力，攻击者必须持续对它们进行改进。(之前讨论的图 24，表明思科产品可在 2016 年 TTD 中值内检测出 Locky 和 Cerber 勒索软件。)

图 27 表明，Locky 勒索软件的 TTD 中值已从 2015 年 11 月的大约 116 小时急剧降至 2016 年 10 月的 5 小时。

图 27 Locky 恶意软件系列的 TTD



来源: 思科安全研究部门

TTE 分析：Nemucod

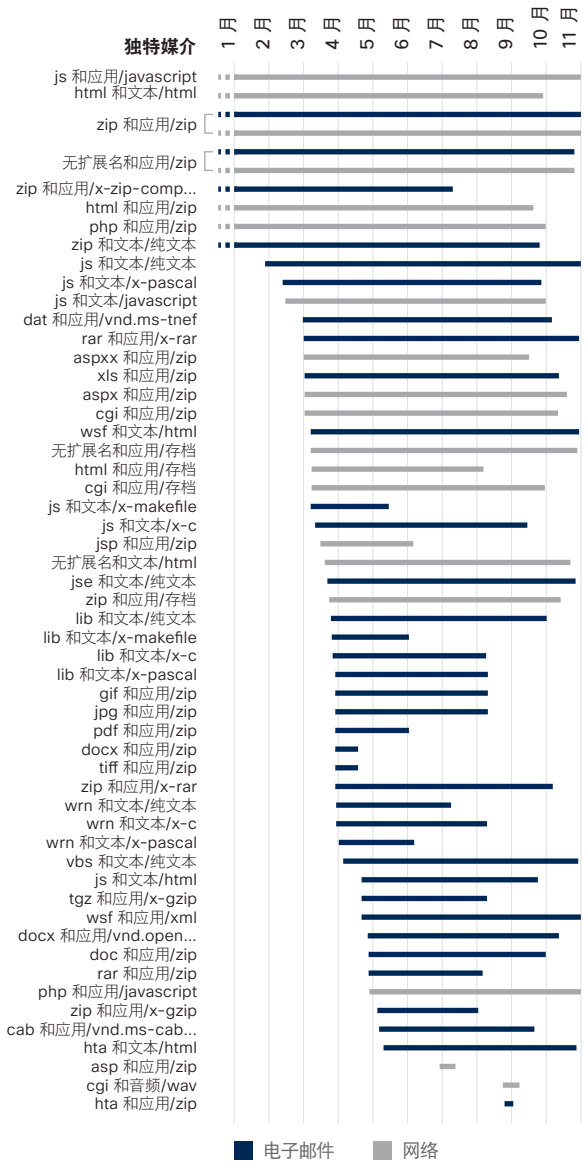
在 2016 年，Nemucod 位于观察结果中最常见恶意软件的榜首，排名前 20 的恶意软件系列见图 24。攻击者使用此下载程序恶意软件传播勒索软件和其他威胁，例如助推点击欺诈攻击活动的后门木马。Nemucod 某些变体也用作传送 Nemucod 恶意软件负载的引擎。

根据我们的威胁研究人员观察，Nemucod 恶意软件在 2016 年盛行的一个原因是，其开发者频繁改进此威胁。思科识已确定超过 15 个与 Nemucod 系列相关的文件扩展名和 MIME 组合，其中 Nemucod 系列通过 Web 传送恶意软件。许多组合用于通过邮件向用户传送威胁（图 28）。

多个文件扩展名和 MIME 组合（Web 和邮件）设计目的在于将用户定向至恶意 .zip 文件或存档。在调查的几个月中，我们发现网络攻击者还重新使用了很多组合。

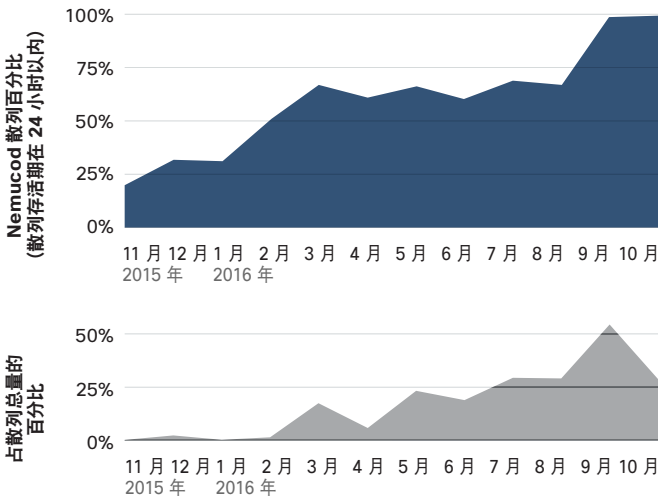
如图 29 所示，许多 Nemucod 散列在不到 2 天的时间内即被检测出。在 2016 年 9 月和 10 月间，几乎所有与 Nemucod 系列相关的二进制文件不到一天就被阻止。

图 28 Nemucod 的文件扩展名和 MIME 组合（Web 和邮件媒介）



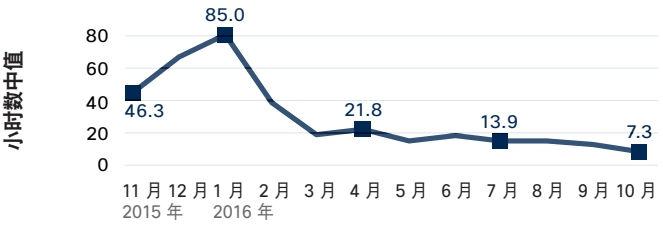
来源：思科安全研究部门

图 29 Nemucod 恶意软件系列的散列存活期以及相对于每月观察到的所有散列的百分比



来源：思科安全研究部门

图 30 Nemucod 恶意软件系列的 TTD



来源：思科安全研究部门

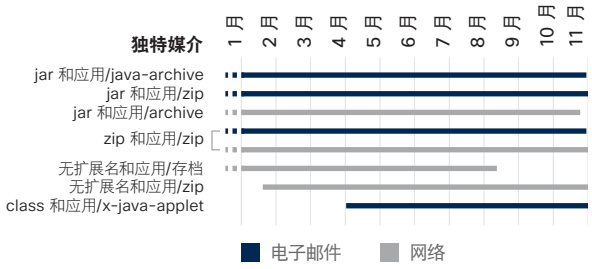
TTE 分析：Adwind RAT

思科威胁研究人员发现，Adwind RAT（远程访问木马）恶意软件通过包含 .zip 或 .jar 文件的文件扩展名和 MIME 组合来传送恶意软件。无论是通过邮件还是 Web 攻击媒介传送恶意软件，这点都毋庸置疑。（请参阅图 31。）

在 2016 年观察的大部分时间内，Adwind RAT 使用广泛的散列存活期，例外情况发生在 9 月和 10 月期间，此期间观察到的大多数文件存活期是 1 至 2 天（图 32）。

我们还发现，Adwind RAT 的 TTD 中值始终高于我们分析的其他恶意软件系列的 TTD 中值（图 33）。显然，恶意软件的开发者已开发出难以检测的传送机制，以确保 Adwind RAT 成功。因此，他们无需像其他恶意软件系列背后的操作者那样频繁或快速通过新的散列来周转。Adwind 木马还具有 JSocket 和 AlienSpy 等其他名称。

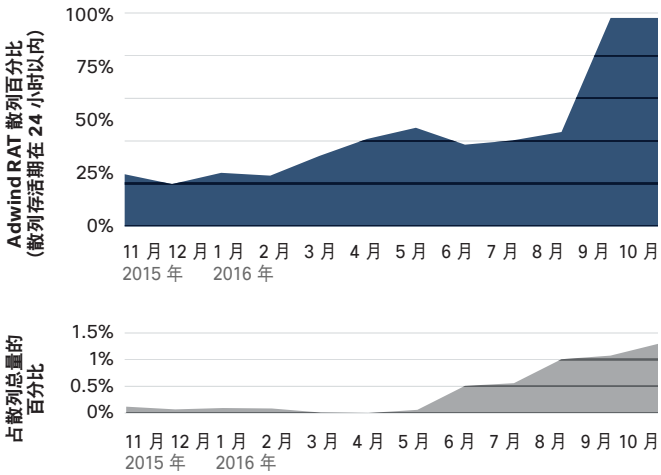
图 31 Adwind RAT 的文件扩展名和 MIME 组合（Web 和邮件媒介）



来源：思科安全研究部门

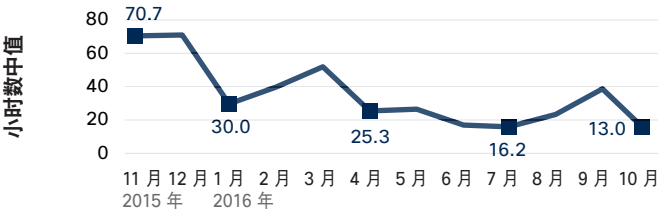
在以下网站下载 2017 年图表：**www.cisco.com/go/acr2017graphics**

图 32 Adwind RAT 恶意软件系列的散列存活期以及相对于每月观察到的所有散列的百分比



来源：思科安全研究部门

图 33 Adwind RAT 恶意软件系列的 TTD



来源：思科安全研究部门

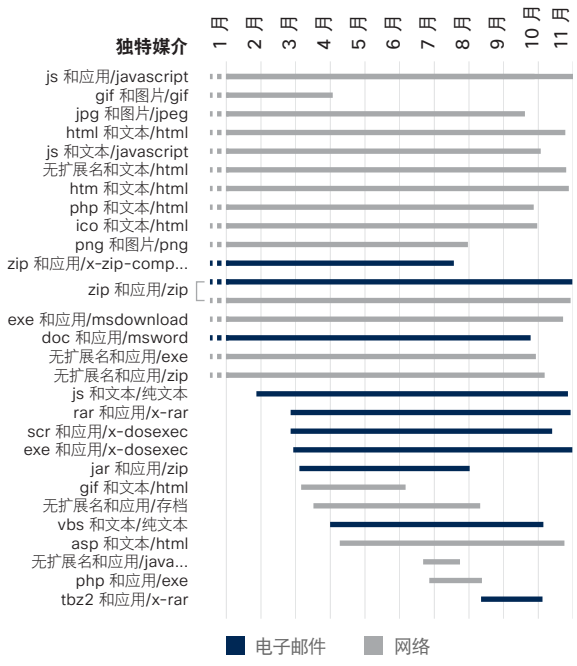
TTE 分析：Kryptik

如同 Adwind RAT 恶意软件，Kryptik 的 TTD 中值始终高于（大约 20 小时）思科在 2015 年 11 月至 2016 年 10 月 TTE 研究期间分析的其他恶意软件系列（图 36）。但是，到 10 月份，思科产品已将 Kryptik 恶意软件的 TTD 中值时间窗缩短至 9 小时以下（图 36）。

特别是在 2016 年上半年，Kryptik 恶意软件系列使用的散列存活期范围较我们分析的其他恶意软件系列更大。Kryptik 的开发者能在如此长的时间内依赖于存活期较久的散列，说明防御者在检测此类恶意软件类型上遇到了困难。

在我们的观察期间，Kryptik 的开发者采用通过 Web 攻击媒介传送负载的方法层出不穷。开发者使用适用于 Web 和邮件的文件扩展名和 MIME 组合形式的 .zip 等 JavaScript 文件和存档文件。（请参阅图 34。）某些组合可追溯到 2011 年。

图 34 Kryptik 的文件扩展名和 MIME 组合（Web 和邮件媒介）

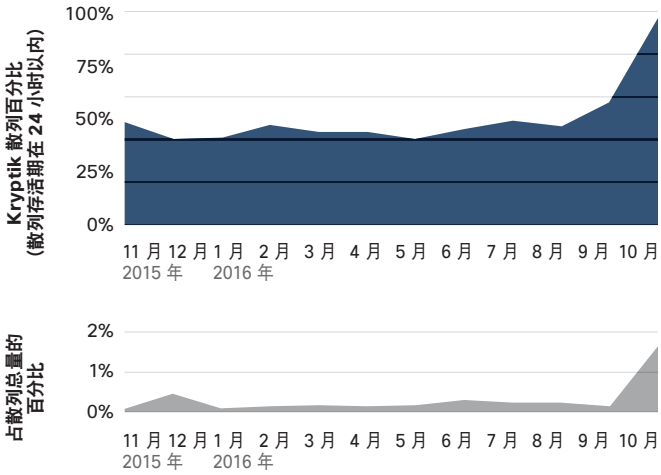


来源：思科安全研究部门

在我们对六个恶意软件系列的分析中，我们发现攻击者必须频繁地转换策略，才能利用较短的时间窗成功实施攻击。这些调整表明防御者已能更好更快地检测已知恶意软件，即使该威胁已进行改进。攻击者不得不寻找新的方式来回避检测并保持攻击活动有利可图。

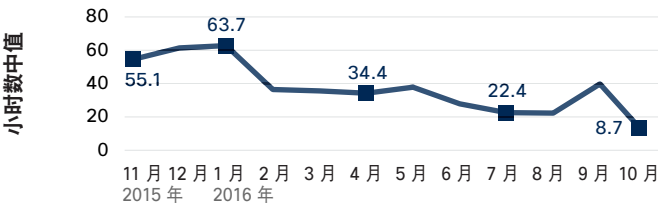
在这种瞬息万变的复杂形势下，所有恶意软件系列行为各异，单靠人类专业知识和单点解决方案并不足以识别并快速应对威胁。防御者必须具备一种集成安全架构，该架构应提供实时威胁洞察力，以及自动检测和防御功能，才能提高 TTD 并确保发生感染时快速进行补救。

图 35 Kryptik 恶意软件系列的散列存活期以及相对于每月观察到的所有散列的百分比



来源：思科安全研究部门

图 36 Kryptik 恶意软件系列的 TTD



来源：思科安全研究部门

防御者行为

防御者行为

2016 年漏洞数呈下降趋势

根据我们的研究，在 2016 年下半年，供应商披露的漏洞数量从 2015 年开始显著下降（图 37）。美国国家漏洞数据库也显示了类似下降趋势。对于所披露的漏洞公告数量下降，原因尚不十分明确。

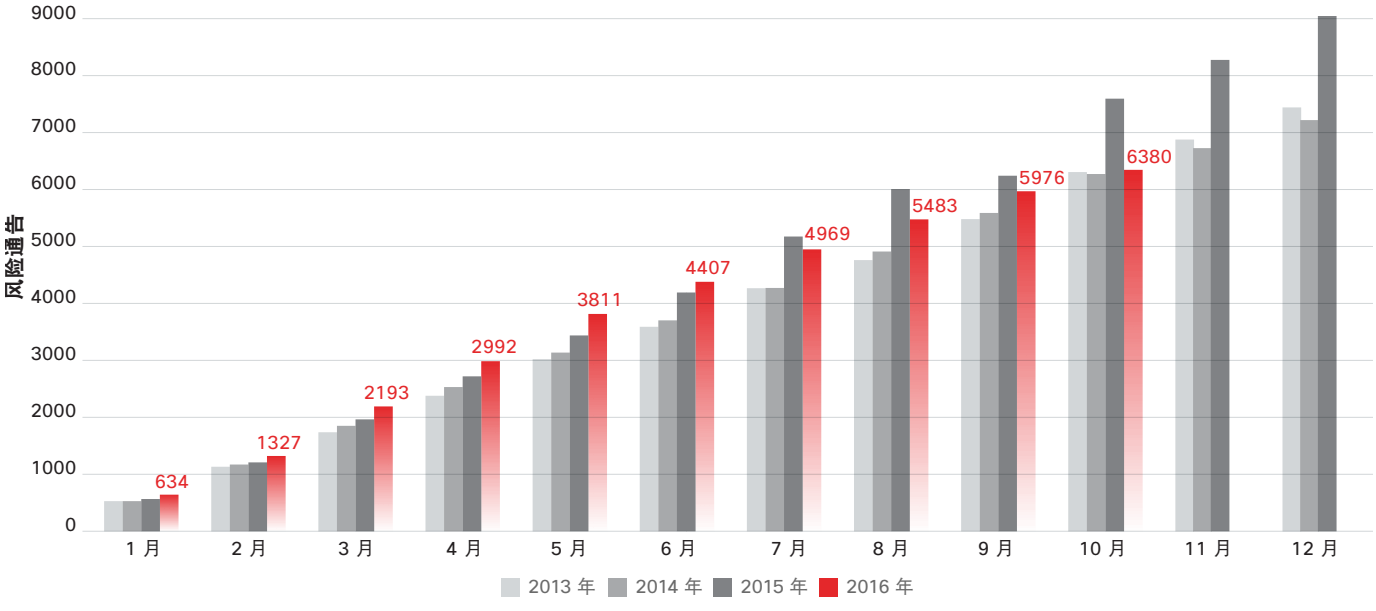
应该注意的是，2015 年是漏洞异常活跃的一年，因此 2016 年的数字可能反映出漏洞通告的正常趋势。从 2015 年 1 月到 10 月，警报总数达到 7602 个。在 2016 年同一时期，警报总数为 6380 个；2014 年同期为 6272 个。

2015 年出现的大量漏洞报告可能表明，供应商更密切关注现有产品和代码，更谨慎地实施安全开发生命周期 (SDL) 实践，以及识别漏洞并随即修复。报告的漏洞下降，可能表明这些措施正在发挥作用。也就是说，现在在产品进入市场之前，供应商已开始关注发现并修复漏洞。

在 2016 年，苹果公司是漏洞数下降最为显著的供应商：该公司在 2015 年报告的漏洞为 705 个，2016 年为 324 个（下降了 54%）。同样，思科在 2015 年报告了 488 个漏洞，2016 年为 310 个（下降了 36%）。

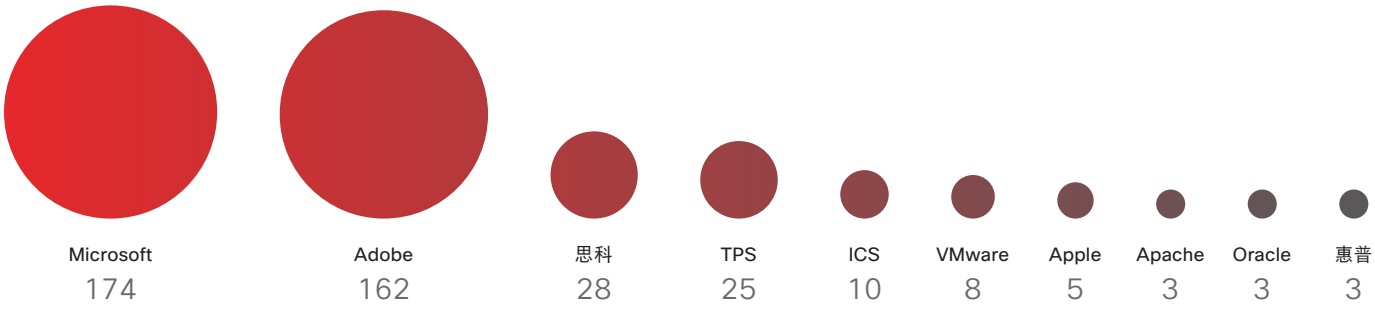
令安全研究人员较为担忧的是，部分安全专业人员可能已进入“漏洞疲乏期”。在最近几个月，尚未有重大漏洞公告像 2014 年披露的 Heartbleed 漏洞那样冲击整个行业。事实上，围绕 Heartbleed 此类“著名”漏洞的大肆宣传以及 2015 年漏洞的激增，可能造成了如今的疲乏现象，或者说，至少令人们报告漏洞的兴趣有所降低。

图 37 年度累计警报总数



来源：思科安全研究部门

图 38 按供应商和类型划分的严重漏洞公告



来源：国家漏洞数据库 (NVD)

思科现在使用严重性/影响评级 (SIR)，包括“严重”、“高”、“中等”和“低”等严重性级别。这些评级反映了简化的通用漏洞评分系统 (CVSS) 的评分优先级。此外，思科还采用 CVSS v3.0，这是 CVSS v2.0 的后继者。由于此项更改，有些漏洞可能具有比以前更高的分数，因此安全专业人员可以看到漏洞级别稍有上升，现在被评级为“严重”和“高”，而不是“中等”和“低”级别。有关此评分更改的详细信息，请阅读思科安全博文，评分安全漏洞的演变：后续。

在《思科 2017 年安全能力基准研究》（第 49 页）中，安全专业人员表示他们对于将安全融入运营的认同程度略有下降。这种下降可能与继续实施升级和补丁的需求“疲乏”有关。例如，2016 年，53% 的安全专业人员表示他们强烈同意会定期地、规范地和战略性地审查和改进安全实践；而在 2014 年和 2015 年，有 56% 的安全专业人员表示强烈同意。

当然，漏洞数量的下降不应导致对威胁形势的过度自信：任何人都不应放松对威胁的警惕，即使在没有出现高度活跃的漏洞的情况下亦是如此。

正如我们在过去的报告中提到的，安全专业人员应齐心协力，确定补丁优先级。如果因人员和其他资源的缺乏而影响到所有可用补丁的及时安装，请评估对网络安全最为关键的补丁并将其置于待办事项列表最前位置。

在以下网站下载 2017 年图表：**www.cisco.com/go/acr2017graphics**

图 39 精选关键漏洞公告

公告标题	发布日期
Adobe Acrobat 和 Acrobat Reader 内存崩溃代码执行漏洞	2016 年 7 月 28 日
Adobe Acrobat 和 Acrobat Reader 内存崩溃远程代码执行漏洞	2016 年 7 月 28 日
Adobe Acrobat 和 Acrobat Reader 内存崩溃漏洞	2016 年 7 月 21 日
Adobe Acrobat 和 Acrobat Reader 整数溢出漏洞	2016 年 5 月 23 日
Adobe Acrobat 和 Acrobat Reader 内存崩溃远程代码执行漏洞	2016 年 2 月 8 日
Adobe Acrobat 和 Acrobat Reader 内存崩溃漏洞	2016 年 7 月 28 日
Adobe Acrobat 和 Acrobat Reader 内存崩溃漏洞	2016 年 7 月 18 日
Adobe Acrobat 和 Acrobat Reader 内存崩溃漏洞	2016 年 7 月 23 日
Adobe Acrobat 和 Acrobat Reader 内存崩溃漏洞	2016 年 5 月 24 日
Adobe Acrobat 和 Acrobat Reader 内存崩溃漏洞	2016 年 5 月 23 日

来源：思科安全研究部门

上面所列的公告是精选的由多个来源报告的 2016 年评级为“严重”的漏洞，它们利用公开发布或在普通环境下可有效利用的代码来发动攻击。

服务器和客户端漏洞

正如《*思科 2016 年年中网络安全报告*》中所述，攻击者会在服务器端解决方案中寻找行动空间和时间。通过在服务器软件中发动攻击，他们有可能控制更多网络资源，或者逐步渗透到其他关键解决方案中。

思科研究人员已经在跟踪供应商带来的客户端和服务器漏洞（图 40）。

图 40 2015—2016 年客户端-服务器漏洞明细

服务器漏洞	客户端漏洞	网络漏洞
（从 2332 降至 3142）	（从 2300 降至 2106）	（从 501 降至 396）
▲34%	▼8%	▼20%

来源：国家漏洞数据库

中间件：攻击者在未打补丁软件中寻找机会

在《*思科 2016 年年中网络安全报告*》中，我们分享了有关服务器端系统攻击的数据。在 2017 年，用于连接平台或应用的中间件仍将吸引攻击者，寻求在防御者对威胁的识别或反应迟缓的环节发起攻击。

思科研究人员在寻找第三方软件漏洞的时候，平均每个月在软件中发现 14 个新漏洞。这些漏洞大部分 (62) 都是因为使用了中间件。在这 62 个漏洞中，有 20 个是在处理 PDF 的代码中发现的；有 12 个是在处理图像的代码中发现的；有 10 个是在常见办公室工作效率解决方案的代码中发现的；有 9 个是在压缩代码中发现的；有 11 个是在其他库中发现的（图 41）。

中间件中的漏洞会形成独特的安全威胁，因为它们的库通常不会像更多地面向客户端的软件（即用户日常直接使用的软件，例如，工作效率解决方案）那样快地更新。中间件库可能会排除在软件审查之外，因此漏洞仍然存在。

图 41 恶意软件库中找到的漏洞

PDF	图像	Office	压缩	其他
20	12	10	9	11

来源：思科安全研究部门

组织可能会存有侥幸心理，认为中间件很安全，并且可能将更多的注意力放在更新重要解决方案上。如果组织以赌博的心态，寄希望于攻击者不会寻求通过这些不惹人注意的途径进入网络，则最终会输掉这种赌局。中间件因而成为防御者的安全盲点，让攻击者有机可乘。

因为许多中间件解决方案来自开源开发人员，所以更新中间件库所面临的挑战与开源软件问题紧密相关（详见《*思科 2015 年年中安全报告*》）。（但是，眼下面临的问题会影响开源和专有中间件开发人员。）因此，中间件库可能需要依赖许多开发人员来使其保持更新。在负担沉重的 IT 或安全团队需要管理的任务列表上，中间件库更新可能不是重中之重，但是也应给予更大的关注。

攻击者利用的中间件漏洞有什么潜在影响？鉴于中间件与邮件或消息传送等其他重要系统之间连接在一起，攻击者会逐步渗透到这些系统并发送网络钓鱼信息或垃圾邮件。或者，攻击者还会伪装成授权用户并滥用用户之间的信任关系以获得进一步访问权限。

要避免遭受通过中间件漏洞发起的攻击，您应该采取以下措施：

- 积极维护您所使用应用中的已知相关性和库列表
- 主动监控这些应用的安全性，并尽可能缓解风险
- 在与软件供应商签订的合同中插入一个服务级别协议，要求及时提供补丁
- 定期审查和复核软件依赖关系和库使用
- 向软件供应商询问有关如何维护和测试其产品的详细信息

简而言之：修补延迟会增大攻击者的行动空间并让他们有更多时间来获得对关键系统的控制。在下一部分，我们将讨论此影响以及修补常见工作效率解决方案（例如，网络浏览器）的趋势。

修补时间：缩短恢复时间

许多用户不及时下载和安装补丁。攻击者可以利用这些未修补的漏洞进入网络。在我们的最新研究中，我们发现鼓励用户下载和安装补丁的关键在于供应商的软件更新节奏。

安全补丁发布对攻击者来说是一个明确指示，表明有可以利用的漏洞。虽然经验丰富的攻击者可能早已开始利用该漏洞，但补丁通知告诉许多其他人，早期版本有可供利用的漏洞。

如果软件供应商按照计划定期发布新版本，用户就会变得习惯于下载和安装更新。相反，如果供应商无规律地发布升级，则用户就不太可能安装更新。他们将继续运行可能包含可被利用漏洞的过时解决方案。

影响升级周期的其他行为因素包括：

- 提示体验的颠覆性
- 决定退出的简便性
- 使用软件的频率

当供应商发布升级时，用户安装升级的时间窗口很可能会不同。我们的研究人员分析了我们客户所用终端上安装的软件。这些软件分为三类：

- **新版本**：终端运行软件的最新可用版本
- **最近版本**：终端运行最新版之前的三个版本之一，但不是最新版本
- **旧版本**：终端运行落后最新版本三个版本之上的软件

例如，如果软件供应商于 2017 年 1 月 1 日发布版本 28，则版本 28 将是新版本；版本 26 是最近版本；版本 23 是旧版本。（下一页的图上包含发布软件的一个或多个版本的每周时段的标注。）

仔细观察 Adobe Flash 用户（图 42）之后，我们发现，在更新发布的第一周内，近 80% 的用户安装了软件的最新版本。换句话说，只用了大约一周时间，用户群就用上了最新版本。这一周“恢复”期是黑客稍纵即逝的好机会。

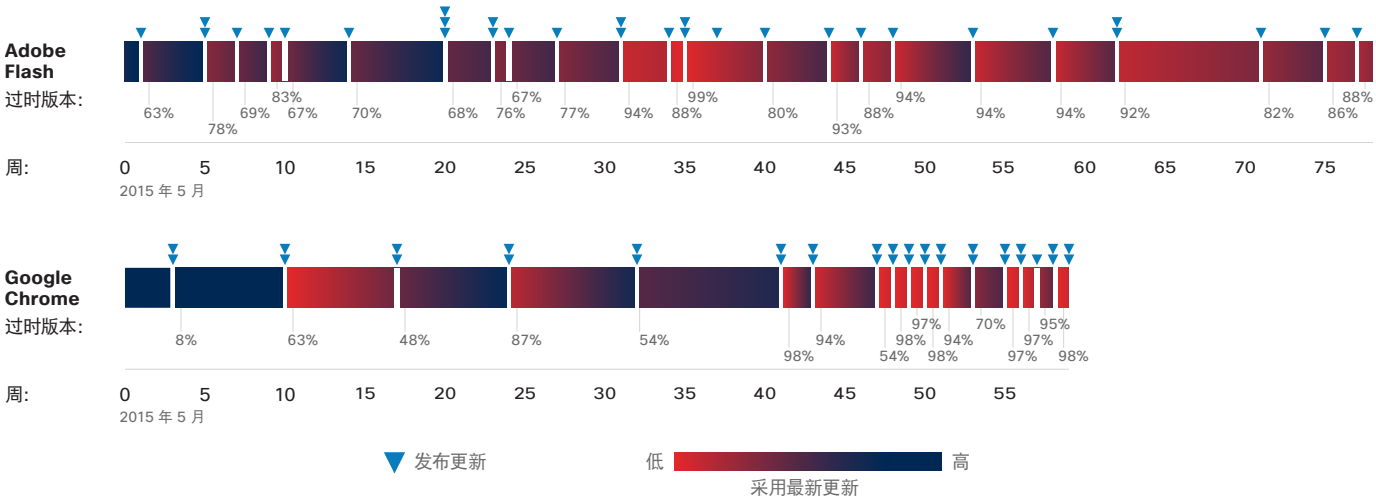
在查看 Adobe Flash 图表中 2015 年第四季度末数据时，我们看到使用该解决方案最新版本的用户数量急剧下降。在我们分析的时间段内，Adobe 紧接着发布了五个 Flash 版本，其中包括新增功能、漏洞修复和安全更新。此类大规模更新可能会让用户感到困惑。他们可能会质疑是否需要下载那么多更新；他们会因为升级通知数太多而变得疲乏；而且他们可能会认为他们已下载重要的更新，而忽略新的通知。不管是什么迫使他们对安装更新缺乏兴趣，这对防御者来说都是坏消息。

在仔细观察 Google Chrome 网络浏览器的升级之后，我们看到一种不同的模式。它体现了更有规律的升级节奏和强硬的选择退出策略，让用户更难以忽略更新通知。从图 42 可以看到，运行最新版本的终端在许多周之后保持相对稳定。

Chrome 数据显示，用户恢复速度相对较快。在定期更新情况下，一周大致上就是恢复时间线。但在贯穿 2016 年第二季度和第三季度的 9 周范围内，有七次更新。在此期间，用户群会更新，但也开始出现升级疲乏。尽管大部分用户选择更新，但坚持使用较旧版本的用户百分比稳步攀升。

Mozilla Firefox 浏览器也提供按照计划定期执行的更新，但发布更新之后的恢复期似乎需要长达一个月。就是说，该浏览器的用户不会像 Chrome 用户那么频繁地下载和安装更新。其中一个原因可能是一些用户可能不经常使用该浏览器，因此未看到通知，所以未下载更新。（请参见下页的图 43。）

图 42 Adobe Flash 和 Google Chrome 的修补时间



来源：思科安全研究部门

我们发现 Firefox 大约每隔一周更新其版本，在观察期间其更新频率有所提高。此频率的提高体现在旧 Firefox 版本用户群的增长中。恢复时间大约为 1.5 周，但时间重叠。尝试保持现状的用户群降至仅占用户基数的 30%。在某一时刻，有三分之二的用户仅运行落后最新版本超过四个版本的浏览器。因此，尽管 Firefox 会快速解决问题并修复漏洞，但用户群未按相同的频率更新和恢复。

对软件来说，使用水平似乎也是其漏洞的一个指标。当用户不经常访问软件并因而不知道需要修补和升级时，被忽视的软件就为攻击者提供了行动空间和时间。

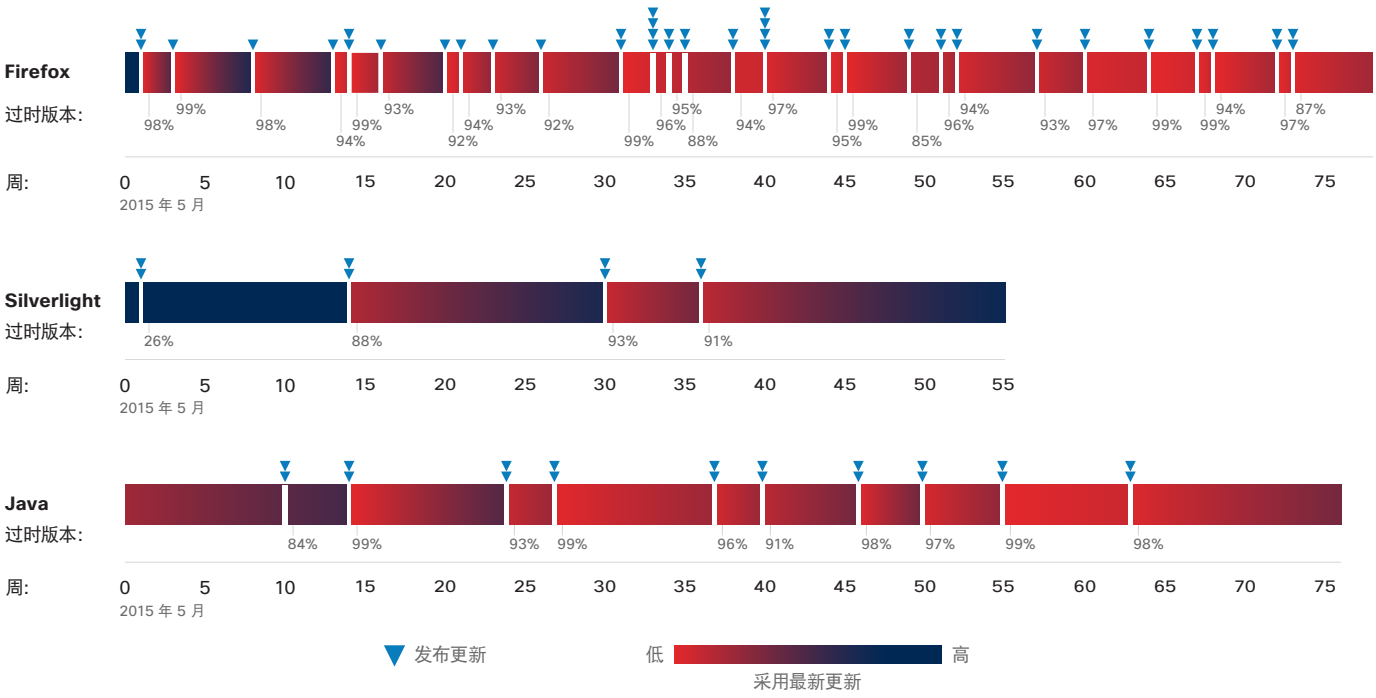
我们对 Microsoft Silverlight 的研究显示，在发布升级之后用户安装升级的恢复期长达 2 个月。正如在 2015 年第四季度至 2016 年第一季度之间可以看到，在某一时间段，5 周内有两次版本发布，对用户群产生的影响超过 3 个月。

Microsoft 在 2012 年宣告 Silverlight 寿命终止，不过，他们仍会发布补丁和漏洞修复。但是这产生了与 Internet Explorer 相同的问题：过时和未修补的软件让攻击者可轻松发起漏洞攻击。

Java 用户的恢复期显示，大多数用户运行的软件版本比最新版本落后一至三个版本。恢复时间大约为 3 周。Java 的不同寻常之处在于主要群体都使用最新版本的用户群。Java 更新周期为 1 至 2 个月。

我们从修补时间周期中获得的总体教训是，升级发布模式是用户安全状态的一个影响因素，可能会让网络处于危险之中。

图 43 Firefox、Silverlight 和 Java 的修补时间



来源：思科安全研究部门

在以下网站下载 2017 年图表：**www.cisco.com/go/acr2017graphics**

思科 2017 年安全能力基准研究

思科 2017 年安全能力基准研究

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) 经理对他们自己的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 2017 年安全能力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 2016 和 2015 年报告的结果进行了比较。该研究在 13 个国家/地区进行，超过 2900 人接受调查。

安全专业人员希望让他们的组织更安全，但在某种程度上需应对复杂的攻击者形势，以及攻击者为扩展行动空间而采取的行动。许多组织依赖于由许多供应商提供的许多解决方案。随着互联网在速度、连接设备和流量方面继续增长，这种策略让保护网络变得更复杂和混乱。如果组织要保护自己，就需要力争实现简单和集成。

观念：安全专业人员对自己的工具信心十足，但不太确定对这些工具的利用是否有效

大多数安全专业人员认为他们手边有充足的解决方案，而且他们的安全基础设施是最新的。但是，根据我们的研究，这种信心含有一些不确定性。这些专业人员并非总是确信他们可以充分利用预算和人才来真正运用他们所拥有的技术。

组织面临来自各个方面的威胁。攻击者狡猾且富有创造力，他们能够击破防御。即使在这个发人深省的环境中，大部分安全专业人员仍相信他们的安全基础设施是最新的，不过这种信心从前几年开始似乎在逐渐减弱。在 2016 年，58% 的受访者表示，他们的安全基础设施绝对是最新的，且随着最新技术不断升级。37% 的受访者表示，他们经常更换或升级安全技术，但未配备最新最好的工具（图 44）。

此外，超过三分之二的安全专业人员认为他们的安全工具非常有效或极为有效。例如，74% 的受访者认为他们的工具在阻止已知安全威胁方面非常有效或极为有效，同时，71% 的受访者认为他们的工具在检测网络异常并动态防御自适应威胁的转变方面很有效（图 45）。

图 44 认为其安全基础设施是最新的安全专业人员的百分比

来源：思科 2017 年安全能力基准研究

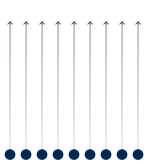
问题是：对工具有信心并不一定会转化为有效的安全性。正如研究所指出，安全部门正在努力解决来自许多供应商的复杂工具带来的问题，而且他们缺乏内部人才。这可以归结为“理想与现实”问题。安全专业人员需要简单、有效的安全工具，但他们没有实现这种愿景所需的综合方法。

安全仍是许多组织的高层人员的优先考虑事项。安全专业人员相信高管团队会在组织的关键目标列表中将安全列为高优先级事项。当然，他们面临的挑战是将高层管理人员的支持与可能影响安全成果的人才和技术相匹配。

强烈赞同高层领导将安全视为高优先级的安全专业人员数量在 2016 年为 59%，与 2015 年的 61% 和 2014 年的 63% 相比稍有下降（图 46）。在 2016 年，55% 的安全专业人员赞同组织的高管团队所明确的安全角色和职责；在 2015 年和 2014 年，有 58% 的受访者赞同此观点。

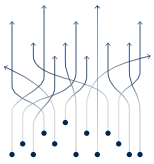
总之，安全专业人员对手边的工具有信心，而且他们在解决安全问题方面似乎得到了公司领导的重视。但是，这种信心稍有下降。安全专业人员开始意识到，攻击者会获得成功且管理不断扩大的攻击面会变得更加困难。

图 45 认为各种安全工具极其有效的安全专业人员的百分比



74%

的受访者认为其工具极其有效，可防御已知安全威胁



71%

的受访者认为其工具在检测网络异常并动态防御自适应威胁的转变方面极其有效

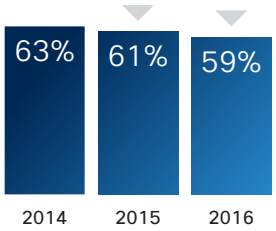
2016 年 (n=2912)

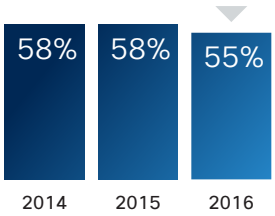
来源：思科 2017 年安全能力基准研究

图 46 认为安全是管理层的优先考虑事项的安全专业人员的百分比，2014-2016 年

强烈赞同高层领导将安全视为高优先级事项

强烈赞同组织的高管团队所明确的安全角色和职责





2014 年 (n=1738)，2015 年 (n=2432)，2016 年 (n=2912)

来源：思科 2017 年安全能力基准研究

分享

限制：时间、人才和资金影响应对威胁的能力

如果安全专业人员相对确信他们拥有检测威胁和减轻损害所需的工具，他们也会认识到某些结构性制约因素会妨碍他们实现目标。紧缩的预算是一个长期挑战。但有关有效安全的其他制约因素也会涉及安全简化和自动化的问题。

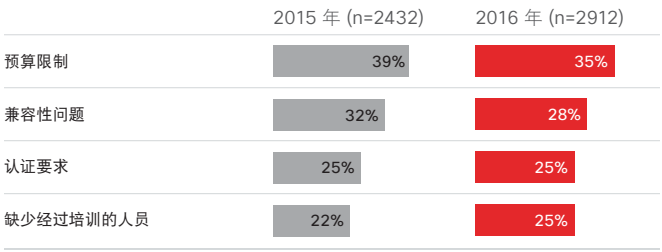
在 2016 年，35% 的安全专业人员说，预算是他们采用高级安全流程和技术的最大障碍（与 2015 年相比略有下降，那一年有 39% 的受访者说预算是最大障碍），正如图 47 所示。正如在 2015 年，传统系统的兼容性问题是第二常见障碍：在 2016 年有 28% 的受访者提到兼容性，而与之相比，2015 年为 32%。

资金仅是该问题的一部分。例如，兼容性问题证明未集成的分离系统存在问题。而对缺少经过培训人员的担忧也突显了以下问题：虽然拥有工具但没有真正了解在安全环境中发生什么情况的人才。

考虑到与针对性攻击作斗争和改变攻击战术所需的专业知识和决策能力，很难找到人才是一个需关注的问题。资源充沛和有经验的 IT 安全团队与适合的工具搭配，可以让技术和策略很好地融合，并取得更好的安全成果。

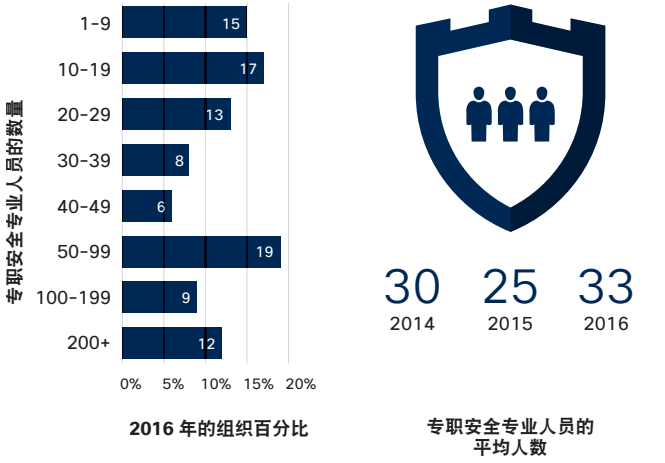
被调查组织中的安全专业人员平均数量为 33，与之相比，2015 年为 25。在 2016 年，19% 的组织拥有 50 至 99 位专职安全专业人员；9% 的组织拥有 100 到 199 位安全专业人员；12% 的组织拥有 200 位或更多安全专业人员（图 48）。

图 47 安全面对的最大障碍



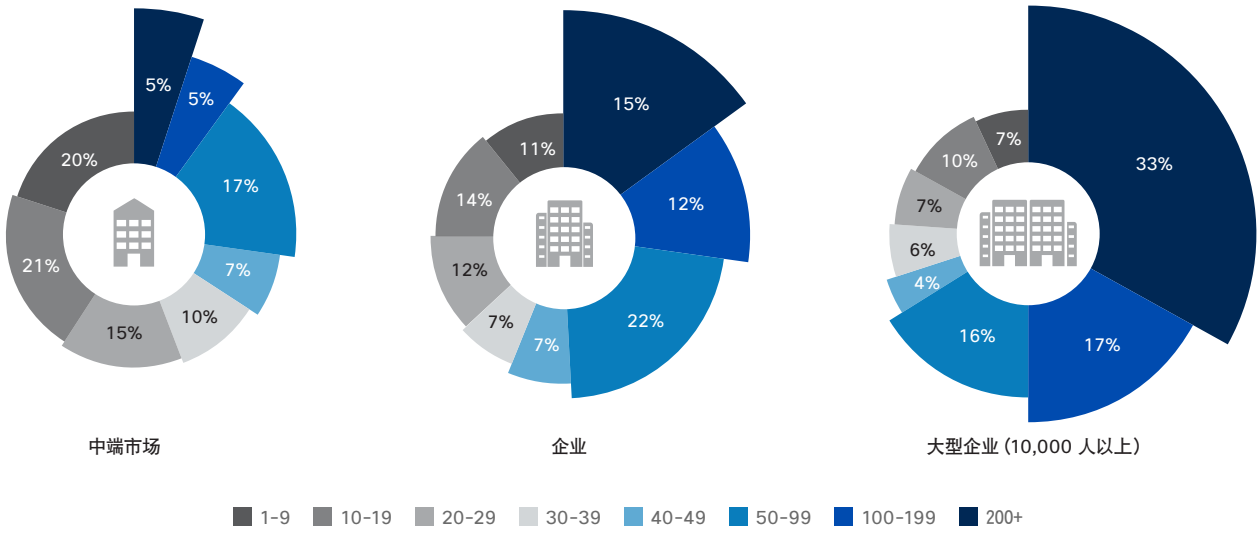
来源：思科 2017 年安全能力基准研究

图 48 组织雇佣的安全专业人员的数量



来源：思科 2017 年安全能力基准研究

图 49 按组织规模划分的安全专业人员的数量



来源：思科 2017 年安全能力基准研究

分享

安全专业人员的数量因组织规模而异。如图 49 所示，员工数在 10,000 以上的大型企业中有 33% 的企业拥有至少 200 名安全员工。

不管制约因素是什么，安全专业人员都需要问出有关限制其面对未来威胁能力的棘手问题。

例如，就预算而论，到底多少预算才真正足够？正如调查受访者所说，安全团队必须与许多其他公司优先事项进行竞争，即使在 IT 环境中也有许多竞争。如果他们无法获得资金来购置更多工具，那么他们就必须更有效地利用他们所拥有的预算。例如，可通过自动化来补偿有限的人力资源。

关于软件和硬件兼容性问题，也应询问类似的问题。随着兼容性问题增加，必须管理多少不同版本的软件和硬件（其中大部分可能无法有效运行）？安全团队将如何处理所需的多个认证要求？

外包和云帮助延伸预算

参与基准研究的许多安全专业人员认为他们在进行安全采购时资金紧缺。他们通过外包一些任务或使用云解决方案以尽量利用他们的预算。他们还依赖于自动化。

除了这些限制之外，安全专业人员也稍微不那么注重将安全融入运营。这种趋势可能会引发担忧，让人们认为安全专业人员建立的是次最优的安全基础设施。如果出现对将安全融入运营关注减弱的迹象，即表明组织尚未准备好防御不断扩大的攻击形势。

例如，在 2016 年，53% 的受访者强烈赞同他们定期、正式和战略性地审查和改进安全实践；在 2014 年和 2015 年，有 56% 的受访者强烈赞同。同样，在 2016 年，53% 的受访者表示他们强烈赞同经常性和有条不紊地调查安全事件，与之相比，在 2014 年此数字为 55%，在 2015 年此数字为 56%（图 50）。

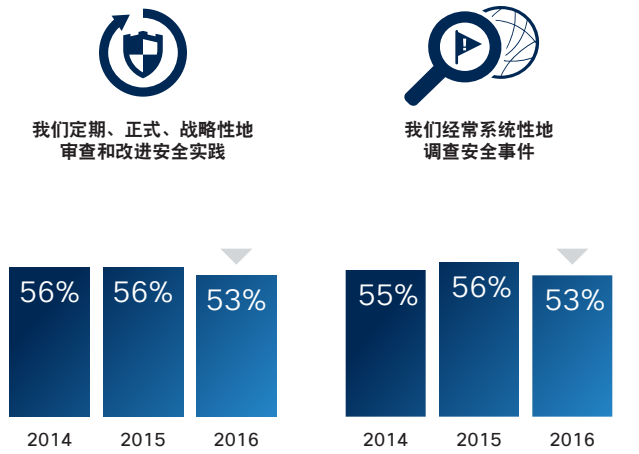
如果安全专业人员下调将安全投入使用的目标，则他们可能无法有效地部署他们所拥有的工具，更不用说增加新工具，这并不令人意外。正如调查受访者告诉我们的那样，如果他们无法使用他们手头上已经拥有的技术，则他们需要更简单的简化工具来使安全流程实现自动化。而这些工具需要让专业人员全面了解网络环境中的整体情况。

缺乏对安全集成即会留下时间和空间缺口，从而让恶意攻击者可以发起攻击。安全专业人员倾向于努力对付来自许多供应商的解决方案和平台，从而使建立无缝防御复杂化。如图 51 所示，大多数公司在其环境与五个以上安全供应商合作和使用五个以上安全产品。55% 的安全专业人员至少与六家供应商合作；45% 的专业人员在任何地方与一到五家供应商合作；而 65% 的专业人员使用六个或更多产品。

如果将安全融入运营的目标降低，如果未最有效地使用工具，以及如果人力资源不够充足，则结果是让安全变得摇摇欲坠。安全专业人员不得不略过对警报的调查，仅仅因为他们没有可用于确定哪些警报很关键以及为什么会发生这些警报的人才、工具或自动化解决方案。

在以下网站下载 2017 年图表：**www.cisco.com/go/acr2017graphics**

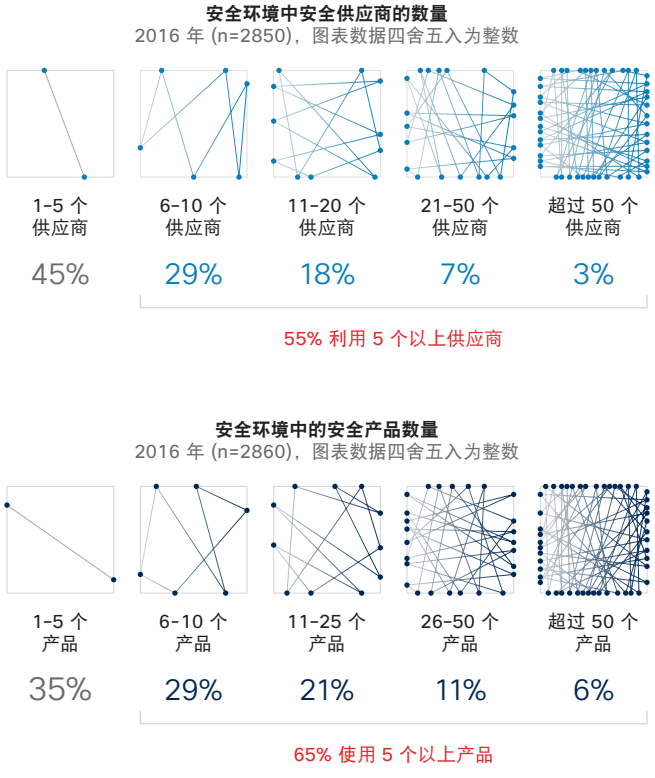
图 50 强烈赞同将安全融入运营的论述的受访者百分比



2014 年 (n=1738)，2015 年 (n=2432)，2016 年 (n=2912)

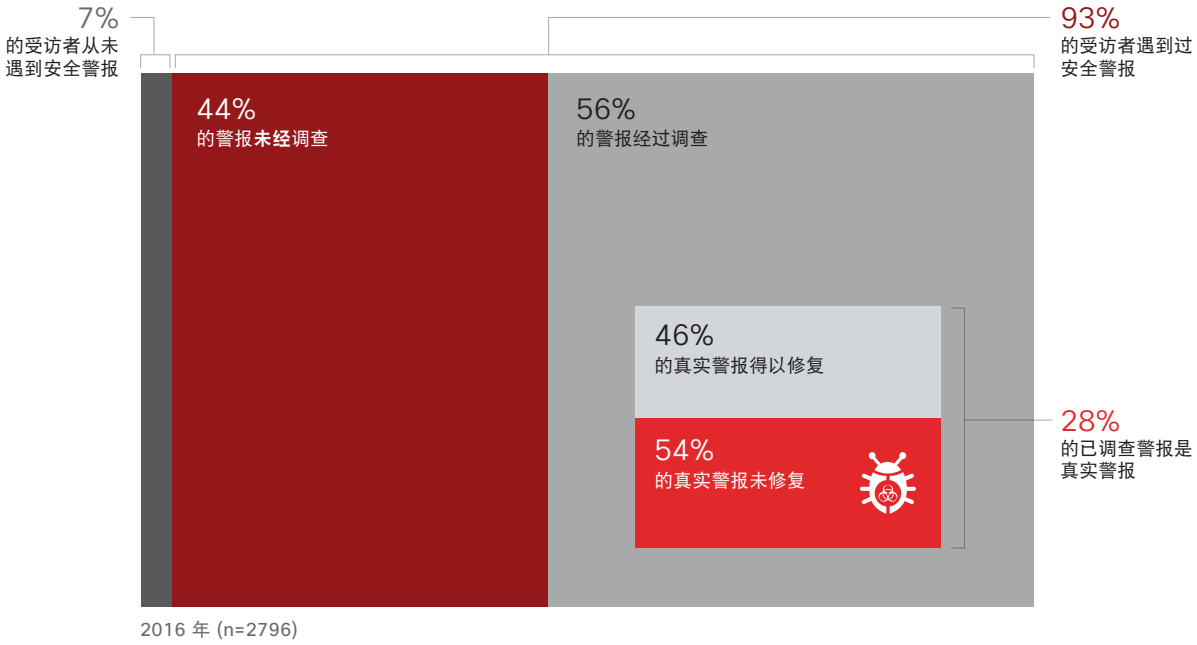
来源：思科 2017 年安全能力基准研究

图 51 组织所用的安全供应商和产品的数量



来源：思科 2017 年安全能力基准研究

图 52 未经调查或修复的安全警报的百分比



来源：思科 2017 年安全能力基准研究

可能由于众多因素的影响（例如，缺乏集成防御系统或员工缺少时间），组织只能够调查他们在某一天所收到的安全警报中的一半多一点。如图 52 所示，56% 的警报经过调查，44% 的警报未经调查；在已调查的那些警报中，有 28% 的警报被认定为真实警报。然后，有 46% 的真实警报得以修复。

为了更具体地说明问题，我们举例来说，如果组织每天记录 5000 条警报，这意味着：

- 2800 条警报 (56%) 经过调查，而有 2200 条 (44%) 未经调查
- 在经过调查的警报中，有 784 条警报 (28%) 是真实的，而有 2016 条 (72%) 不是真实警报
- 在真实警报中，有 360 条 (46%) 得以修复，而有 424 条 (54%) 未修复

事实上，有近一半的警报未经调查，这应当引起重视。在没有修复的警报组中有什么：它们可能只是传播垃圾邮件的低级威胁，也可能会导致勒索软件攻击或削弱网络？要调查和了解更大的威胁形势，组织需要依赖自动化且适当集成的解决方案。自动化可帮助组织尽量利用宝贵的资源及让安全团队摆脱检测和调查的重担。

安全团队无法查看如此多的警报，从而会引发关于它们对组织的总体成功产生的影响问题。这些未经调查的威胁对工作效率、客户满意度和企业信心造成什么样的影响？正如受访者告诉我们的那样，即使微小的网络中断或安全漏洞也会对最后结果产生长期影响。即使损失相对较小，且受影响的系统非常容易识别和隔离，但因为对组织造成了压力，所以安全领导也认为这些中断有重大影响。

分享

压力会在许多方面对组织产生影响。安全团队必须花费时间来管理出现安全漏洞后发生的网络中断。这些中断中有近一半会持续长达 8 小时。45% 的中断持续 1 至 8 小时（图 53）；15% 的中断持续 9 至 16 小时，11% 的中断持续 17 至 24 小时。这些中断中有 41% 会影响组织中 11% 至 30% 的系统。

影响：越来越多的组织因漏洞而蒙受损失

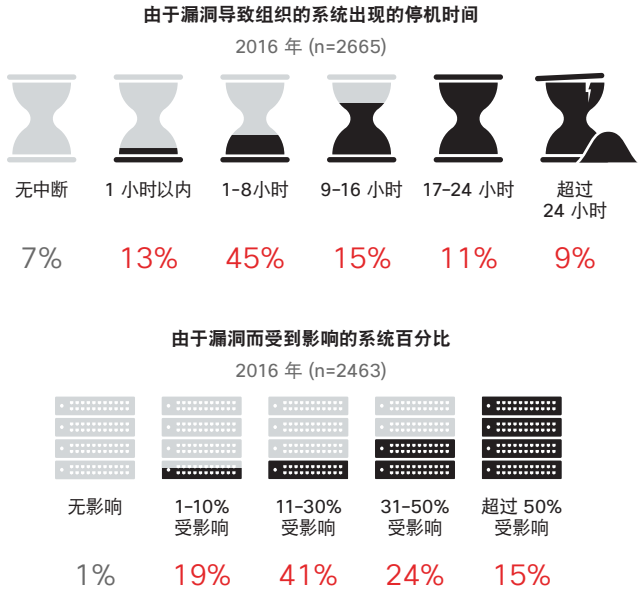
漏洞的影响不仅限于中断。漏洞也意味着金钱、时间和声誉损失。认为自己能躲过这一劫的安全团队忽视现实数据。正如我们的研究所示，几乎半数组织在出现安全漏洞之后不得不应对公众关注。鉴于攻击者具备能力和战术，问题不在于是否会出现安全漏洞，而在于何时出现。

正如基准研究所示，安全专业人员在出现漏洞时才认清现实。他们经常更改安全策略或增强防御。其网络还未被攻击者攻破的组织可能会因为逃脱攻击而松了一口气。但是，这种信心可能投错了地方。

有 49% 的被调查安全专业人员表示，其组织不得不应对安全漏洞的公众关注。在这些组织中，有 49% 的组织主动披露漏洞，而 31% 的组织表示其漏洞由第三方披露（图 54）。换句话说，接受调查的组织中有近三分之一不得不应对非自愿披露的漏洞。很明显，安静地处理漏洞的时代已经一去不复返。有太多的监管机构、媒体和社交媒体用户会揭露问题。

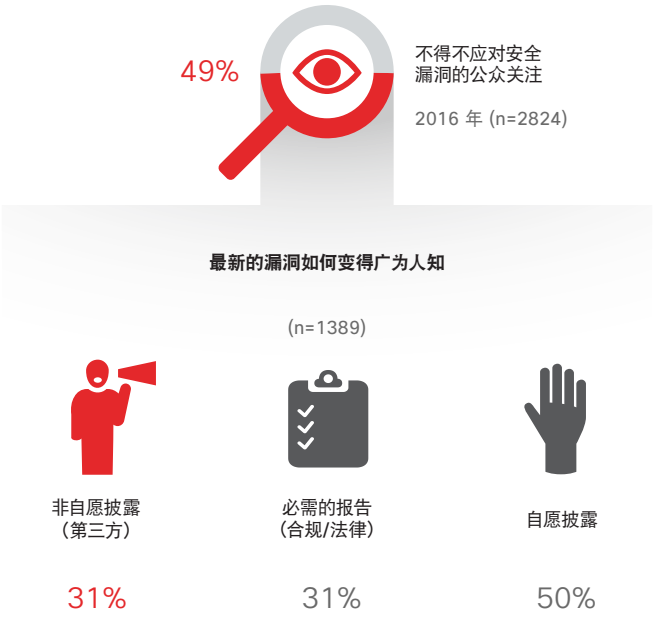
分享

图 53 由安全漏洞引起的中断的时间长度和广度



来源：思科 2017 年安全能力基准研究

图 54 遇到公开漏洞的组织的百分比



来源：思科 2017 年安全能力基准研究

图 55 最有可能受到公开漏洞影响的职能

来源：思科安全研究部门

对组织造成的损害远远超过组织处理漏洞或中断所花的时间。企业应尝试竭尽全力避免真正和实质性的影响。

如图 55 所示，36% 的安全专业人员表示，运营是最有可能受到影响的职能。这意味着将影响从运输到医疗保健到制造的各个行业的核心生产力系统会放慢速度，甚至会完全停止。

在运营之后，财务是最有可能受影响的职能（有 30% 的受访者选择此项），然后是品牌声誉和客户保留率（均为 26%）。

任何打算获得增长和取得成功的组织都不希望面临重要部门受到安全漏洞影响的状况。安全专业人员在查看调查结果应考虑到他们自己的组织，然后问问自己：如果我的组织因漏洞而遭受此类损失，则在一段时间之后企业会发生什么？

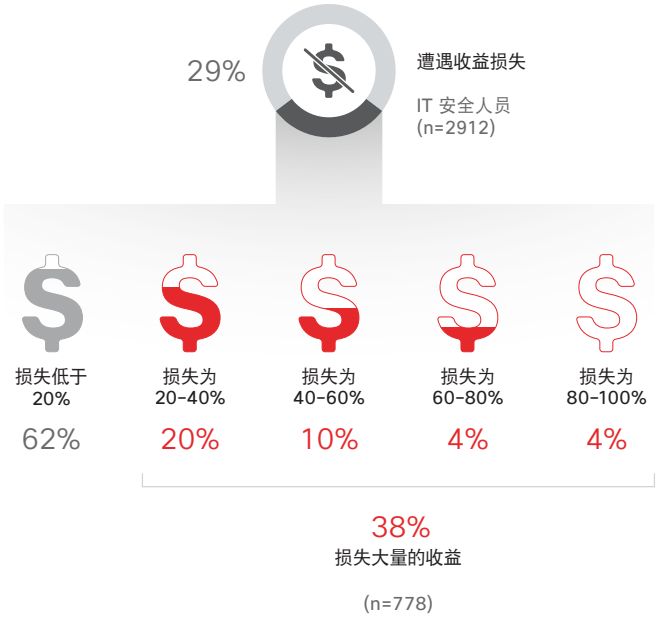
遭受在线攻击的公司的商机损失使人气馁。接受调查的安全专业人员中有 23% 表示，其组织在 2016 年因受到攻击而错失商机（图 56）。在该组中，有 58% 的受访者表示，总计错失的商机低于 20%；有 25% 的受访者表示错失的商机介于 20% 至 40% 之间，9% 的受访表示错失的商机总计达 40% 至 60%。

许多组织可量化他们因公开漏洞而遭受的收入损失。如图 57 所示，29% 的安全专业人员表示，他们的组织因受到攻击而遭受收入损失。在该组中，有 38% 的受访者表示，收入损失达到 20% 或更高。

在线攻击也导致客户减少。如图 58 所示，22% 的组织表示，他们因受到攻击而失去客户。在该组中，有 39% 的受访者表示他们的客户减少 20% 或更多。

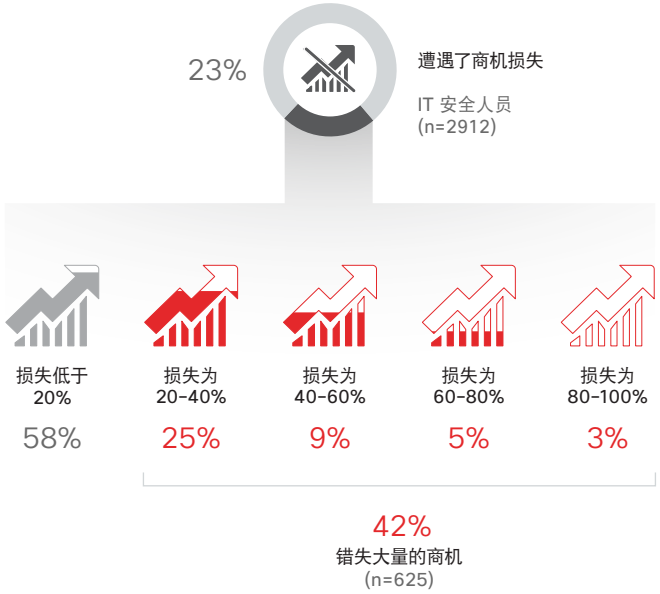
在以下网站下载 2017 年图表：**www.cisco.com/go/acr2017graphics**

图 57 由于受到攻击而导致组织收益损失所占百分比



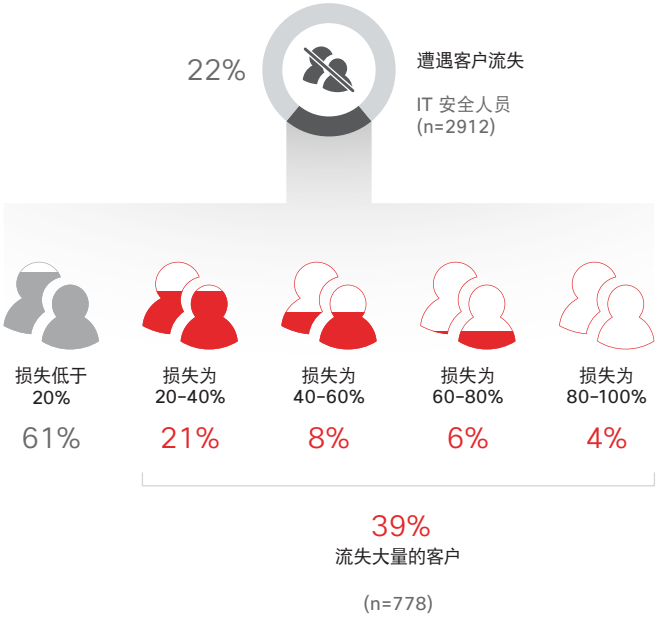
来源：思科 2017 年安全能力基准研究

图 56 由于受到攻击而错失商机所占百分比



来源：思科 2017 年安全能力基准研究

图 58 由于受到攻击而导致公司流失客户所占百分比



来源：思科 2017 年安全能力基准研究

结果：增强监管将有利于改善安全性

正如调查结果所示，漏洞的影响持久且广泛。如果一个人认为组织在某一时刻会受到漏洞影响，那么问题是接下来会发生什么？管理层应将其注意力和资源转移到哪个方面，以便让漏洞不太可能出现？

漏洞出现之后是一个学习的机会，我们不应该浪费这种经验，让我们投资于更好的方法。

多达 90% 的安全专业人员表示，安全漏洞推动了威胁防御技术和流程的改进，如图 59 所示。在受漏洞影响的组织中，有 38% 的组织表示，他们作出的回应是将安全团队从 IT 部门中分离出来；38% 的组织表示他们在增强员工的安全意识培训；37% 的组织表示他们加大了对风险分析和缓解措施的关注。

图 59 安全漏洞如何推动改进

来源：思科 2017 年安全能力基准研究

组织认识到他们必须发挥创造性以超越人才、技术兼容性和预算的限制。一种策略是采用外包服务来加强预算并挖掘外部人才。

在 2016 年，51% 的安全专业人员将顾问与咨询工作外包，而 45% 的人员将事件响应外包（图 60）。52% 的受访者表示他们会外包服务以节约成本，而 48% 的受访者则称其外包服务是为了获得客观的见解。

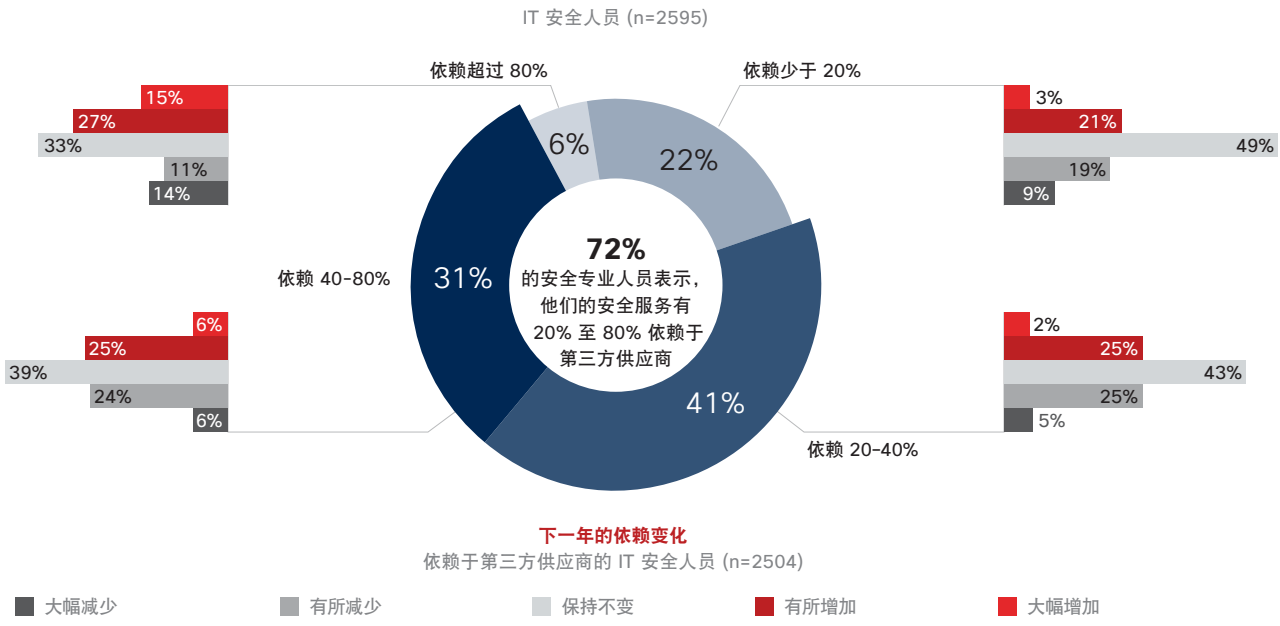
正如他们处理外包工作那样，组织也依靠第三方供应商来增强其防御策略。安全生态系统为他们提供分担安全责任的方法。

72% 的安全专业人员表示，他们的安全服务中有 20% 至 80% 依赖于第三方供应商，如图 61 所示。严重依赖于外部帮助以实现安全的那些组织最有可能在未来增加利用第三方供应商的服务。

图 60 组织对外包的依赖

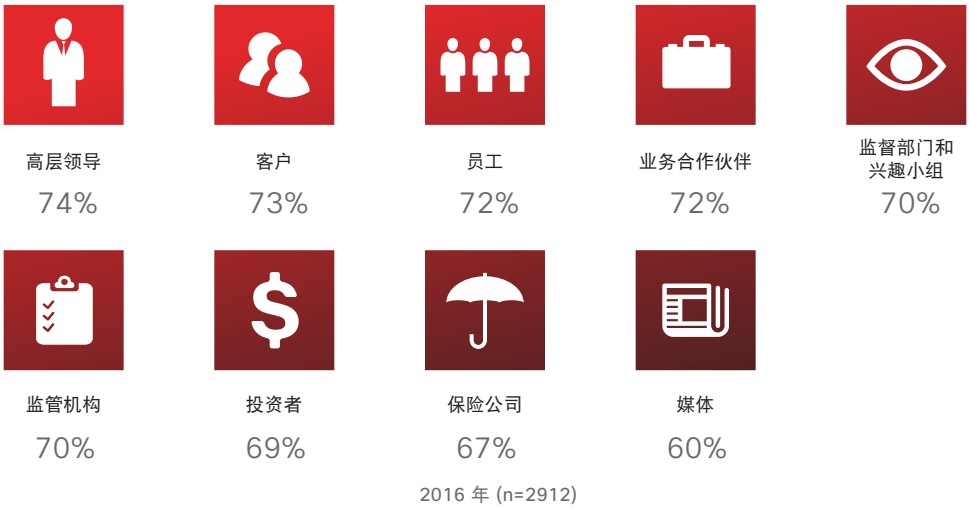
来源：思科 2017 年安全能力基准研究

图 61 组织对外包依赖的百分比



来源：思科 2017 年安全能力基准研究

图 62 加强监管的来源

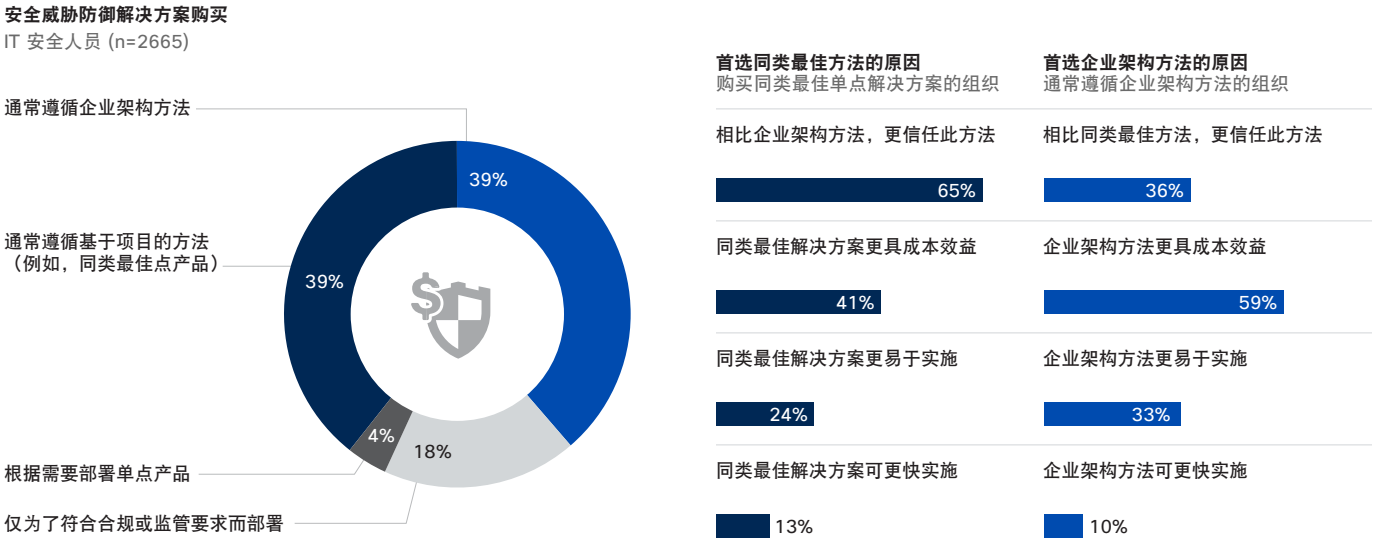


来源：思科 2017 年安全能力基准研究

随着组织采取措施来增强其安全状态，他们预计可将更多注意力集中于他们的工作上。这种监管由有影响力的受众来执行，因此不能被忽视。如何应对这些受众的关注会对组织保卫自己的能力产生重大影响。

74% 的安全专业人员表示，监管由高层领导执行；73% 由客户执行；72% 由员工执行，如图 62 所示。

图 63 如何信任和具成本效益地推动安全决策



来源：思科 2017 年安全能力基准研究

信任与成本：购买安全产品的驱动因素是什么？

安全专业人员想要使用最好的解决方案来保护其组织，但他们对如何打造理想安全环境持不同意见。他们是否因为相信这些解决方案可以解决许多不同的问题而向各种不同的供应商购买同类最佳解决方案？或者因为他们相信集成架构更具成本效益而转向此方法？虽然安全投资有许多驱动因素，但更加简单可惠及每个组织。

如图 63 所示，信任和投入资金选择同类最佳解决方案和集成架构解决方案的安全专业人员似乎各占一半。65% 的受访者表示，他们喜欢同类最佳解决方案，因为相较于企业架构方法，他们更信任此方案。另一方面，59% 的受访者表示他们喜欢架构方法，因为他们认为这会更具成本效益。

这不是进退两难的困境。组织需要同类最佳和集成安全这两种解决方案。两种方法都有各自的优势，并可简化安全，同时提供自动响应工具（图 63）。

通过将同类最佳解决方案与集成方法结合在一起，安全团队可以采取措施以实现复杂程度下降且更有效的安全。集成方法帮助安全专业人员了解在防御的每个阶段发生了什么。这种方法缩小了攻击者的活动空间。它非常简单，使团队能够大规模部署解决方案。它还是开放的，可根据需要结合同类最佳解决方案。并且它是自动化的，可加快检测。

总结：该基准研究揭示了什么

将安全工具集合在一起与实际具备使用这些工具来降低风险以及封闭攻击者活动空间的能力之间存在天壤之别。基准研究的受访者认为自己拥有可抵御攻击者的工具。但他们也承认，缺少人力和产品兼容性不佳等制约因素会导致好工具的效率远远不如预期。

有关漏洞影响的令人深省的发现应为安全专业人员提供改进流程和协议所需的充分证据。组织会面临损失收入和客户等切实直接的影响，不再只是希望消除安全保护方面的差距，因为问题不在于是否会出现安全漏洞，而在于何时出现。

通过基准研究得出的一个信息是，使安全的灵活性和有效性受到限制的制约因素始终和我们在一起：永远不会有安全专业人员认为他们需要的那么多预算和人才。如果我们接受这些限制，则简化安全和部署自动化解决方案的想法变得有意义。

简化安全还利用了同类最佳解决方案和集成架构。组织需要这两个方法带来的好处。

行业

行业

价值链安全：全数字化世界的成功取决于第三方风险的缓解

价值链安全是在互联经济环境中获得成功的基本要素。确保在适当的时间和地点在整个价值链（硬件、软件和服务的端到端生命周期）获得适当的安全是当务之急。

图 64 显示了价值链的八个阶段。

信息技术和运营技术在这个全数字化世界中融合。组织只注重保护其内部业务模式、产品组合和基础设施是不够的。组织必须整体着眼于其价值链并考虑其业务模式中涉及或与其产品组合有关系的每个第三方是否会对其安全招致风险。

简短的回答是他们很可能会招致风险：系统网络安全协会 (SANS Institute) 的研究发现，80% 的数据泄露源于第三方。[15] 为降低风险，组织必须培育一个这样的价值链：让信任不再是一种盲从，且确保安全人人有责。作为实现这一目标的基本步骤，组织应该采取以下行动：

- 识别第三方生态系统中的主要参与者，并了解那些第三方提供什么产品
- 开发一个可以在生态系统中的各个第三方之间分享和部署的灵活安全架构
- 评估这些第三方是否在组织的安全架构设置的耐受度内运行
- 对于在全数字化增长时生态系统可能引入的新安全风险保持警惕

在推出需要涉及或以其他方式影响其第三方生态系统的新业务模式或产品组合之前，组织也必须考虑安全。必须将任何潜在价值和工作效率提高与潜在风险放在一起加以权衡，特别是在数据安全和隐私方面。

对价值链重要性的认知在全球和特定行业都在增长。最近，美国 IT 采购立法规定必须由美国国防部对信息技术和网络安全采购中的开放技术标准进行一年的评估。[16] 在高度集中的能源领域内，北美电力稳定性公司 (NERC) 积极制定应对其网络价值链的新要求。[17]

图 64 价值链的阶段

来源：思科

分享

[15] *应对供应链中的网络风险*，SANS Institute，2015 年：https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252。
[16] 公法 114-92 §
[17] 美国联邦能源管理委员会要求 NERC 承担这项工作，18 CFR 第 40 部分 [文档编号 RM15-14-002；订单号 829]。

组织连同其第三方都需要回答以下这类问题，“数据如何生成以及由谁生成？”、“数据是否应以数字方式挖掘？”进一步明晰需要确定以下这类问题的答案，“谁拥有我们收集或创建的数字资产？”、“我们必须与谁分享该信息？”需要回答的另一个重要问题是：“一旦出现漏洞，由谁承担何种责任和义务？”

这种以价值链为中心的方法有助于确保安全考虑嵌入解决方案生命周期的每个阶段。使用正确的架构，再加上遵守适当的安全标准，将有助于在整个价值链中推动全面安全性（及建立信任）。

地缘政治最新动态：加密、信任以及对透明度的呼吁

在之前的网络安全报告中，思科地缘政治专家审查了互联网治理格局中的不确定性、个体权利与国家权利以及政府和私营企业解决数据保护困境的方法。所有这些讨论中的一个共同主题是加密。我们认为加密将继续发展，也许在可预见的未来，加密在网络安全辩论中甚至可能占主导地位。

国家和地区性数据隐私法律的激增给尝试规避那些法律的供应商和用户带来了担忧。在这个不确定的环境中，数据主权和数据本地化等问题也涌现出来，在企业寻找创造性解决以应对复杂且不断发展的隐私法规时，帮助促进云计算和本地化数据存储的增长。[18]

同时，数据泄露和高级持续性威胁数逐步上升，以及由单一民族国家发起的非法闯入的公开（包括在美国总统选举等备受瞩目事件中进行的那些黑客活动）使得用户对其敏感数据和隐私受到的保护更加缺乏信心。

后斯诺登时代的政府越来越渴望能够控制数字通信以及在需要时访问数据。但是，用户却热切于其对隐私的要求。例如，最近发生了 Apple 和 FBI 之间对于归属于恐怖分子的 iPhone 进行交锋的事件，这并没有消除用户对隐私的担忧。要说有什么不同的话，它向这一代数字用户（尤其是美国的用户）传授了关于端到端加密的知识。许多用户现在要求其技术提供商提供端到端加密，并且他们希望保有加密密钥。

正如我们所知，这预示着网络安全形势发生了根本性转变。组织需要将其环境设计为让他们可以掌握并响应竞争日程的模式。

当发生这种转变时，越来越多的政府为它们自己授予合法权利（通常在更广的层面上），以便绕过或破坏加密或技术保护措施，并且通常是在不通知制造商、通信提供商或用户的情况下进行。这不仅会在当局和技术公司之间，而且会在各个政府之间制造紧张态势，它们并不一定希望公民的数据被第三国家/地区的当局访问。许多政府收集有关它们在供应商软件中发现的零天攻击和漏洞的信息；然而，它们不一定会及时告知供应商或与供应商分享它们所占有的信息。

隐藏此类有价值的信息会妨碍供应商改进其产品的安全性以及为用户提供更好的威胁防护。即使政府可能有充分的理由秘密保留此类情报，但在全球网络安全环境中也需要实现更高的透明度和信任。因此，政府应该对他们有关隐藏零天攻击的现行策略进行坦率的评估。他们应认同，与供应商分享信息可以为每个人带来更加安全的数字环境。

[18] 有关此主题的更多信息，请参阅《华尔街日报》的 Stephen Dockery 于 2016 年 6 月 6 日发表的文章：“Data Localization Takes Off as Regulation Uncertainty Continues”（*随着监管不确定性继续，数据本地化突然成功*）：http://blogs.wsj.com/riskandcompliance/2016/06/06/data-localization-takes-off-as-regulation-uncertainty-continues/。

高速加密：在传输过程中保护数据的可扩展解决方案

正如第 65 页的地缘政治部分所述，在可预见的未来，端到端加密仍是政府和行业之间有着很多争论和恐慌的话题。虽然由于此问题产生了一些紧张感，但用户对于由客户保有密钥的端到端数据加密的需求不断增加。

思科地缘政治专家预计，至少在短期内，有一些数据流和数据池将很可能仍使用供应商管理的密钥来加密，特别是在依靠广告获利的商业模式中。但在其他地方，我们应该期望看到使用客户保有的密钥进行端到端加密，从而获得更大的吸引力，与之相反的是缺少法律授权。

同时，期待组织也在数据传输时寻求对其数据保护方式进行更多控制，特别是从一个数据中心高速移动到另一个数据中心时。由于传统技术的限制和对网络性能的影响，这对企业来说曾是一项艰巨的任务。但是，新方法使此流程变得更轻松。

一种解决方法是应用层安全，通过修改应用来加密数据。部署这种安全会大量占用资源、实现起来很复杂且运行起来代价高昂（具体取决于组织使用多少个应用）。

越来越受欢迎的另一种方法是将加密功能融入网络或云服务以保护传输数据。这是传统网关 VPN 模式的一种发展演进，该解决方案解决了网络的动态性质和数据中心流量的高速传输速率。当来自该环境中的任何应用的数据以高速行进到另一个位置时，企业使用新功能提供的运营和成本效率来保护它们。

但是基于网络的加密只是用于保护数据的一个工具。要确保他们在数据传输过程中或处于静止状态时足以对它们提供保护，组织应整体着眼于挑战。一个很好的入手点就是向技术供应商提出一些基本但重要的问题，例如：

- 当数据在传输时如何保护它？
- 当数据处于静止状态时如何保护它？
- 谁可访问数据？
- 数据存储在何处？
- 删除数据的政策是什么，在何时以及是否必须删除它？

此外，这些问题仅是有关数据保护的更广泛对话的一个起点，应逐渐发展为包括数据恢复能力和可用性等主题的讨论。

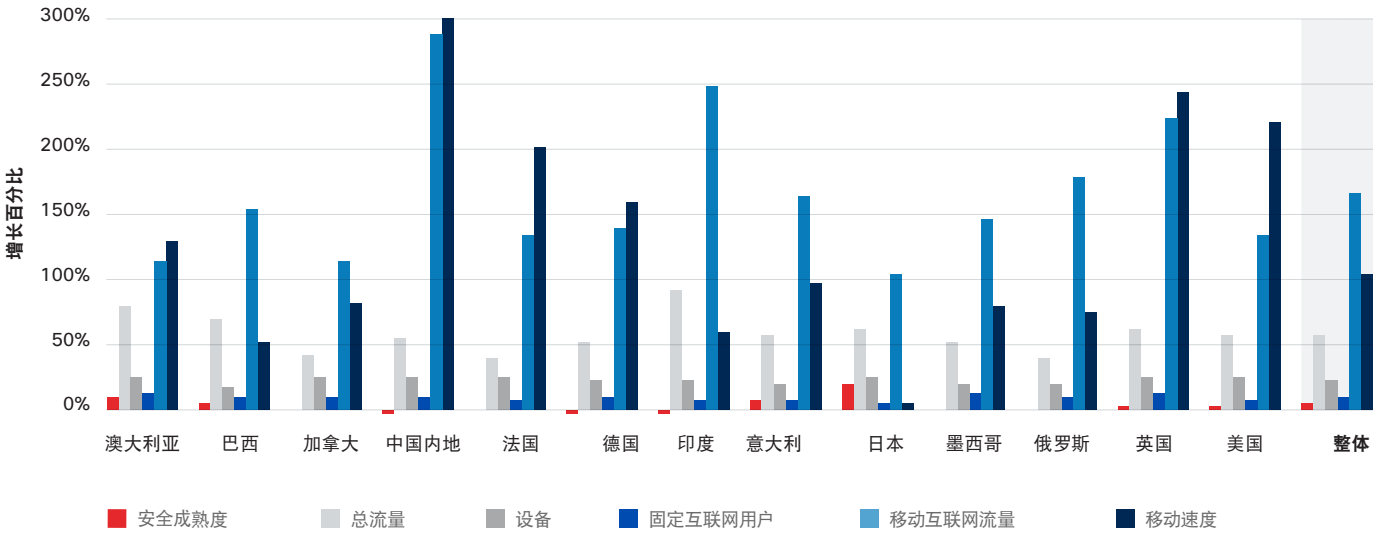
网络性能和采用与安全成熟度：在线速度、流量和准备未同步发展

防御者希望走在其网络攻击者前面。落后于他们很可能会处于危险的境地。令人担忧的是，防御者无法同步改善其安全状态，从而让攻击者能够赢得行动空间和时间。鉴于全球的固定和移动互联网流量保持稳步增长步伐，防御者必须让此增长与其安全基础设施成熟度上的收益相匹配。

思科 VNI 预测指数可以分析每年的全球 IP 流量，包括移动和 Wi-Fi 流量。该预测为 IP 流量、互联网用户数量以及 IP 网络支持的个人设备和机器间 (M2M) 连接数量提供了 5 年的预测。（有关 VNI 预测的更多详情，请访问此处。)例如，该预测估计到 2020 年，智能手机产生的流量占总 IP 流量的 30%。

思科将 VNI 预测与取自思科每年安全能力基准研究的防御者成熟度数据相匹配（参见第 49 页）。在分析 2015、2016 和 2017 年基准报告中的成熟度增长率之后（如图 65 所示），我们发现，与互联网流量增长相比，安全成熟度发展缓慢。中国和德国等一些国家/地区在这段时期内的成熟度实际上略有下降。尤其是宽带速度以比图 65 中所示的其他网络变量明显更高的速率改进和增长。更快的速度和更多连接设备促进更大的流量增长，但组织正在努力支持其安全措施和基础设施以类似的速率增长。

图 65 安全成熟度和增长率



来源：思科安全研究部门、思科 VNI 和思科 2017 年安全能力基准研究

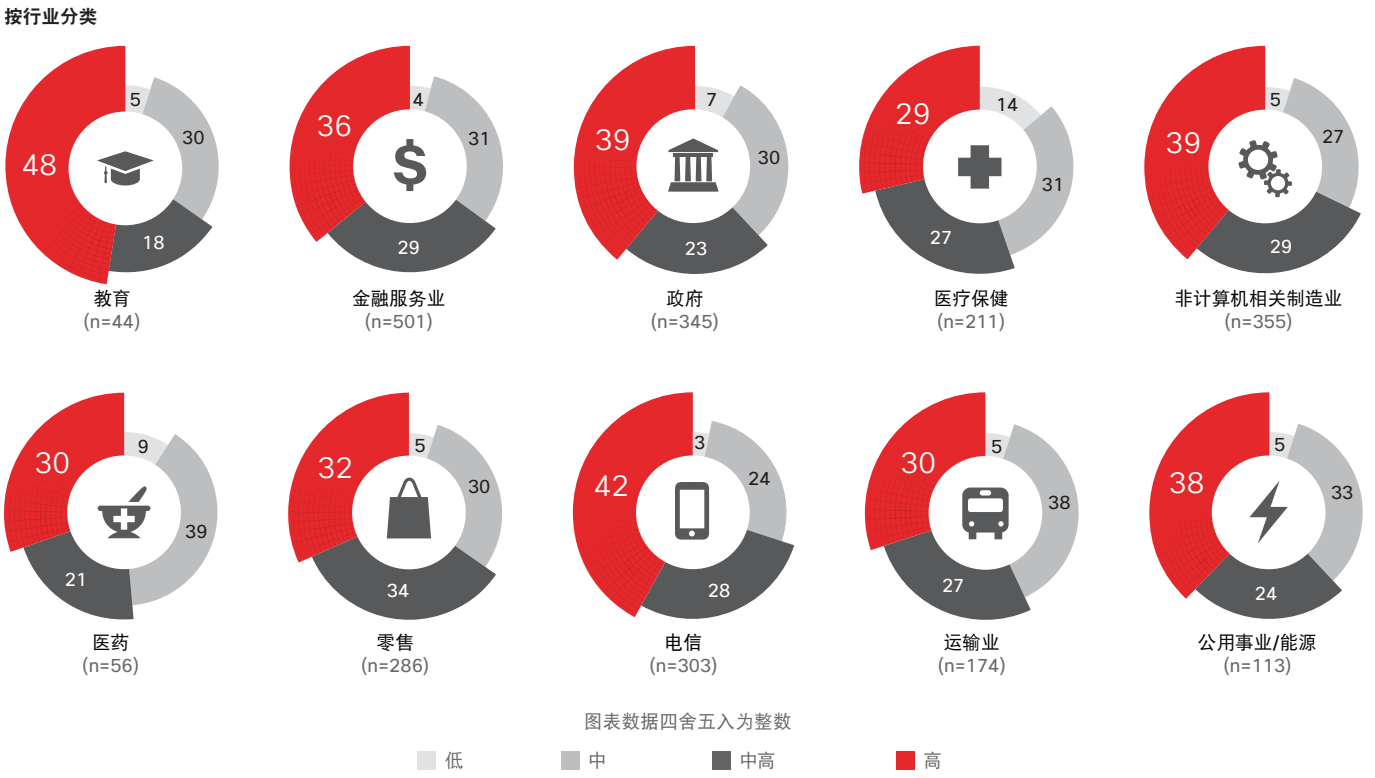
分享

相比于其他行业，一些行业的安全成熟度相对滞后，如图 66 所示。特别是，制药、医疗保健和运输落后于其他产业。

务必注意的是，移动速度的急剧上升是电信提供商广泛采用 4G 和 LTE 网络的成果。在这个十年结束时，随着 5G 网络大规模部署，移动速度预计可比得上固定网络速度。根据目前的移动 VNI 预测，当 5G 得以广泛采用时，全球移动流量很可能在总 IP 流量占据更大的份额。根据 VNI 预测，2015 年全球移动流量占总 IP 流量的 5%；到 2020 年，移动流量预计将占总 IP 流量的 16%。

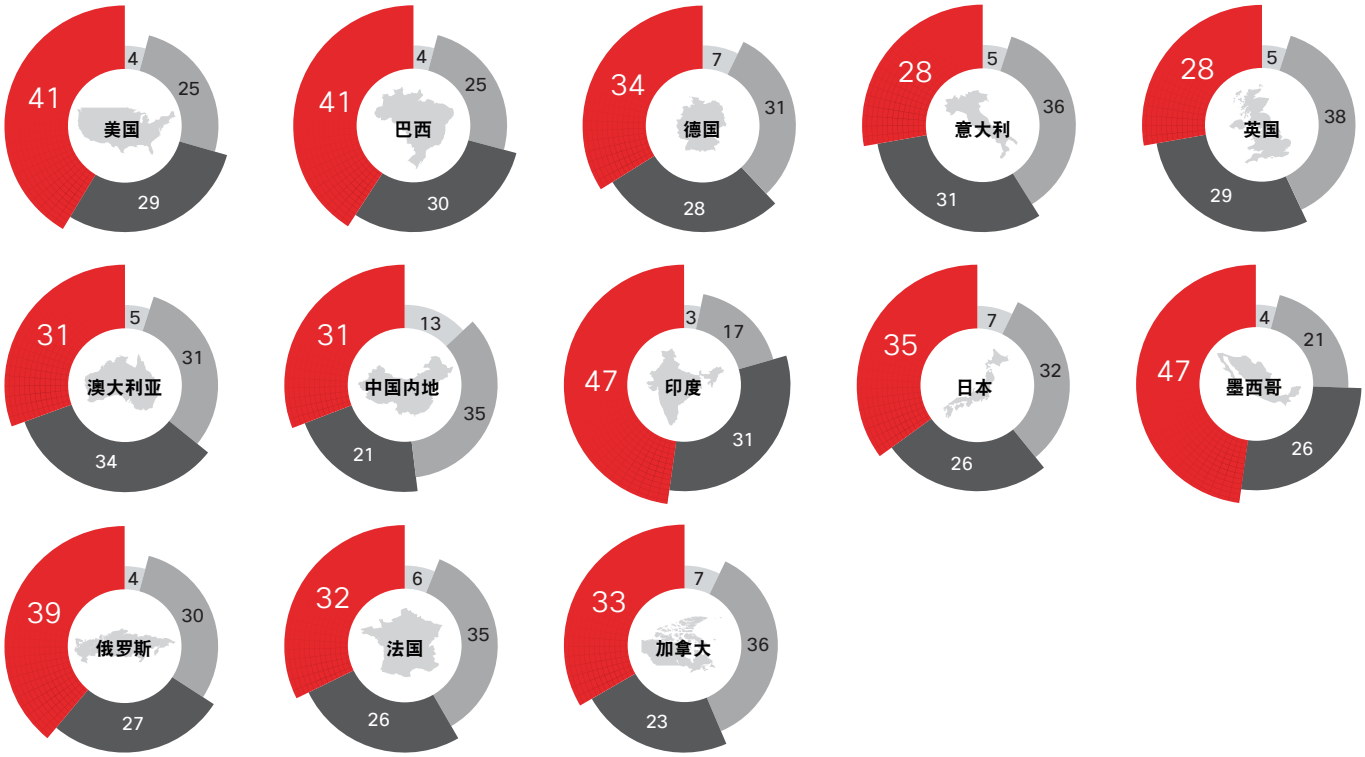
很明显，安全组织必须加强其成熟度工作，而如果需要与互联网流量增长（预示着潜在受攻击面增大）相匹配，则必须加快步伐。此外，组织必须应对不是通过固定或有线方式连接到企业网络的终端设备的使用量增长。他们还必须适应员工更广泛地使用个人设备来访问公司数据。

图 66 垂直行业中的安全成熟度



来源：思科 2017 年安全能力基准研究

图 67 按国家/地区划分的安全成熟度



来源：思科 2017 年安全能力基准研究

速度的提高不是导致互联网流量增长的唯一因素。物联网的出现促使连接到互联网的设备数增加，不仅导致流量增长，而且为攻击者增加了潜在攻击路径。

有关思科 VNI 预测的详细信息，请访问思科网站或阅读思科博文2015 至 2020 年的每年 VNI 预测。

结论

结论

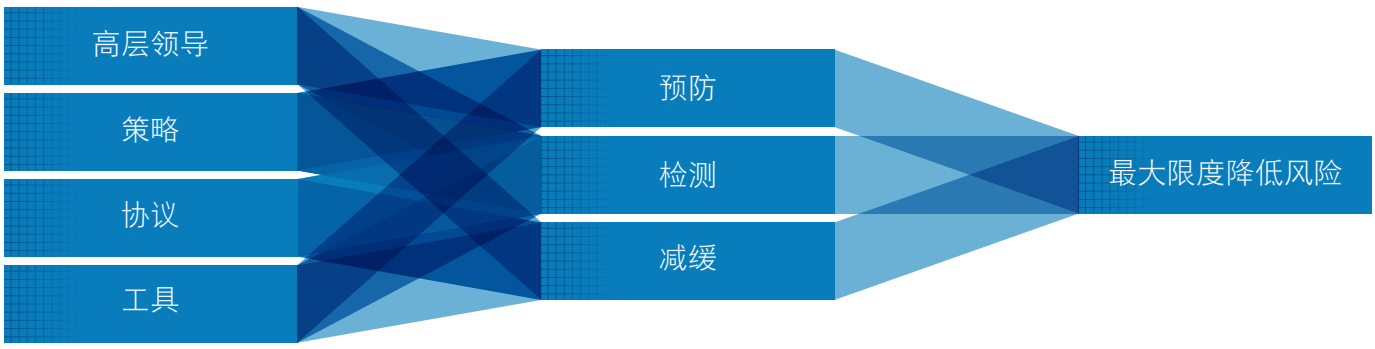
迅速扩大的受攻击面需要一个互联和集成的安全方法

在分析来自安全能力基准研究的数据时（请参阅第 49 页），我们可看到有助于组织最大限度降低风险的模式和决策。因此我们可看到应在哪个方面进行安全投资，从而让风险敞口实现很大的转变。我们通过分析漏洞的时间长度以及系统停机时间的百分比来衡量风险（请参见第 55 页图 53，了解有关漏洞时间长度和受影响系统的信息）。

要了解组织如何有效防御风险，我们需要分析有哪些驱动因素影响其预防、检测和缓解风险的能力。（请参见图 68。）这些驱动因素必须包括以下元素：

- **高层领导：**最高领导层必须将安全视为优先事项。这对减缓和预防攻击来说至关重要。高管团队还应通过明确和既定的指标来评估安全计划的有效性。
- **策略：**策略与规避有密切关系。对网络、系统、应用、功能和数据的访问权限进行控制，会影响其缓解安全漏洞造成的损害的能力。此外，制定政策以确保安全实践的定期审查将有助于预防攻击。
- **协议：**适当的协议有助于预防和检测漏洞，但它们也与缓解措施有密切关系。特别是，定期审查网络上的连接活动以确保安全措施正常起作用是预防和缓解威胁的关键。随着时间的推移定期、正式和战略性地审查与改进安全实践也很有用。
- **工具：**作出正确判断和适当地使用工具与缓解效果有密切关系。拥有工具后，用户可审查并提供对检测、预防和缓解威胁至关重要的反馈。

图 68 为最大限度降低风险而采取的驱动因素和防御措施



来源：思科 2017 年安全能力基准研究

在以下网站下载 2017 年图表：**www.cisco.com/go/acr2017graphics**

组织所使用的安全防御（预防、检测和缓解）可以视为组织最大限度缓解风险能力的影响措施。（请参见图 68。）

这些防御必须包括以下元素：

- **预防：**要使安全漏洞的影响降至最低，员工必须报告安全故障和问题。它对于清楚和很好地理解安全流程和程序也很重要。
- **检测：**使漏洞影响降至最低的最佳检测方法是让组织能够在安全事件全面爆发前检测到安全漏洞。为此，重要的是要有很好的系统，可以对事件相关信息进行分类。
- **缓解：**妥善记录事件响应的流程和程序并跟踪是有效缓解漏洞的关键。组织还需要强大的协议来管理对危机的响应。

所有这些驱动因素和防御是相互联系和相互依赖的。安全专业人员无法仅仅择优挑选几个驱动因素和一两个防御措施，就认为他们已解决安全问题。他们需要每个驱动因素和每个防御。安全团队必须分析它们的弱点所在（例如，领导层提供低水平的支持或缺乏缓解漏洞的工具）并计算必须在哪方面进行安全投资。

主要目标：减少攻击者的行动空间

减少（在理想状况下，消除）攻击者不受限制的行动空间，并且使攻击者的行踪暴露，这必须是防御者的首要任务。现实情况是任何人都无法阻止所有攻击，也无法保护可以和应该保护的一切事物。但如果您将重点放在封闭网络犯罪分子有效和有利可图地完成其活动所必须拥有的行动空间上，则您可以阻止他们在完全避开检测的情况下接触到关键系统和数据。

此报告对攻击者用来入侵和攻击用户和系统的不同方法进行了分类。我们根据攻击通常部署在攻击链中的哪个位置来分类，例如侦测、武器化、传输和安装。本行动旨在说明攻击者在何时、如何以及在何处利用漏洞及其他缺陷以在设备或系统中取得立足点，发动攻击，然后收获他们所寻求的回报。

我们建议防御者调整其安全方法以领先于攻击者的基本流程。例如，要在侦测阶段瓦解攻击者的行动，安全团队应该：

- 收集有关最新威胁和漏洞的信息
- 确保他们可控制对其网络的访问
- 限制组织受攻击面扩大
- 管理配置
- 根据这项工作的信息制定一致的响应措施和程序

在应对武器化威胁时，防御者必须应用其武器库中的每个工具来防止它们传播和恶化。在这个阶段，集成安全架构变得至关重要。它可实时洞察威胁以及执行自动检测和防御，这对改进威胁检测至关重要。

在安装阶段，安全团队在应对和调查危害时必须随时了解环境状态。如果该环境简单、开放而且实现了自动化，且防御者已采取上述前瞻性措施，那么他们可将其资源集中于帮助企业解答各种关键问题，例如：

- 攻击者访问了哪些内容？
- 他们为什么可以访问那些内容？
- 他们去向何处？
- 他们是否仍在我们的网络中活动？

回答这些问题让安全团队不仅能够采取相应的措施来阻止进一步攻击，而且还可向管理层和董事会通报有关可能的风险和必要的披露。然后，企业可以开始相应流程，确保企业具有全面的控制和缓解措施来弥合任何在漏洞攻击期间发现的安全鸿沟，即为攻击者提供获得成功所需行动空间的薄弱环节。

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，这些方案覆盖了最宽广的攻击媒介。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、公共和私人来源及开源社区处取得的遥感勘测数据，来自思科综合安全情报 (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、终端、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。

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《2017 年年度网络安全报告》撰稿人

CloudLock

CloudLock 是思科旗下公司，作为云访问安全代理 (CASB) 解决方案的领先提供商，致力于帮助组织安全地使用云。CloudLock 为软件即服务 (SaaS)、平台即服务 (PaaS) 和基础设施即服务 (IaaS) 环境的用户、数据和应用提供可视性与可控性。CloudLock 通过其数据科学家领导的 CyberLab 和大众安全分析提供切实可行的网络安全情报。有关更多信息，请访问 https://www.cloudlock.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开发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。

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。

认知威胁分析

思科认知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。认知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。

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 安全情报服务，其支持多种思科产品和服务。

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。

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 提供各种新服务（例如，思科定制威胁情报 (CTI) 服务），从而识别现有安全基础设施未检出或未缓解的感染指标。

思科可视化网络指数 (VNI)

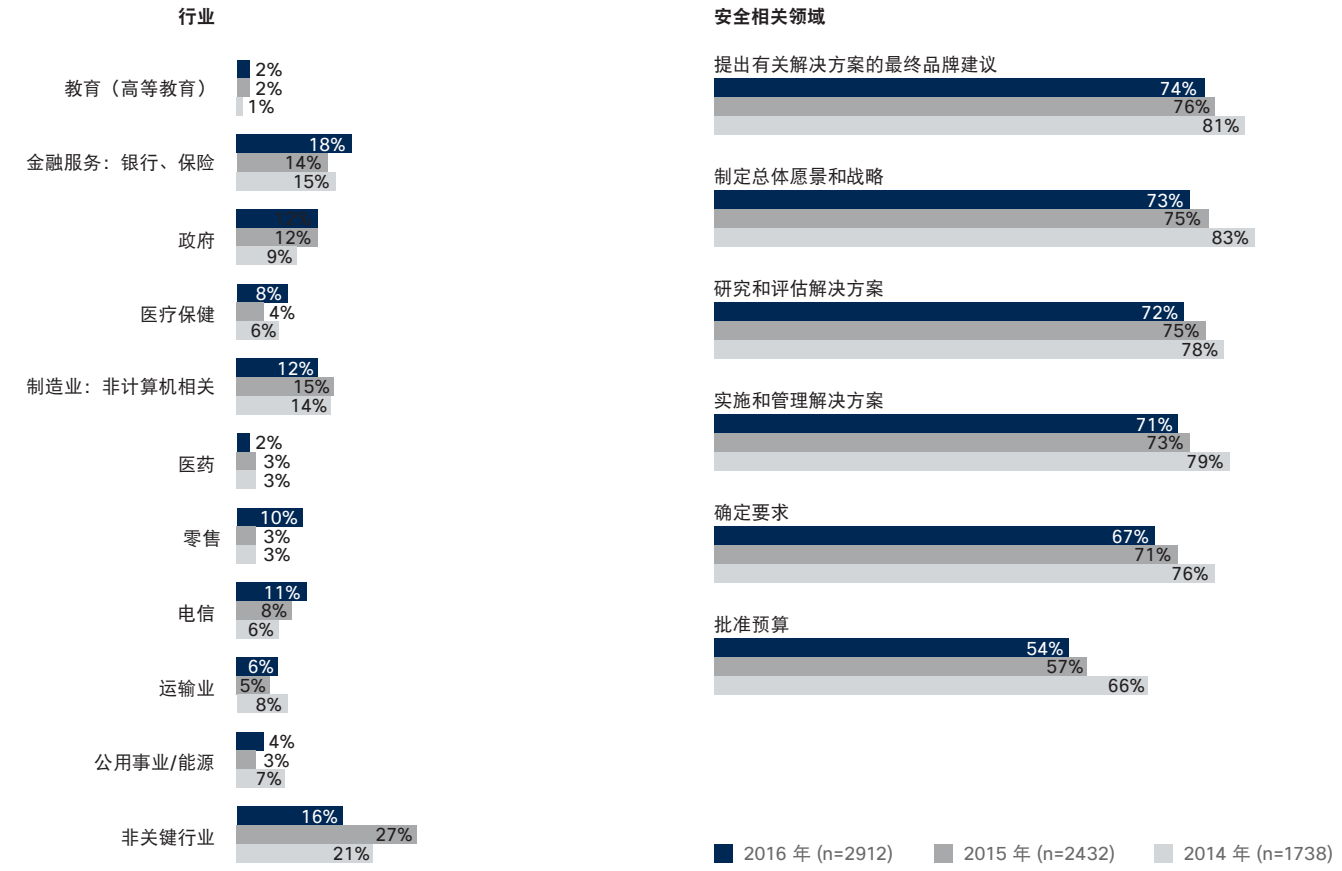
2015 年至 2020 年的思科 VNI 全球 IP 流量预测依赖于独立分析预测和实际网络使用数据。在此基础上，思科针对全球 IP 流量和服务采用情况进行了分层预测。具体方法在完整版报告中有详细的说明。经过 11 年的发展，思科 VNI 研究已成为公认的互联网发展风向标。国家政府、网络监管机构、学术研究人员、电信公司、技术专家，以及行业和商业媒体和分析师都将此年度研究的结果作为数字化发展规划的基础。

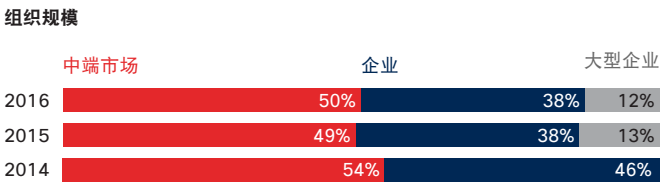
附录

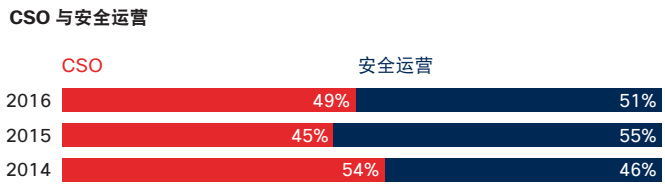
附录

思科 2017 年安全能力基准研究

图 69 调查功能基准研究







来源：思科 2017 年安全能力基准研究

图 70 专职安全专业人员的数量

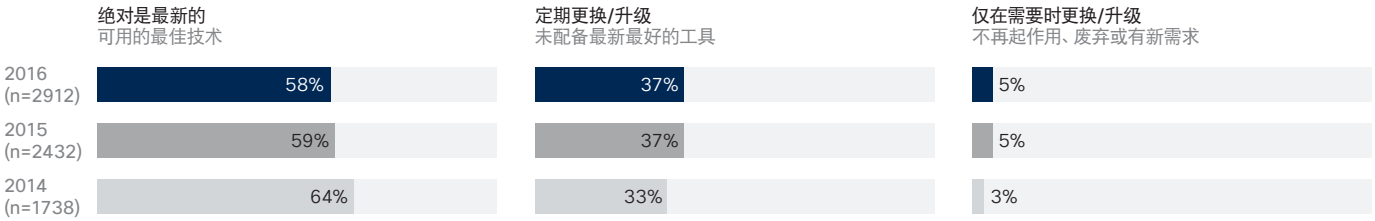
	2014 年 (n=1738)	2015 年 (n=2432)	2016 年 (n=2912)
1-9	18%	17%	15%
10-19	16%	18%	17%
20-29	12%	17%	13%
30-39	8%	9%	8%
40-49	4%	4%	6%
50-99	19%	16%	19%
100-199	9%	9%	9%
200 个或更多	15%	10%	12%
专职安全专业人员的平均人数	**30**	**25**	**33**

来源：思科 2017 年安全能力基准研究

认知

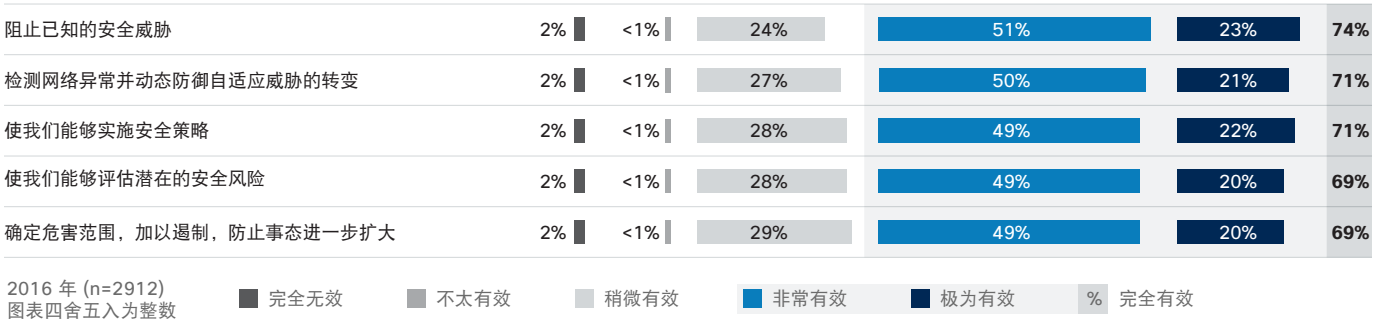
图 71 大多数安全专业人员认为其安全基础设施是最新的

您如何描述您的安全基础设施?



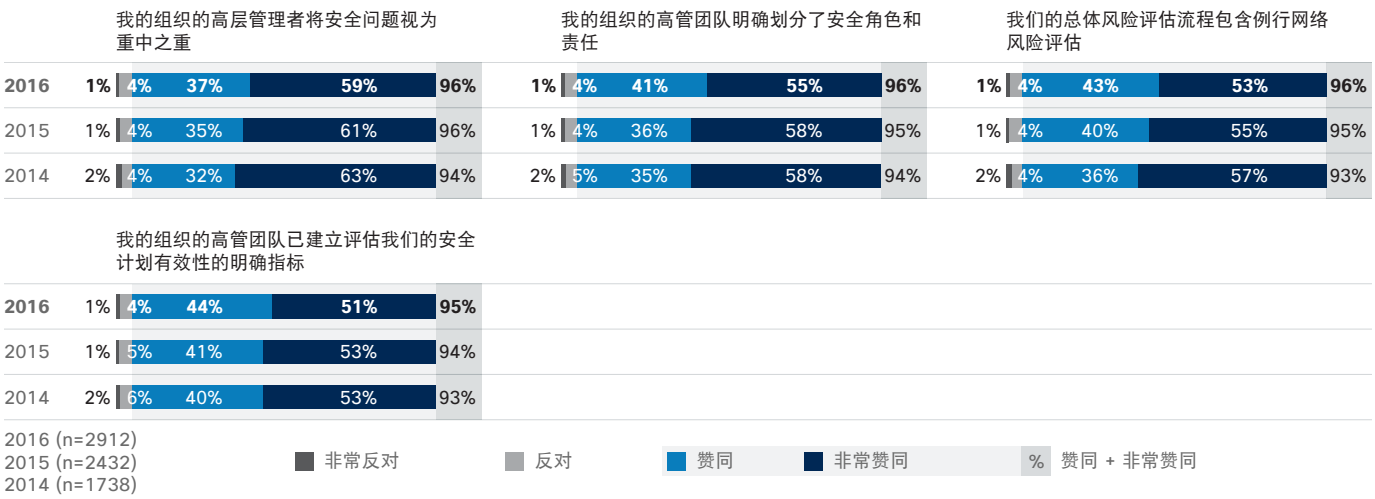
来源：思科 2017 年安全能力基准研究

图 72 认为各种安全工具极其有效的安全专业人员的百分比



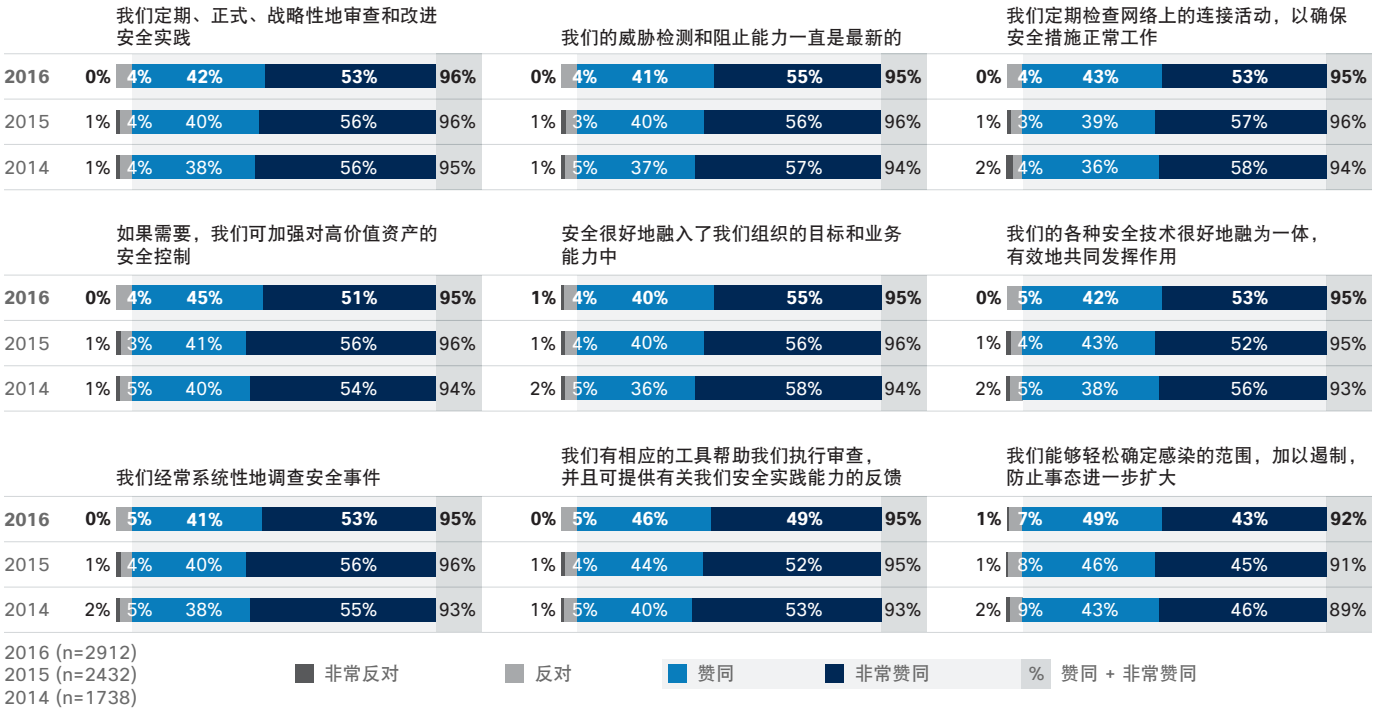
来源：思科 2017 年安全能力基准研究

图 73 认为安全是管理层的优先考虑事项的安全专业人员的百分比



来源：思科 2017 年安全能力基准研究

图 74 强烈赞同将安全融入运营的论述的受访者百分比



来源：思科 2017 年安全能力基准研究

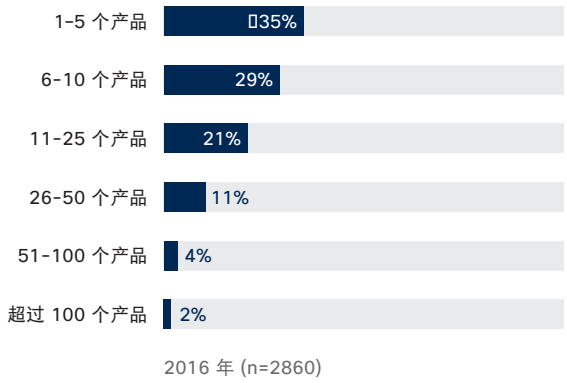
限制

图 75 安全面对的最大障碍

	2015 年 (n=2432)	2016 年 (n=2912)
预算限制	39%	35%
兼容性问题	32%	28%
认证要求	25%	25%
缺少经过培训的人员	22%	25%
优先事项冲突	24%	24%
当前工作负载太繁重	24%	23%
缺乏知识	23%	22%
在经过检验之前不愿购买	22%	22%
组织文化/态度	23%	22%
组织对于攻击者不属于高价值目标	不适用	18%
安全不是管理层的优先考虑事项	不适用	17%

来源：思科 2017 年安全能力基准研究

图 76 组织所用的安全供应商和产品的数量



来源：思科 2017 年安全能力基准研究

图 77 按组织规模划分的所用安全供应商数量

您的安全环境中有多少个不同的安全供应商（即品牌、制造商）？	中型企业 250 - 1000 名员工	企业 1000 - 10000 名员工	大企业 10000 名以上员工
1-5	46.9%	43.4%	39.9%
6-10	28.4%	30.9%	21.3%
11-20	17.6%	15.8%	23.1%
21-50	5.6%	7.1%	8.7%
50 多个	1.4%	2.8%	6.9%
组织总数	**1435**	**1082**	**333**

来源：思科 2017 年安全能力基准研究

图 78 按组织规模划分的所用安全产品数量

您的安全环境中有多少个不同安全产品?	中型企业 250 - 1000 名员工	企业 1000 - 10000 名员工	大企业 10000 名以上员工
1-5	37.9%	32.7%	25.1%
6-10	29.0%	30.1%	22.5%
11-25	19.8%	20.4%	23.7%
26-50	9.6%	10.5%	15.6%
51-100	3.0%	4.3%	7.8%
100 多个	0.8%	1.9%	5.4%
组织总数	**1442**	**1084**	**334**

来源：思科 2017 年安全能力基准研究

图 79 来自 IT 预算中的安全预算年同比下降

安全预算是否包含在 IT 预算内？（IT 部门成员）	2014 年 (n=1673)	2015 年 (n=2374)	2016 年 (n=2828)
完全包含在 IT 中	61%	58%	55%
部分包含在 IT 中	33%	33%	36%
完全独立	6%	9%	9%

来源：思科 2017 年安全能力基准研究

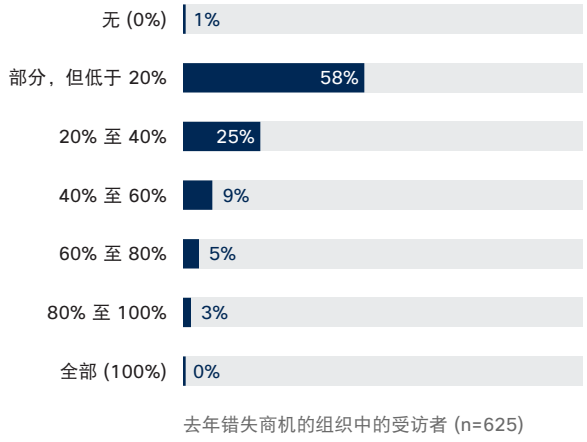
图 80 安全花费在 IT 预算中所占比例年同比下降

安全职能支出占 IT 预算的百分比	2014 年 (n=1673)	2015 年 (n=2374)	2016 年 (n=2828)
0%	7%	9%	10%
1-5%	4%	3%	4%
6-10%	12%	11%	16%
11-15%	23%	23%	27%
16-25%	29%	31%	26%
26%-50%	21%	19%	15%
51% 或以上	5%	4%	2%

来源：思科 2017 年安全能力基准研究

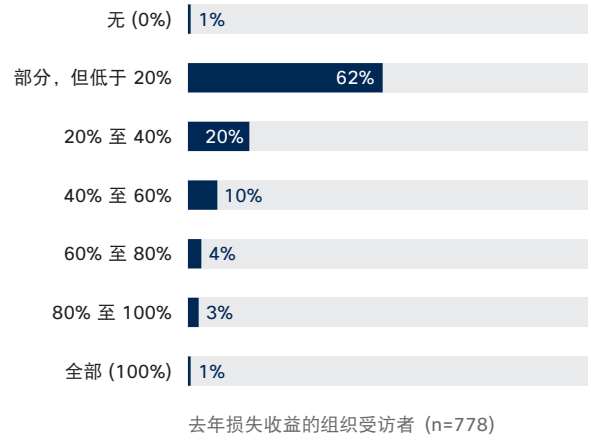
影响

图 81 由于受到攻击而导致组织错失商机所占百分比



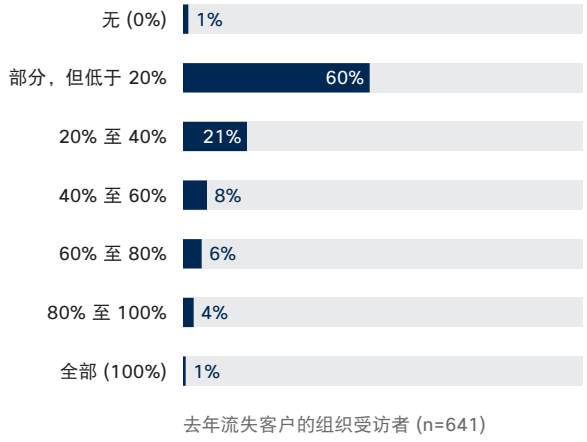
来源：思科 2017 年安全能力基准研究

图 82 由于受到攻击而导致组织损失收益所占百分比



来源：思科 2017 年安全能力基准研究

图 83 由于受到攻击而导致组织流失客户所占百分比



来源：思科 2017 年安全能力基准研究

成果

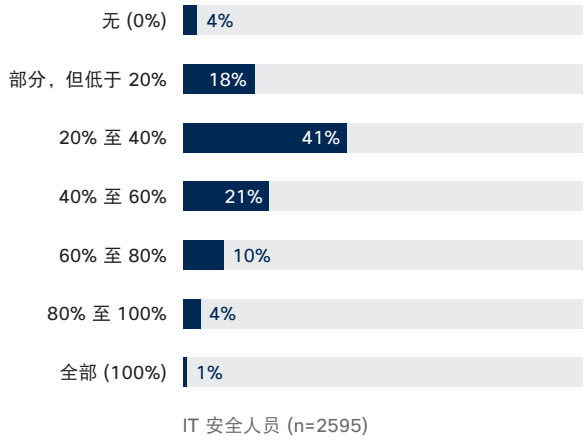
图 84 组织对外包依赖的百分比

哪些安全服务是外包的?	2014 年 (n=1738)	2015 年 (n=2432)	2016 年 (n=2912)
建议与咨询	51%	52%	51%
审核	41%	47%	46%
事件响应	35%	42%	45%
监控	42%	44%	45%
威胁情报	不适用	39%	41%
补救	34%	36%	35%
无/所有内部	21%	12%	10%

为什么外包这些服务?	2015 年 (n=2129)	2016 年 (n=2631)
更具成本效益	53%	52%
需要获得客观公正的见解	49%	48%
更及时的事件响应	46%	46%
缺乏内部专业知识	31%	33%
缺乏内部资源	31%	33%

来源：思科 2017 年安全能力基准研究

图 85 组织的安全依赖于第三方供应商所占百分比



来源：思科 2017 年安全能力基准研究

图 86 按组织规模划分的外包安全服务百分比

哪些安全服务是外包的?	中端市场 (n=1459)	企业 (n=1102)	大型企业 (n=351)
建议与咨询	50%	52%	51%
审核	44%	47%	50%
监控	46%	43%	44%
威胁情报	41%	41%	40%
事件响应	48%	44%	39%
补救	35%	34%	37%
无/所有内部	8%	11%	11%

来源：思科 2017 年安全能力基准研究

图 87 加强监管的来源

高层领导	2%	4%	20%	44%	30%	74%
客户	2%	4%	21%	41%	32%	73%
员工	2%	5%	22%	44%	28%	72%
业务合作伙伴	2%	5%	22%	43%	29%	72%
监督部门和兴趣小组	2%	5%	23%	44%	26%	70%
监管机构	2%	4%	24%	43%	27%	70%
投资者	3%	5%	23%	41%	28%	69%
保险公司	3%	5%	25%	41%	26%	67%
媒体	4%	8%	28%	39%	21%	60%

2016 年 (n=2912)
图表四舍五入为整数

完全没有审查 | 不是经常审查 | 稍微审查 | 经常审查 | 几乎全部审查 | % 完全审查

来源：思科 2017 年安全能力基准研究

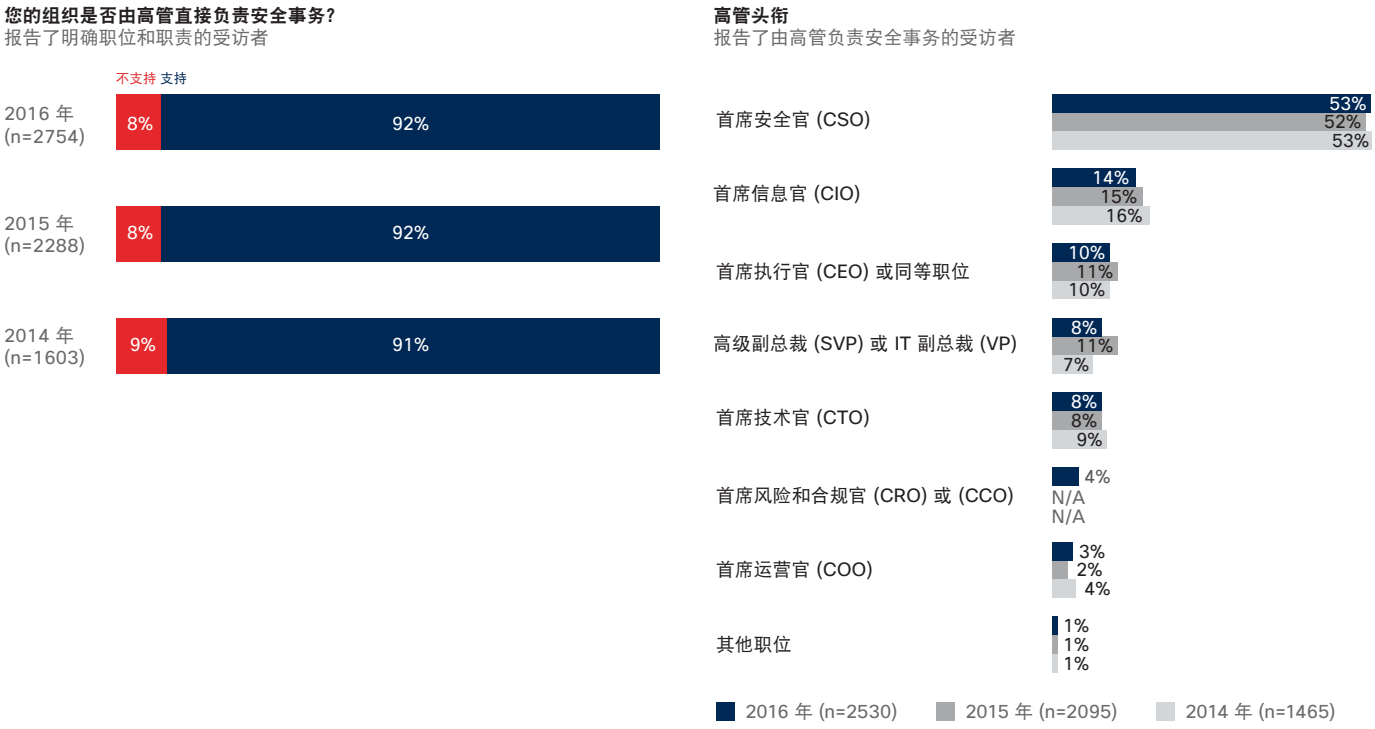
图 88 外部部署私有云和由第三方管理的内部部署托管的增长

网络托管位置	2014 年 (n=1727)	2015 年 (n=2417)	2016 年 (n=2887)
作为私有云的一部分内部部署	50%	51%	50%
内部部署	54%	48%	46%
内部部署但由外部第三方管理	23%	24%	27%
私有云外部部署	18%	20%	25%
公共云外部部署	8%	10%	9%

来源：思科 2017 年安全能力基准研究

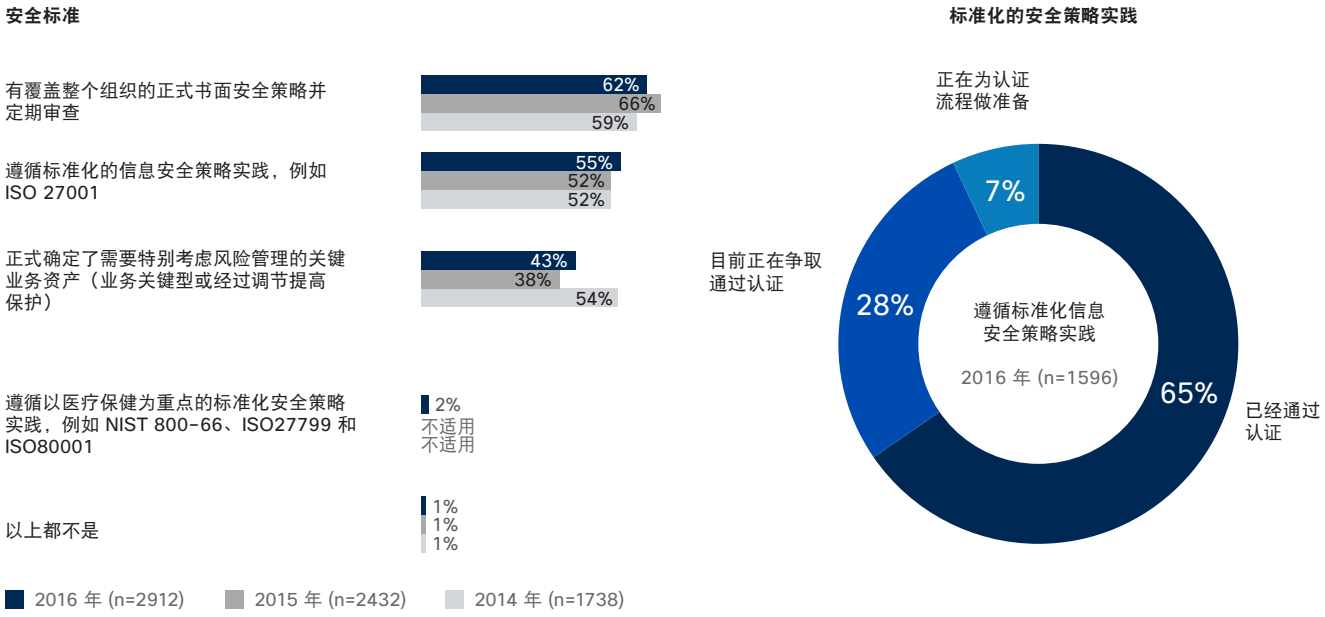
运营、策略、程序和功能

图 89 拥有安全高管的公司所占比例



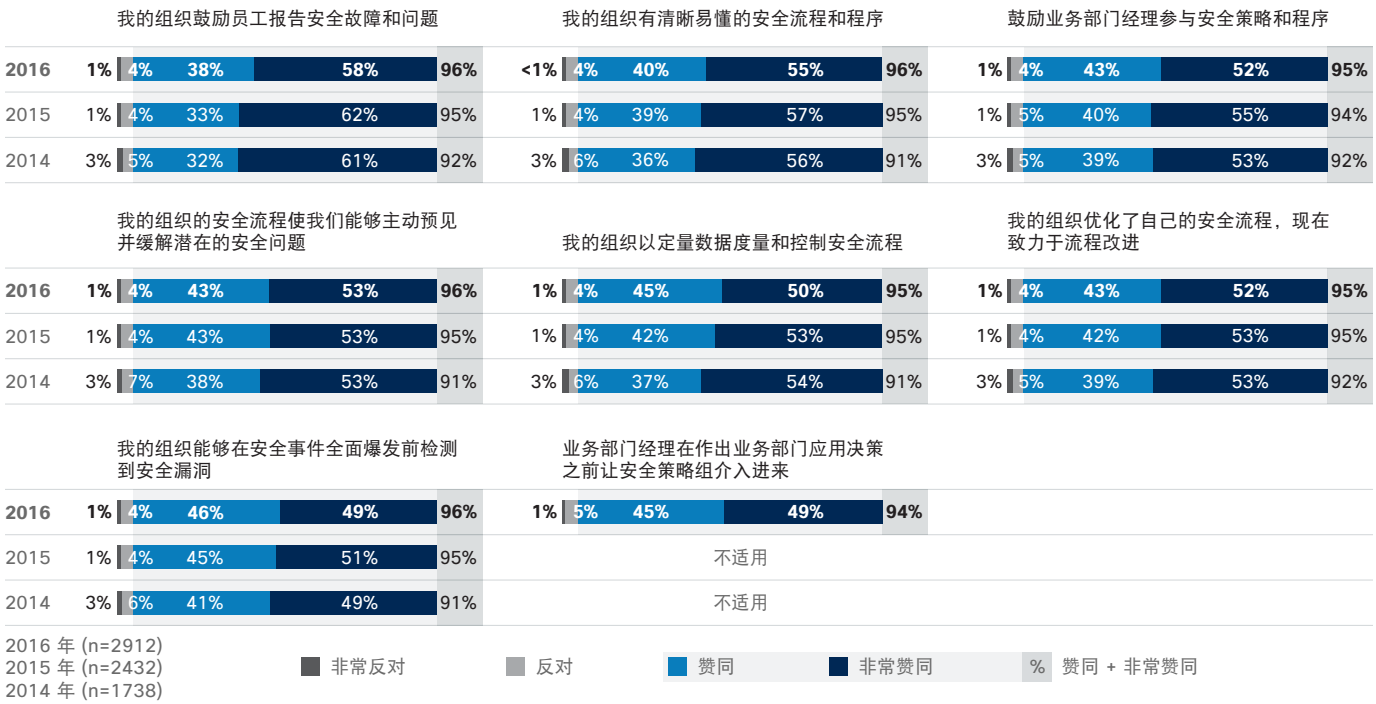
来源：思科 2017 年安全能力基准研究

图 90 有覆盖整个组织的正式安全战略且遵循标准化安全政策实践的公司所占百分比



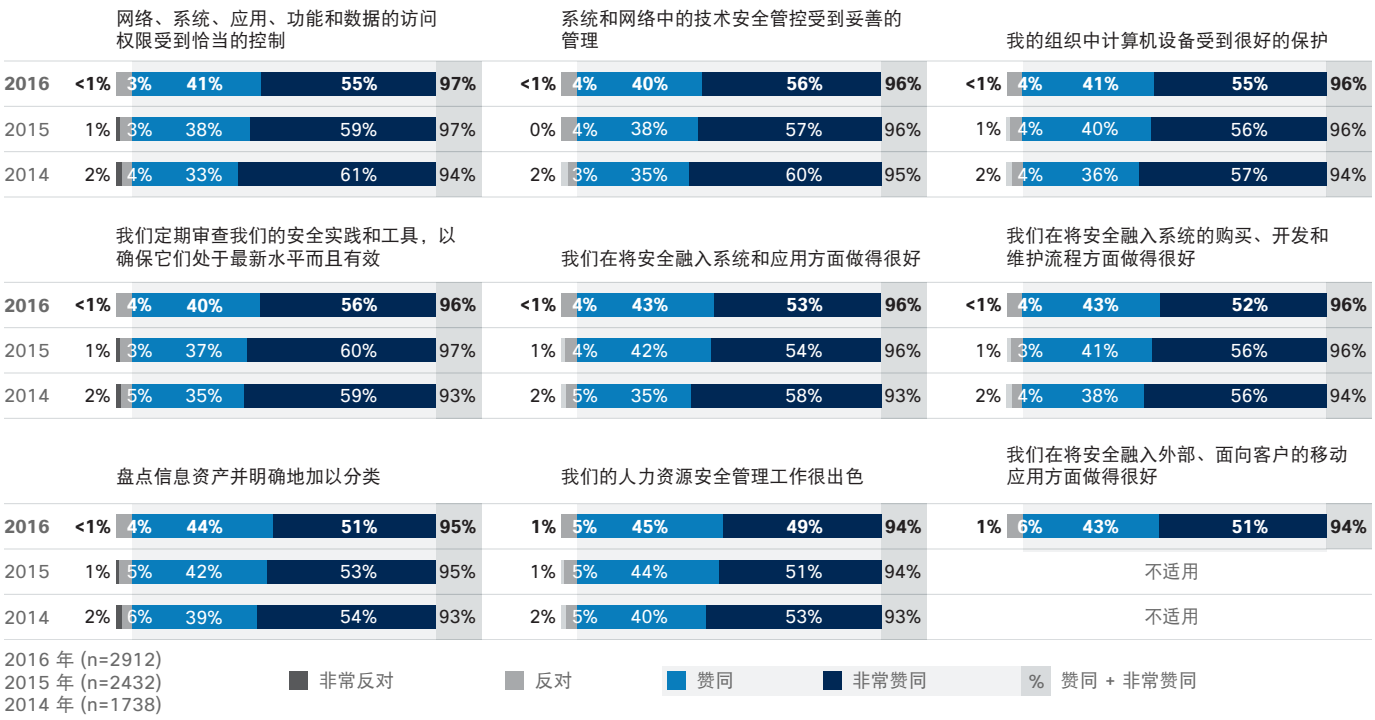
来源：思科 2017 年安全能力基准研究

图 91 强烈赞同安全流程声明的受访者百分比



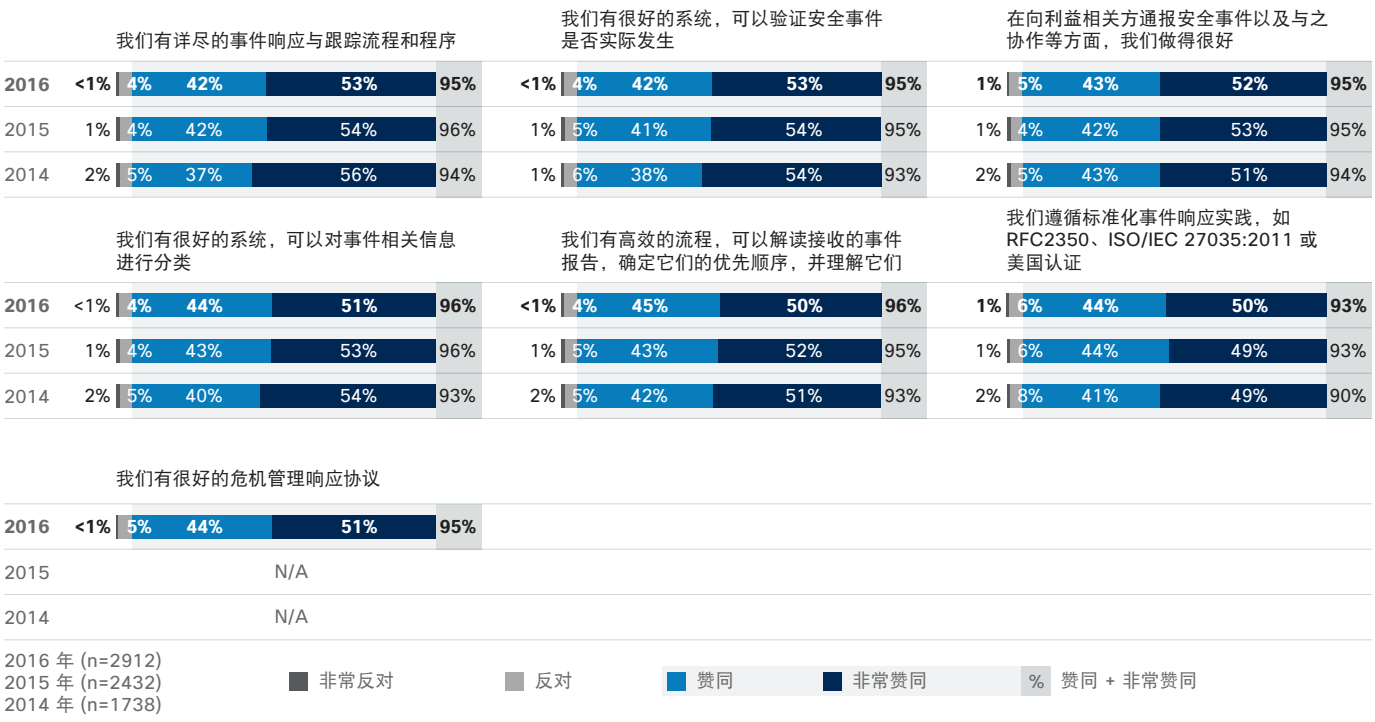
来源：思科 2017 年安全能力基准研究

图 92 强烈赞同安全流程声明的受访者百分比



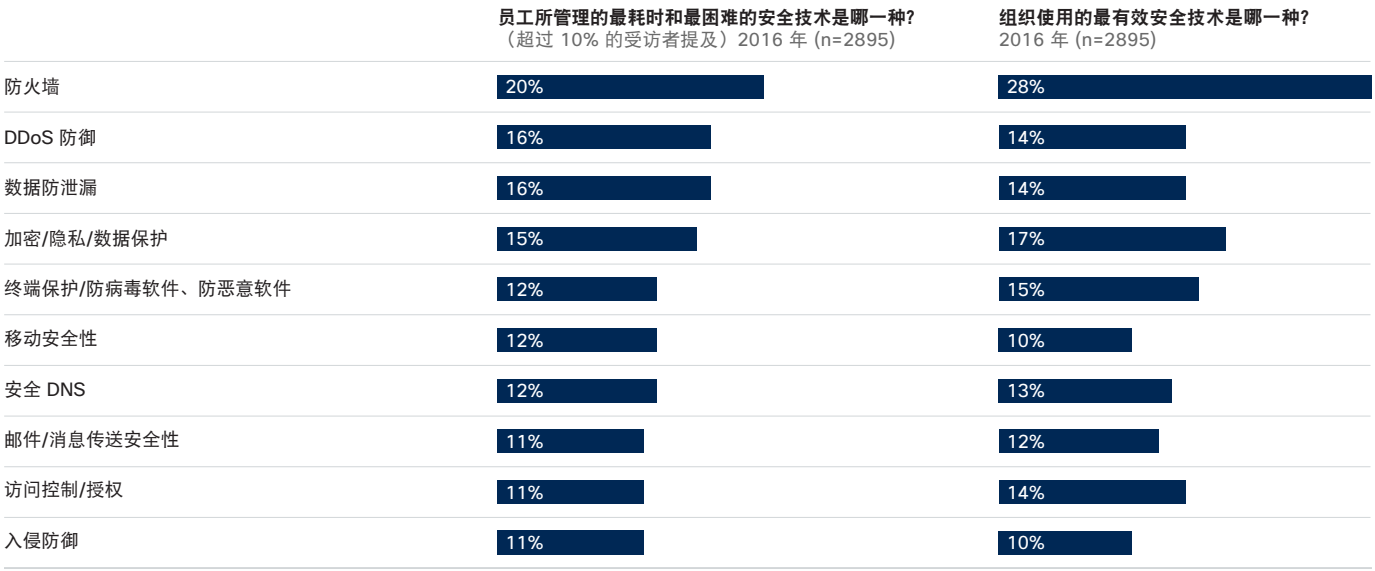
来源：思科 2017 年安全能力基准研究

图 93 强烈赞同安全控制声明的受访者百分比



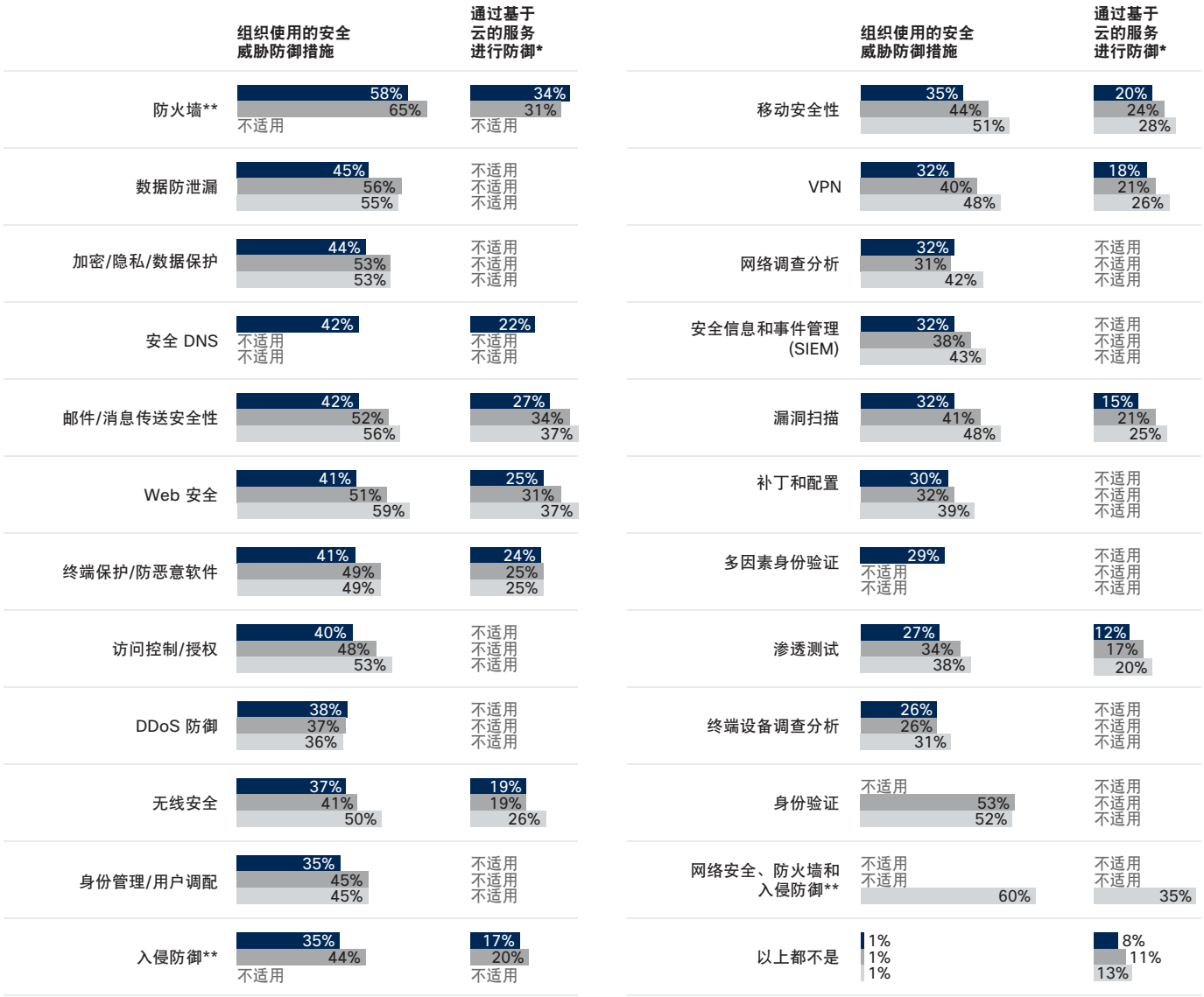
来源：思科 2017 年安全能力基准研究

图 94 安全技术的管理和效力



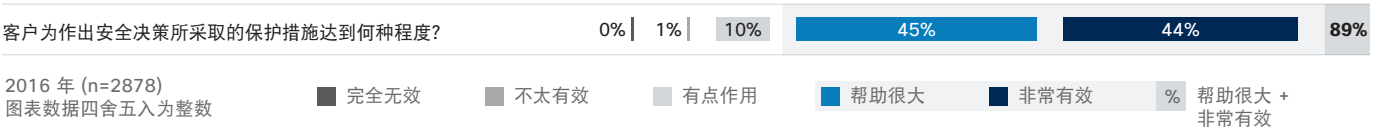
来源：思科 2017 年安全能力基准研究

图 95 安全威胁防御措施的年同比使用情况



来源：思科 2017 年安全能力基准研究

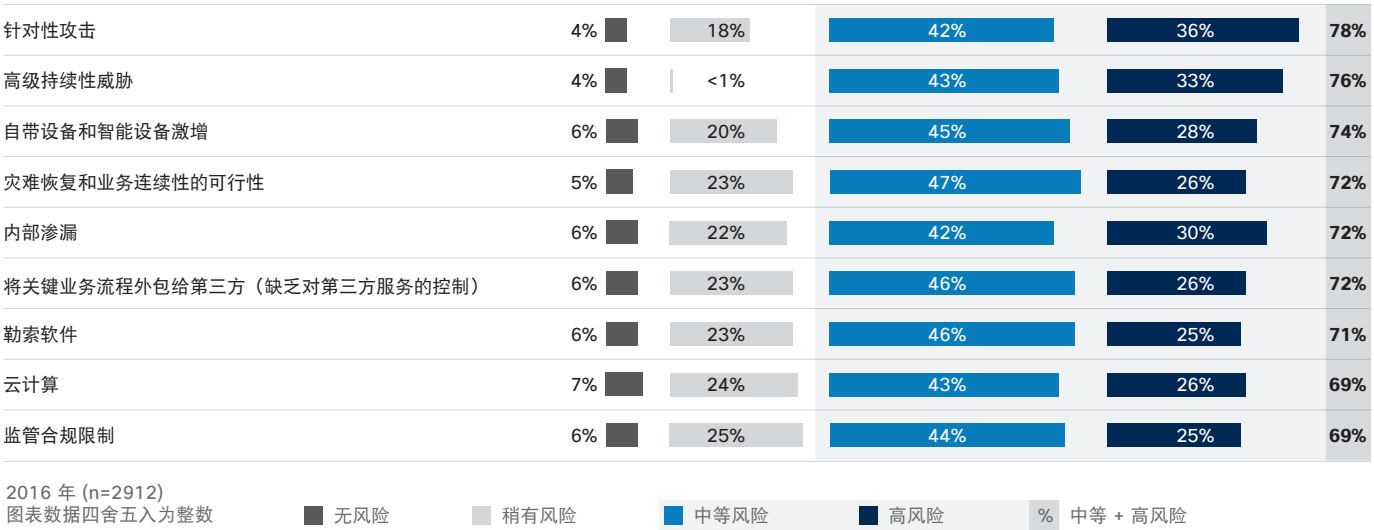
图 96 客户为作出安全决策所采取的保护措施达到的程度



来源：思科 2017 年安全能力基准研究

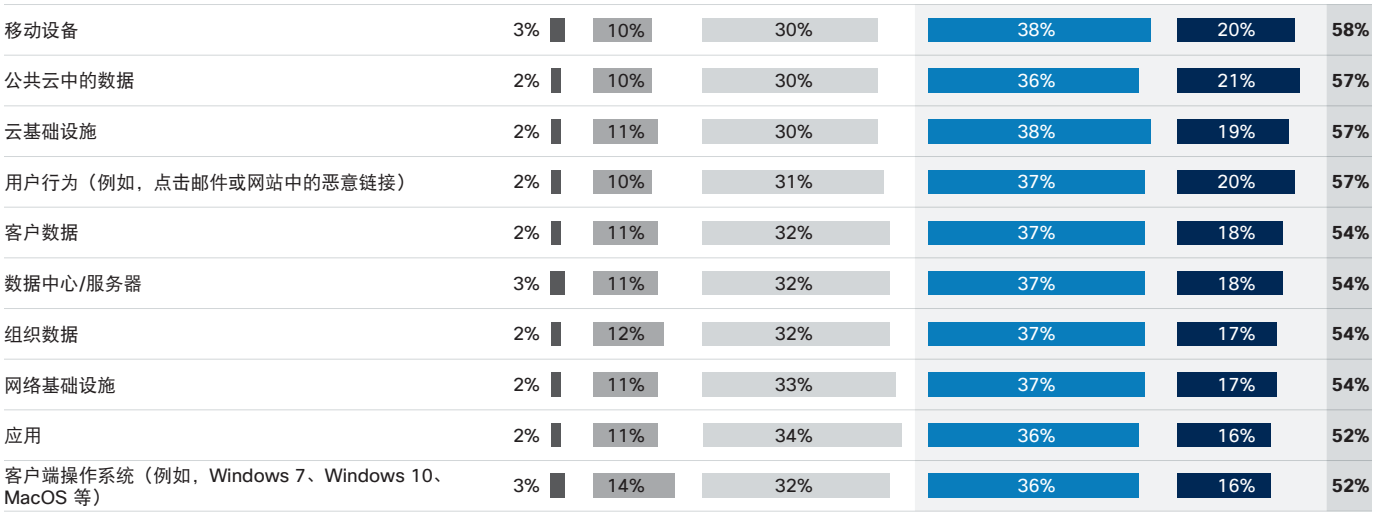
风险和漏洞

图 97 IT 安全人员与网络攻击相关的最大担忧来源



来源：思科 2017 年安全能力基准研究

图 98 安全专业人员与网络攻击相关的最大担忧来源



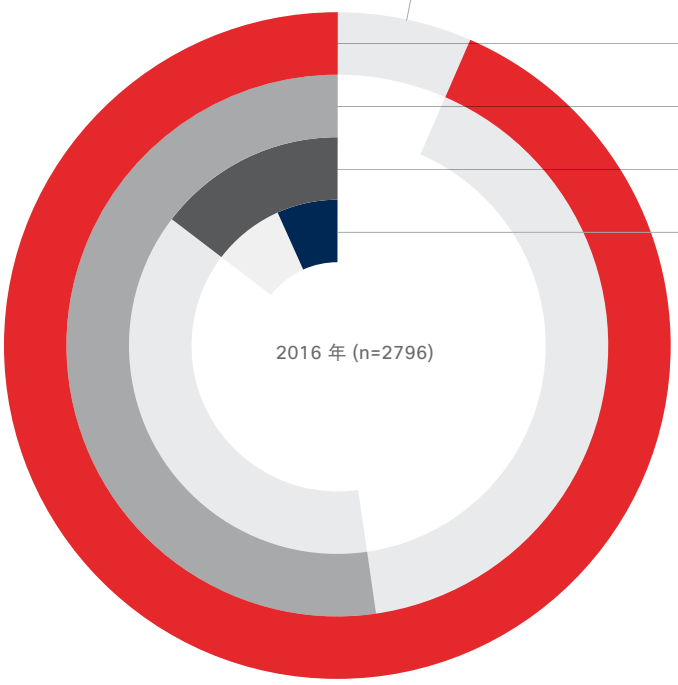
来源：思科 2017 年安全能力基准研究

图 99 安全团队的工作分布

来源：思科 2017 年安全能力基准研究

事件响应

图 100 经过调查或修复的安全警报的百分比



7% 未遇到过安全警报

93% 遇到过安全警报

56% 在已发现的警报中，有 56% 会得到调查

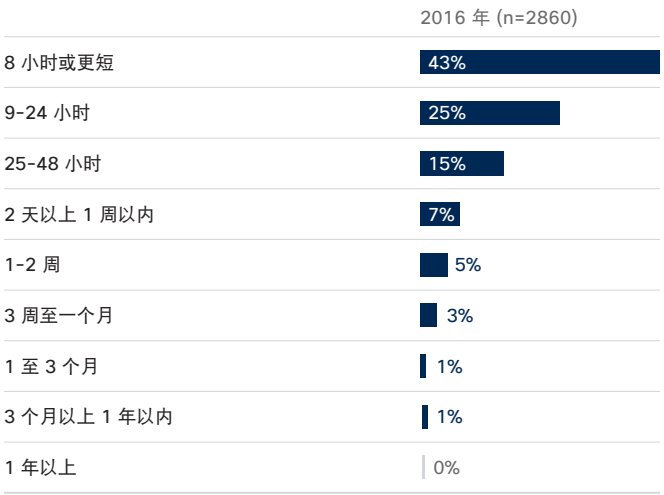
28% 的已调查警报是真实警报

46% 的真实警报得以修复

组织每天看到的平均警报数	
少于 5000	50%
5000 – 10,000	15%
10,000 – 50,000	11%
50,000 – 100,000	8%
100,000 – 150,000	6%
超过 150,000	4%

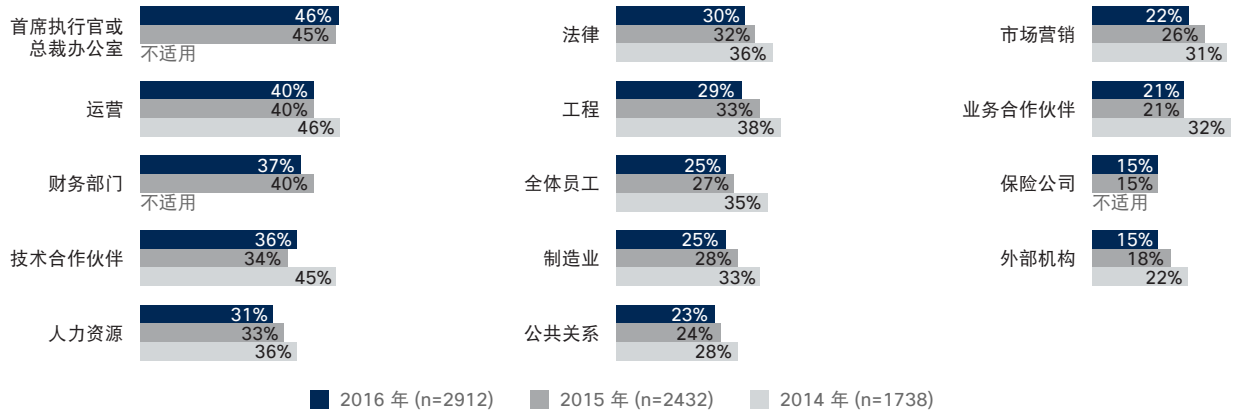
来源：思科 2017 年安全能力基准研究

图 101 检测安全漏洞的平均时间



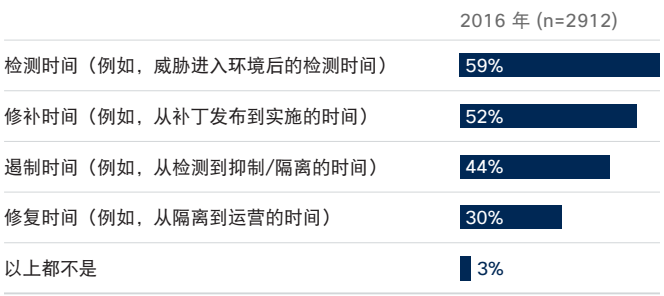
来源：思科 2017 年安全能力基准研究

图 102 发生事件时通知的群体



来源：思科 2017 年安全能力基准研究

图 103 组织用于评估安全性能的 KPI



来源：思科 2017 年安全能力基准研究

图 104 用于分析已被入侵系统的流程的年同比使用情况

被入侵系统的分析流程	2014 年 (n=1738)	2015 年 (n=2432)	2016 年 (n=2912)
防火墙日志	61%	57%	56%
系统日志分析	59%	53%	50%
网络流量分析	53%	49%	49%
恶意软件或文件回归分析	55%	48%	47%
注册表分析	50%	47%	43%
完整数据包捕获分析	47%	38%	40%
IOC 检测	38%	35%	38%
磁盘调查分析	40%	36%	36%
关联事件/日志分析	42%	37%	35%
内存调查分析	41%	34%	34%
外部事件响应/分析团队	37%	33%	34%
以上都不是	2%	1%	1%

来源：思科 2017 年安全能力基准研究

图 105 用于消除安全事件根本原因的流程的年同比使用情况

安全事件成因消除流程	2014 年 (n=1738)	2015 年 (n=2432)	2016 年 (n=2912)
隔离或删除恶意应用	58%	55%	52%
根本原因分析	55%	55%	51%
阻止恶意软件传播	53%	53%	48%
其他监控	52%	48%	48%
策略更新	51%	47%	45%
阻止受感染应用的传播	48%	47%	43%
长期修复方案开发	47%	40%	41%
将系统重新镜像到以前的状态	45%	41%	39%
以上都不是	2%	1%	1%

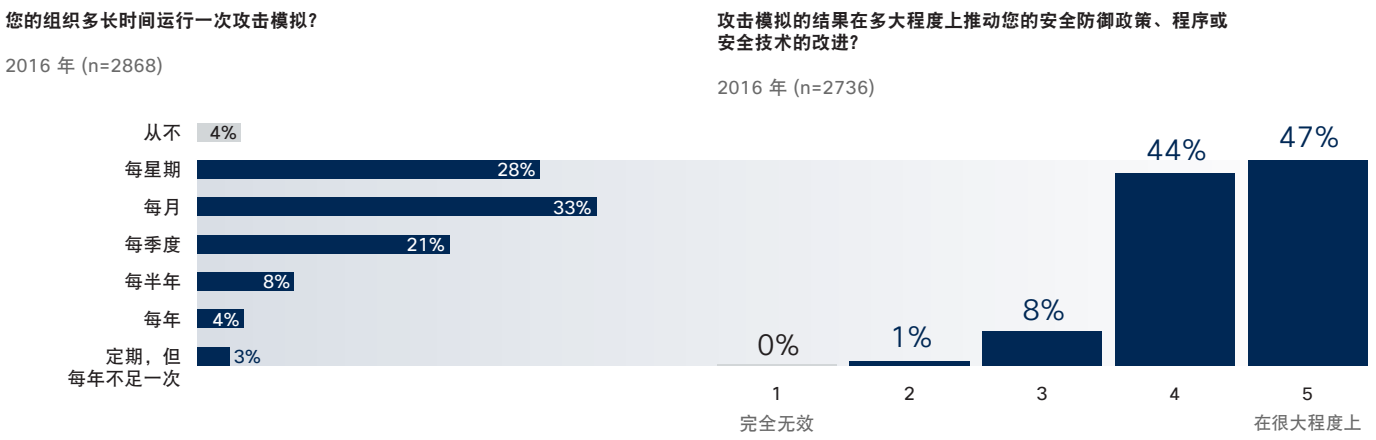
来源：思科 2017 年安全能力基准研究

图 106 用于恢复受影响系统的流程的年同比使用情况

受影响系统的恢复流程	2014 年 (n=1738)	2015 年 (n=2432)	2016 年 (n=2912)
根据事后查明的漏洞，实施其他或全新检测和控制措施	60%	56%	56%
用事件前的备份进行恢复	57%	59%	55%
修补和更新视为有漏洞的应用	60%	55%	53%
差异恢复（删除事件引起的变更）	56%	51%	50%
黄金映像恢复	35%	35%	34%
以上都不是	2%	1%	1%

来源：思科 2017 年安全能力基准研究

图 107 攻击模拟：推动安全防御改进的频率和程度



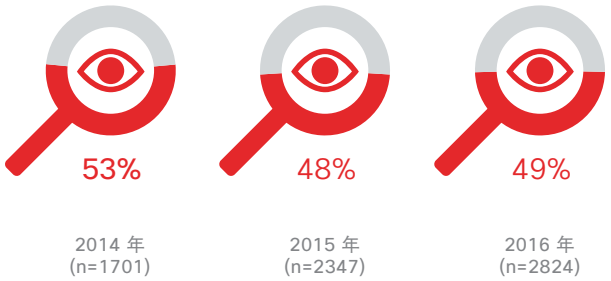
来源：思科 2017 年安全能力基准研究

图 108 确定安全漏洞起源的重要性

来源：思科 2017 年安全能力基准研究

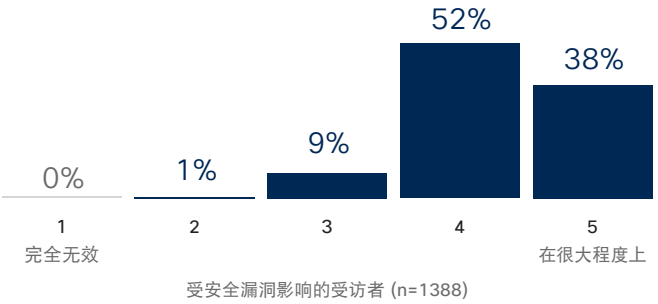
漏洞及其影响

图 109 遇到公开漏洞的组织的百分比



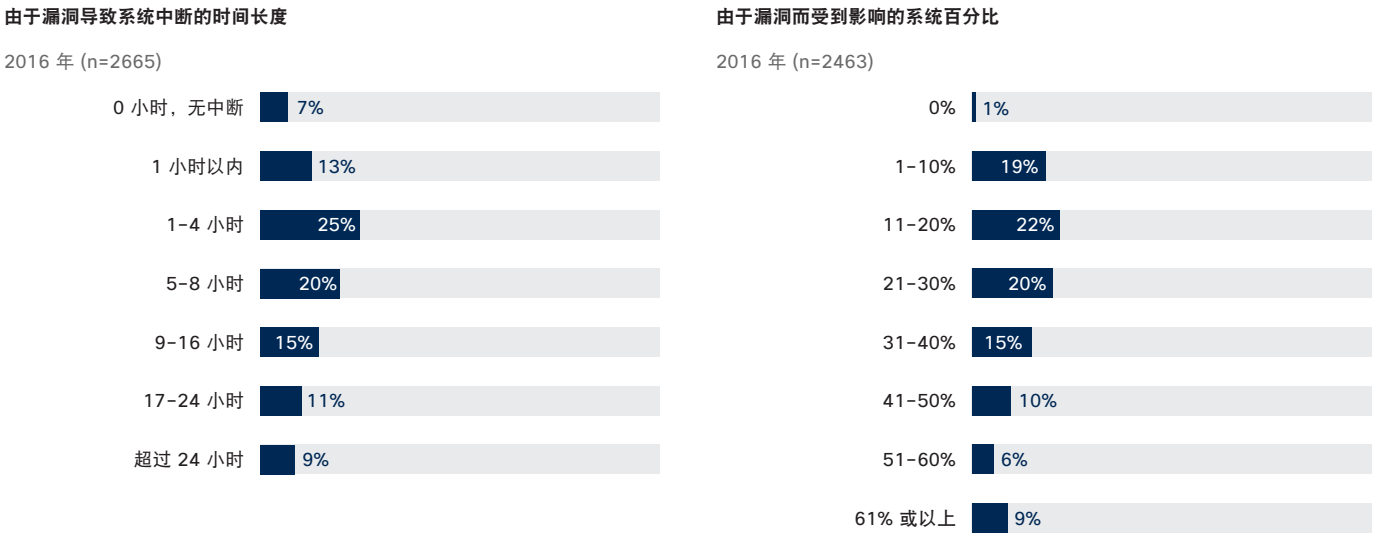
来源：思科 2017 年安全能力基准研究

图 110 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?



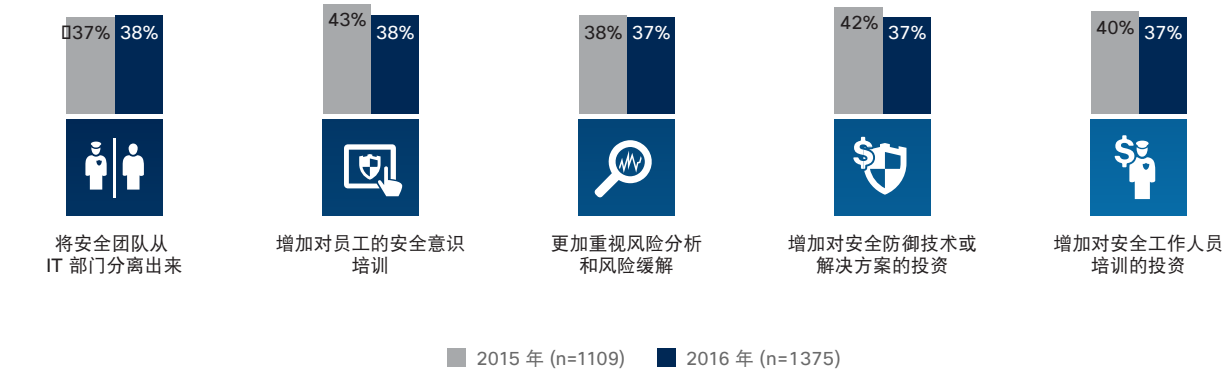
来源：思科 2017 年安全能力基准研究

图 111 由安全漏洞引起的中断的时间长度和广度



来源：思科 2017 年安全能力基准研究

图 112 为保护公司免受安全漏洞影响而作出的改进



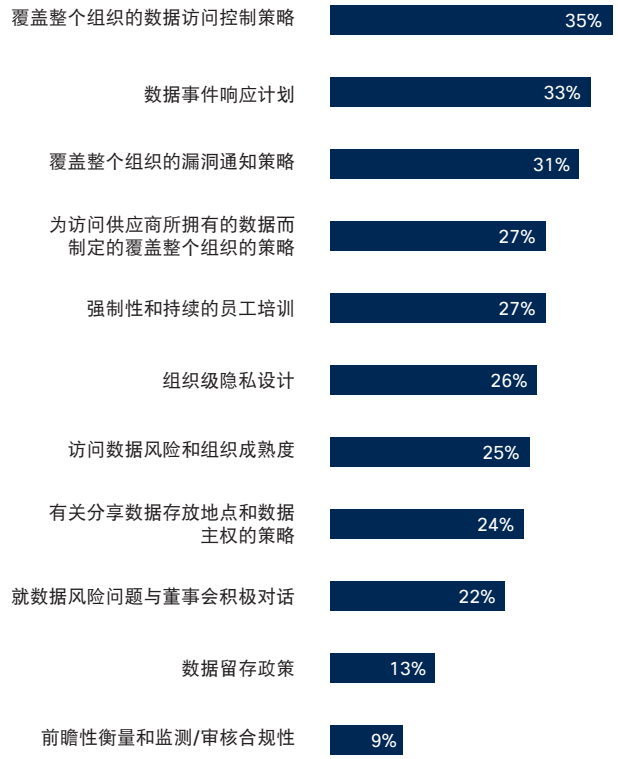
来源：思科 2017 年安全能力基准研究

供应商选择和期望

图 113 供应商数据保护和隐私的重要性

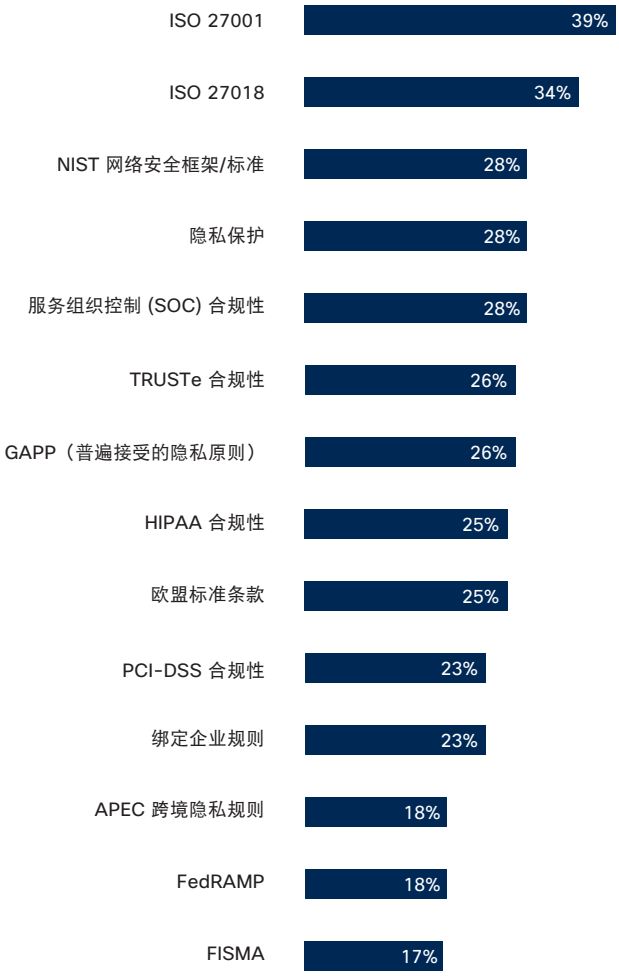
最重要的是，供应商应制定什么样的数据保护以及隐私流程和政策？

2016 年 (n=2912)



供应商如需与您的组织合作，需要达到什么样的数据保护、隐私权标准和认证要求？

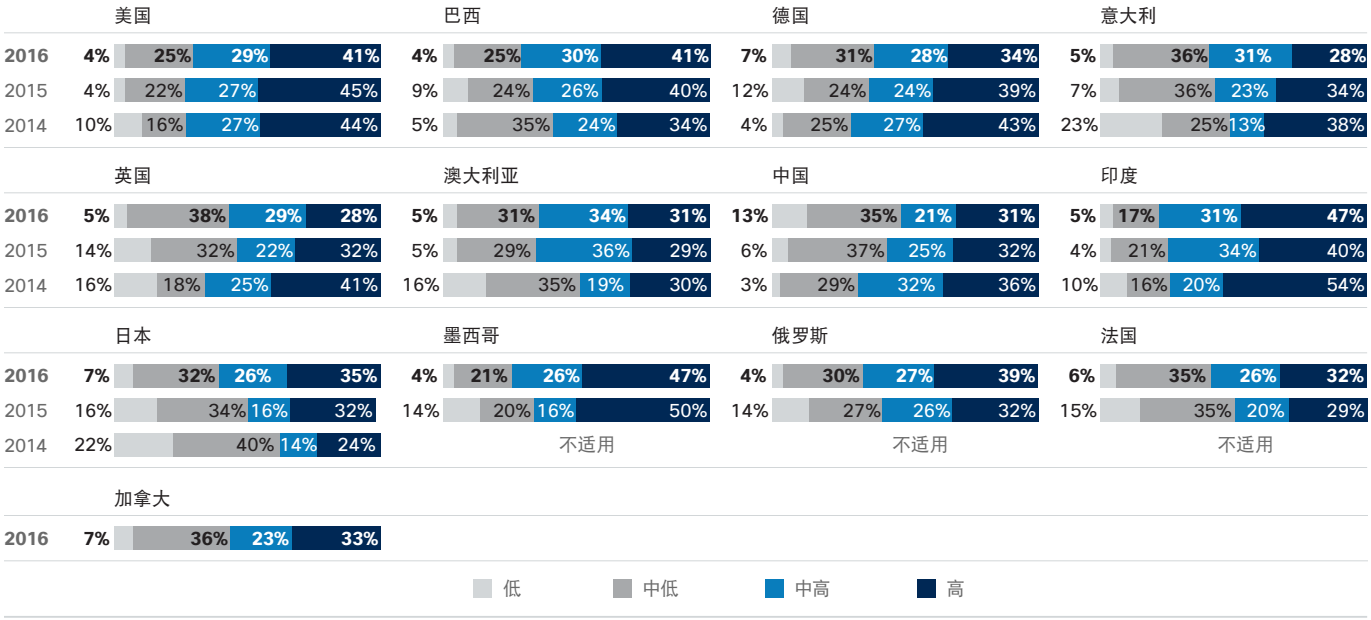
2016 年 (n=2870)



来源：思科 2017 年安全能力基准研究

安全能力成熟度模型

图 114 按国家/地区划分的安全成熟度

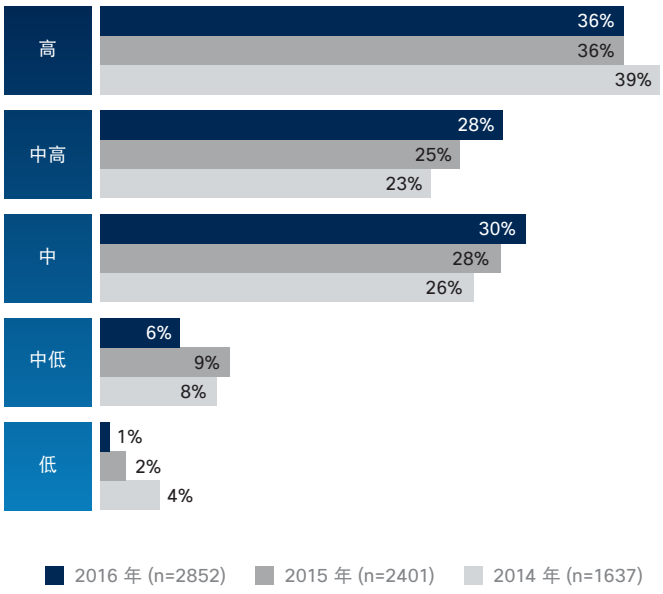


来源：思科 2017 年安全能力基准研究

图 115 成熟度模型根据安全流程评定组织

来源：思科 2017 年安全能力基准研究

图 116 成熟度模型的分段大小

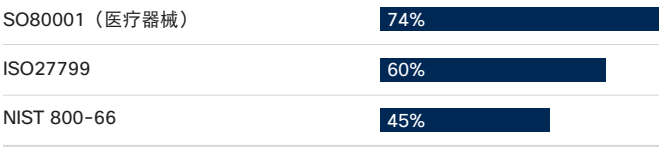


来源：思科 2017 年安全能力基准研究

行业特定

图 117 已实施标准化安全策略的医疗保健企业的百分比

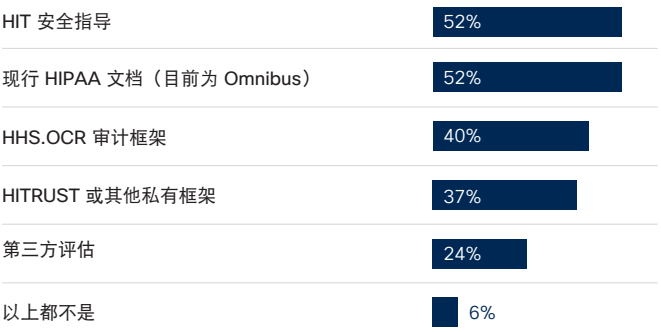
已实施标准化安全策略
遵循医疗保健特定信息安全策略实践的医疗保健企业，2016 年 (n=65)



来源：思科 2017 年安全能力基准研究

图 118 医疗保健公司用于对照 HIPAA 隐私规则衡量他们自己的资源

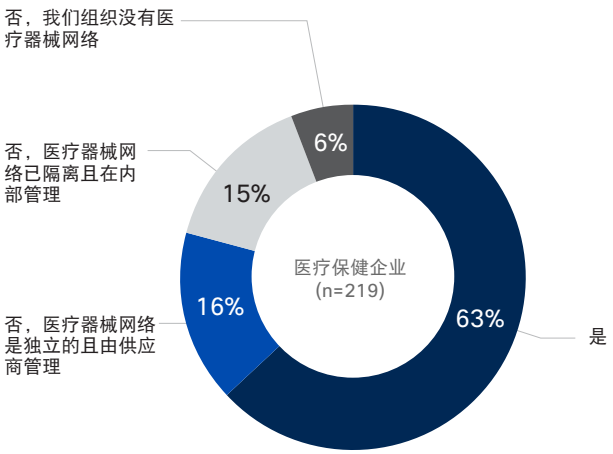
哪些资源用于按照 HIPAA 隐私规则和安全来衡量公司?
医疗保健企业，2016 年 (n=219)



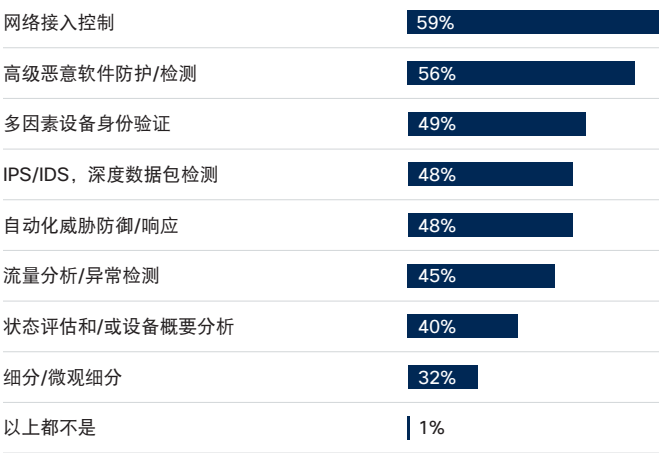
来源：思科 2017 年安全能力基准研究

图 119 具有医疗器械网络的医疗保健企业最常见的安全措施

您的组织是否有与医院主网络融合在一起的医疗器械网络?



您的公司实施了这些安全措施（如有）中的哪一项来保护您的医疗器械网络?
其组织中有医疗器械网络的公司 (n=207)



来源：思科 2017 年安全能力基准研究

图 120 电信行业的样本概要分析

您的组织主要涉及哪一种电信细分领域？
电信企业 (n=307)

通信设备	47%
运营商（传统）	33%
有线/卫星运营商	11%
媒体/广播	7%
OTT 提供商（Netflix、Hulu 等）	2%

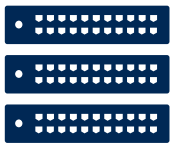
您的公司向客户提供这其中哪些服务？
电信企业 (n=308)

向最终客户提供托管安全服务	71%
核心生产网络，例如 IP（包括电视）、移动等	60%
企业环境	59%
数据中心	57%

来源：思科 2017 年安全能力基准研究

图 121 电信的安全策略因素

安全策略和协议的相对优先级
电信企业 (n=308)



可用性的平均百分比

34%

可用性：确保可靠地访问数据

保密性的平均百分比

36%

保密性：确保数据仅可被相关方访问

完整性的平均百分比

31%

完整性：确保数据精确和准确

来源：思科 2017 年安全能力基准研究

图 122 电信的安全优先级

组织中的安全优先事项排名

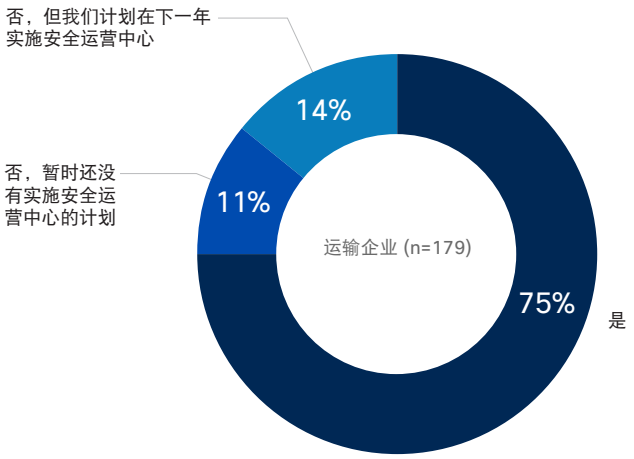
电信企业 (n=308)

	排名第一	排名第二	排名第三	排名第四
保护数据中心	34%	21%	24%	22%
在提供高可用性 IP 和/或移动服务的核心生产网络中	26%	21%	29%	24%
提供托管安全服务	21%	30%	19%	30%
企业网络和内部数据	20%	28%	29%	24%

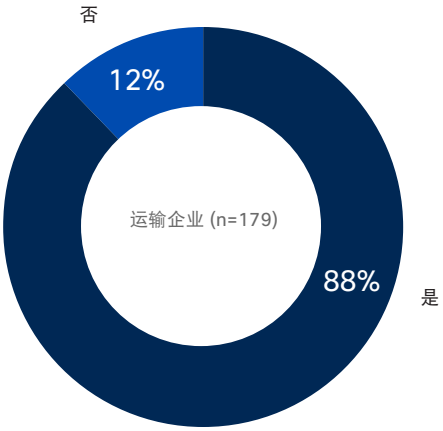
来源：思科 2017 年安全能力基准研究

图 123 运输行业的样本概要分析

您的公司是否利用安全运营中心 (SOC)?



您的公司是否参加安全标准实体或行业组织?



您的组织主要涉及哪一种运输细分领域?
运输企业 (n=180)

货运和物流	54%
公共运输	11%
铁路	9%
公路	9%
航空	7%
海运	5%
车辆	5%

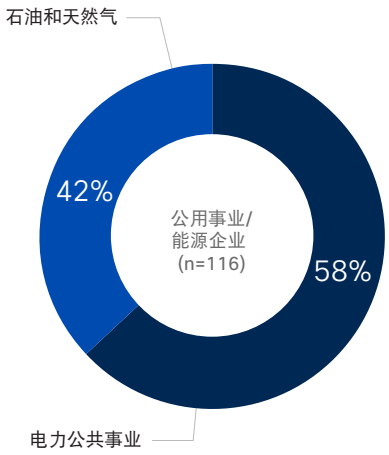
您负责以下哪一种安全领域?
运输企业 (n=180)

运营技术安全	84%
关键基础设施安全	71%
车辆安全	43%

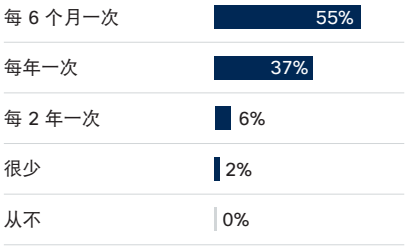
来源：思科 2017 年安全能力基准研究

图 124 公用事业/能源行业的样本概要分析

您的组织主要涉及哪一种公用事业/能源细分领域?

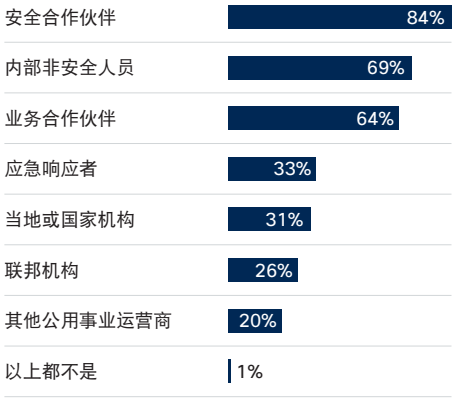


您的组织多长时间演练或测试一次您公司的网络安全事件响应计划?



公用事业/能源企业 (n=116)

在执行这些演练或测试时，涉及哪些方?

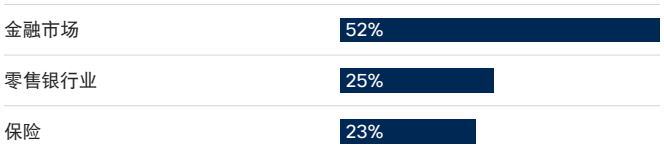


公用事业/能源企业 (n=116)

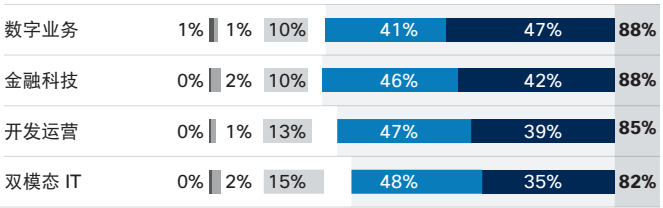
来源：思科 2017 年安全能力基准研究

图 125 金融服务行业的样本概要分析

您的组织主要涉及哪一种金融服务细分领域?



您认为安全会受到以下趋势的多大影响?

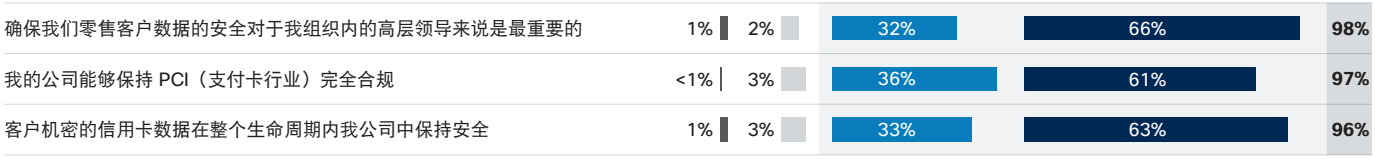


金融服务企业 (n=509)
图表数据四舍五入为整数

来源：思科 2017 年安全能力基准研究

图 126 零售行业的数据安全

您对以下每个说法的赞同程度如何?



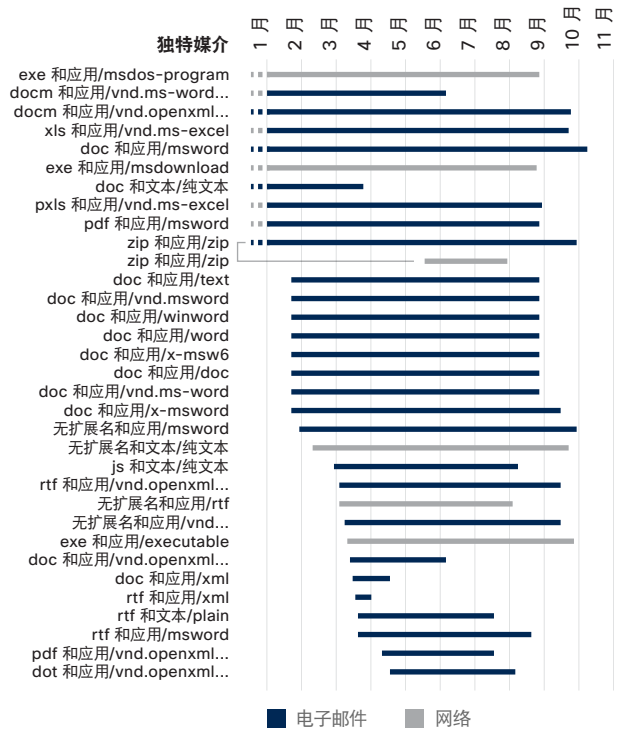
零售企业 (n=290) 图表数据四舍五入为整数

非常反对　不太赞同　比较赞同　非常赞同　% 比较 + 强烈赞同

来源：思科 2017 年安全能力基准研究

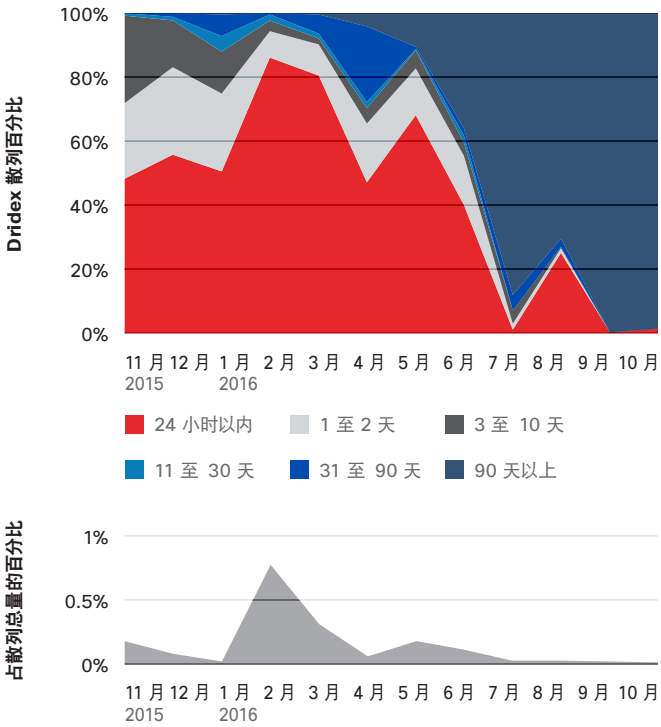
恶意软件系列

图 127 Dridex 的文件扩展名和 MIME 组合（Web 和邮件媒介）



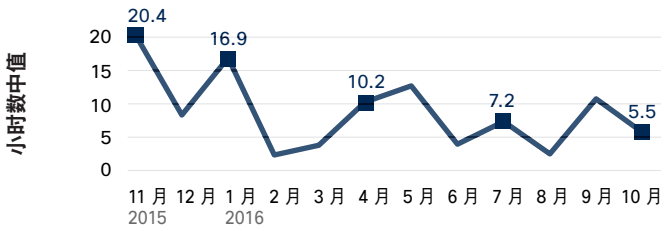
来源：思科安全研究部门

图 128 Dridex 恶意软件系列的散列存活期和每月观察到的散列总量百分比



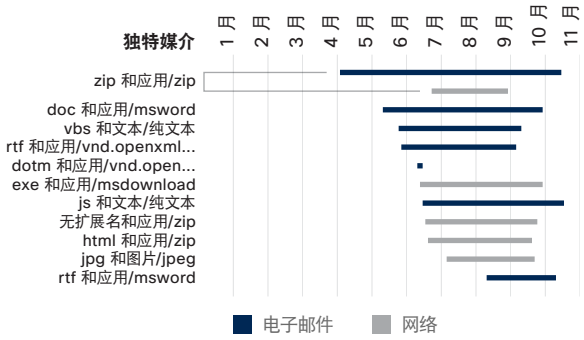
来源：思科安全研究部门

图 129 Dridex 恶意软件系列的 TTD



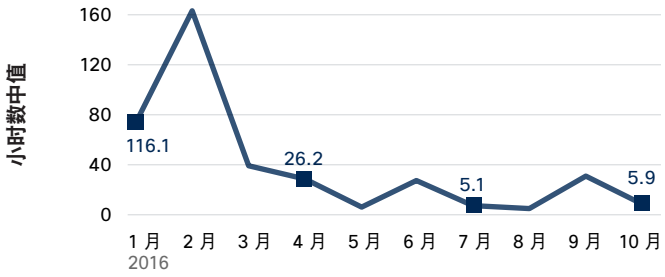
来源: 思科安全研究部门

图 130 造成和包括 Cerber 负载（Web 和邮件媒介）的威胁和指标系列的文件扩展名和 MIME 组合



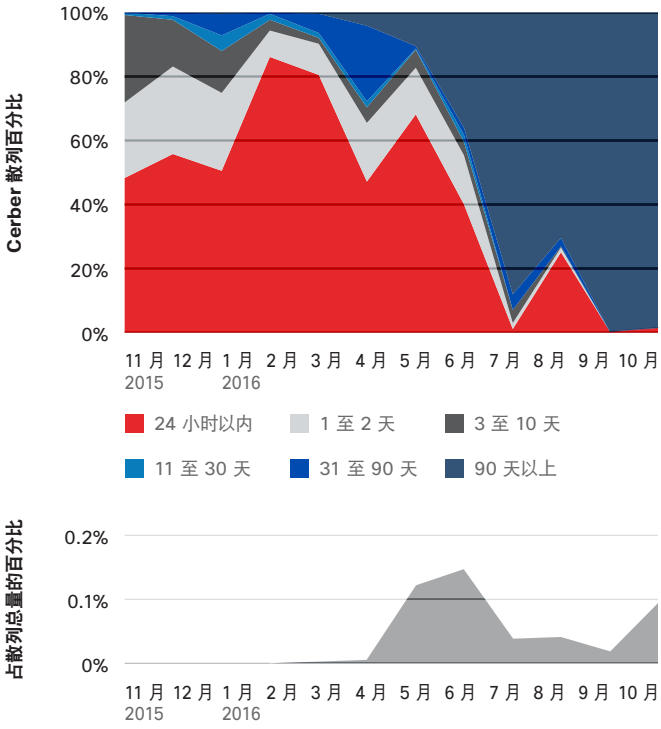
来源：思科安全研究部门

图 131 Cerber 恶意软件系列的 TTD



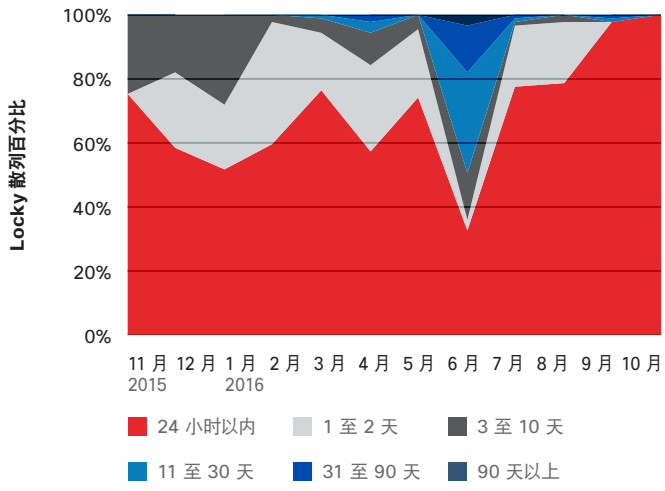
来源：思科安全研究部门

图 132 Cerber 恶意软件系列的散列存活期以及相对于每月观察到的所有散列的百分比



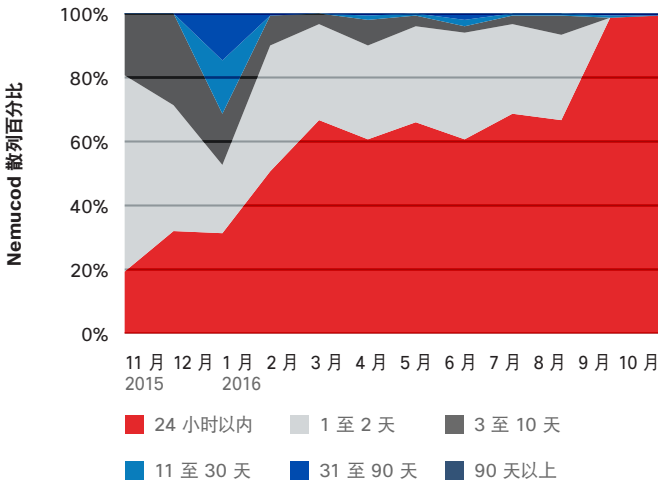
来源：思科安全研究部门

图 133 每月的 Locky 恶意软件系列的散列存活期



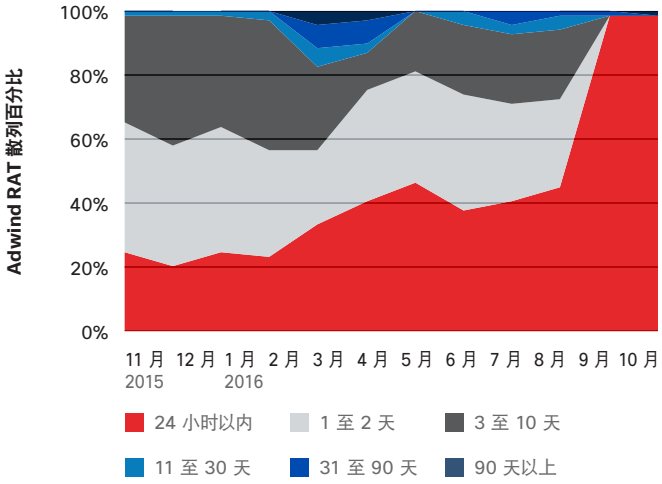
来源：思科安全研究部门

图 134 每月的 Nemucod 恶意软件系列的散列存活期



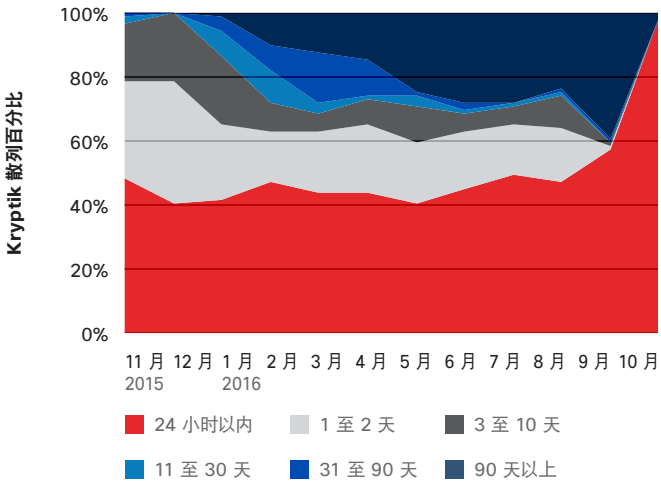
来源：思科安全研究部门

图 135 每月的 Adwind RAT 恶意软件系列的散列存活期



来源：思科安全研究部门

图 136 每月的 Kryptik 恶意软件系列的散列存活期



来源：思科安全研究部门

下载图表

本报告中的所有图表都可以通过以下网址下载：
www.cisco.com/go/acr2017graphics

更新和修正

要查看对本报告中信息的更新和修正，请访问：
www.cisco.com/go/acr2017errata

美洲总部
思科系统公司
加州圣荷西

亚太总部
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。思科网站上列有各办事处的地址、电话和传真，网址为：www.cisco.com/go/offices。

2017 年 1 月发布