CLOUDFLARE

完善网络风险防范 保障未来发展：亚太地区网络安全形势调查报告

目录

内容摘要

作为 Cloudflare 的首席安全官，我有幸能与来自各行各业的首席安全官、CEO 和董事会成员进行交流。我们的讨论中总是会提到一个问题："我们安全吗？"

这是一个简单却几乎无法回答的问题。一种方法是将网络安全比作个人健康。某人今天可能健康，但明天可能变得不健康。同样地，一家公司的网络安全今天可能没有受到威胁，但明天可能就不一样了。

从这些讨论中也清晰显示，同样类型的网络安全问题持续影响着该地区许多组织的运营"健康"。自我们首次发布"亚太地区网络安全形势调查报告"以来已经过去一年，我们的最新研究结果显示，在 3844 名受访者中，有 41% 在 2023 年至 2024 年间经历过一次数据泄露事件，76% 受访者表示他们的公司在同一时期经历的数据泄露事件次数有所增加。代表 IT 和技术、媒体和电信、零售和金融服务行业的受访者报告过去 12 个月中遭受的攻击次数增加最多。

雪上加霜的是，认为已经做好抵御网络攻击准备的受访者比例减少了 29%。这个前景令人担忧，尤其是 51% 的受访者表示，数据泄露造成的财务损失超过 100 万美元。

经济损失、预算压力、保障业务转型技术安全的责任、管理日益增多的 IT 供应商和解决方案，加上类似 AI 驱动的攻击的新兴风险，这些因素的综合作用下，推动各种组织陷入一场复杂性危机。

事实上，86% 的受访者表示，复杂性正使他们的组织更容易受到攻击。这种复杂性在调查结果中得到证明：49% 的受访者已经部署了 20 种以上的安全工具，82% 的受访者仅在今年就增加了更多的供应商和工具。

要有效解决复杂性，就需要做出改变。

首先，企业需要在 AI 方面加倍投入，否则就有可能被淘汰。87% 的受访者表示，AI 要么被用来增加对其组织的攻击次数，要么使攻击变得更加复杂。然而，只有 28% 的受访者认为他们在缓解 AI 攻击方面做好了充分准备。虽然 AI 引发了新的网络相关威胁，但它也是业务转型、生产力和增长的关键驱动力。各组织必须从现在开始着眼未来，列出新兴 AI 技术可在未来给其网络安全策略带来的潜在优势。

其次，实现运营韧性对任何组织的成功都至关重要，而且这是与强大的网络安全计划相辅相成的。在监管机构制定任何强制要求之前，就必须将韧性充分融入网络安全策略中。近期的全球网络安全事件凸显了，缺乏现代化、具有韧性的基础设施，或者深思熟虑的危机应对计划，企业将可能面临怎样的挑战。

最后，重要的是立即行动以消除复杂性。近 90% 的受访者表示复杂性正使他们的组织更容易受到攻击，因此迫切需要采取行动。整合安全和技术栈，精简流程并现代化 IT 架构，转移资源以确保业务成果，并开始改造网络员工队伍，以便支持部署基于 AI 的解决方案。我们将以这样的方式改变本行业过去 20 年中所面临的历史结果。

我希望这份报告能帮助各组织的 CISO 及其团队应对未来 12 个月的挑战，并提供如何抓住新机遇的指引。从这份报告中获得的见解应该能够帮助 CISO 识别在应对网络安全栈复杂性时的障碍，以便可以更明智地决定如何应对 AI 驱动的威胁和机遇，战略性地重新调整资源以克服人才限制，并研究出如何最好地应对错综复杂的监管环境。要防范日益复杂的攻击并确保组织安全，还有大量工作要做。因此，从身居类似岗位的其他人那里获得的经验可能会为您提供急需的灵感，帮助您做好充分准备以应对那个至关重要的问题：“我们安全吗？”

此致！

Grant Bourzikas
高级副总裁兼首席安全官

方法

该报告基于 2024 年 6 月进行的一项双盲调查的结果，该调查涉及 3844 名负责各自组织网络安全的领导者，包括高管层、安全领导、安全管理，以及网络安全技术领导。

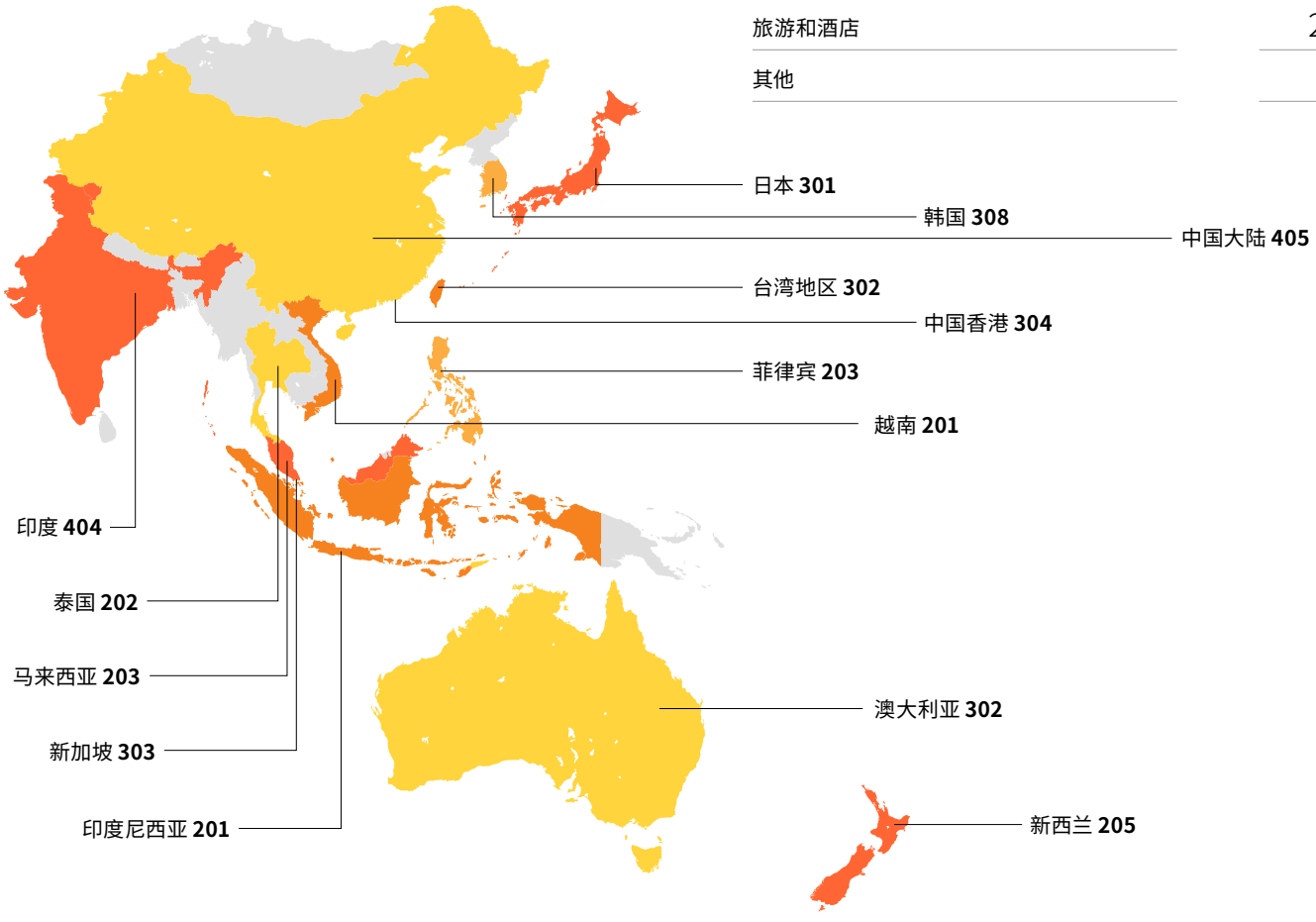
受访者来自亚太地区的 14 个市场：澳大利亚、中国、香港特别行政区、印度、印度尼西亚、日本、马来西亚、新西兰、菲律宾、新加坡、韩国、台湾地区、泰国和越南。

今年的调查聚焦于亚太地区企业面临的网络安全挑战，受访者所在组织规模不少于 250 名员工，并更侧重于大型组织。来自小型组织（250-999 名员工）的受访者占样本的 18%，而来自中型和大型组织的受访者分别占参与者的 27% 和 55%。

参与者来自各行各业

行业	受访者人数
商业和专业服务	371
建筑与房地产	355
教育	204
能源、公用事业和自然资源	347
金融服务	349
游戏	65
政府机构	263
医疗保健	254
IT 和技术	368
法律/法律服务	4
制造业	352
媒体与电信	163
零售	342
交通运输	151
旅游和酒店	236
其他	9

受访者分布



数据泄露让组织不堪重负

自我们上一份报告以来已经过去了 12 个月，亚太地区的网络安全领导者继续努力应对复杂的威胁形势。68% 的受访者表示在过去 12 个月内经历了网络安全事件，今年的报告更深入探讨了这些事件是如何发展的。我们的研究显示，在经历过网络安全事件的受访者中，61% 遭遇了数据泄露[1]。

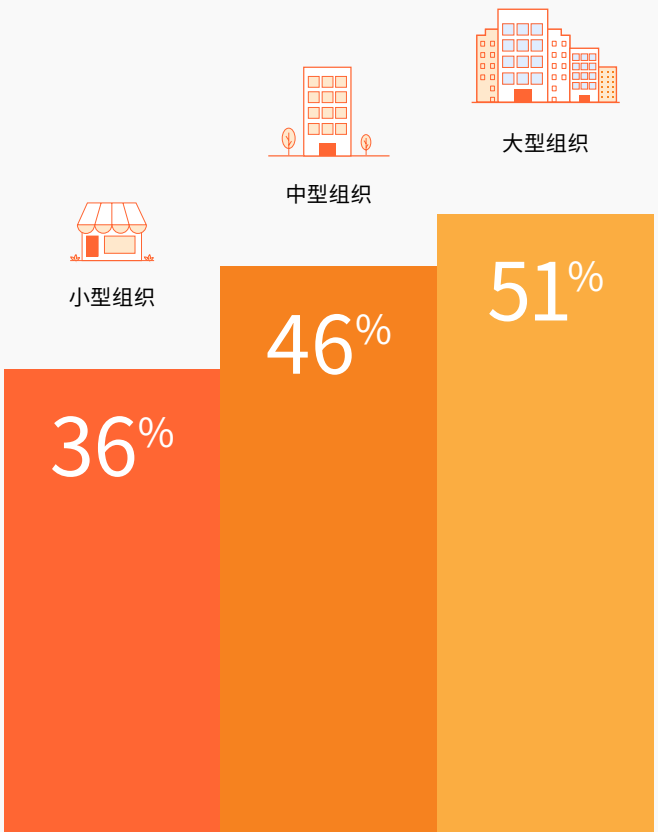
许多存在暴露漏洞的组织在能够堵住防御漏洞之前反复受到攻击。47% 的受访者表示，他们的组织在本次研究前的 12 个月内经历了 10 次以上的数据泄露。攻击者似乎特别关注大型组织。过去一年中最有可能经历 10 次或更多数据泄露的组织来自建筑和房地产、旅游和酒店以及金融服务行业。

在过去一年经历过数据泄露的受访者中，76% 表示数据泄露的频率有所增加。58% 认为未来 12 个月内会看到更高的数字。此外，70% 的受访者在过去一年中经历了一次数据泄露，或者认为他们将在未来一年内可能会成为受害者。来自越南 (86%)、印度 (82%)、马来西亚 (80%) 和新加坡 (80%) 的受访者表示过去 12 个月内数据泄露有明显增加。

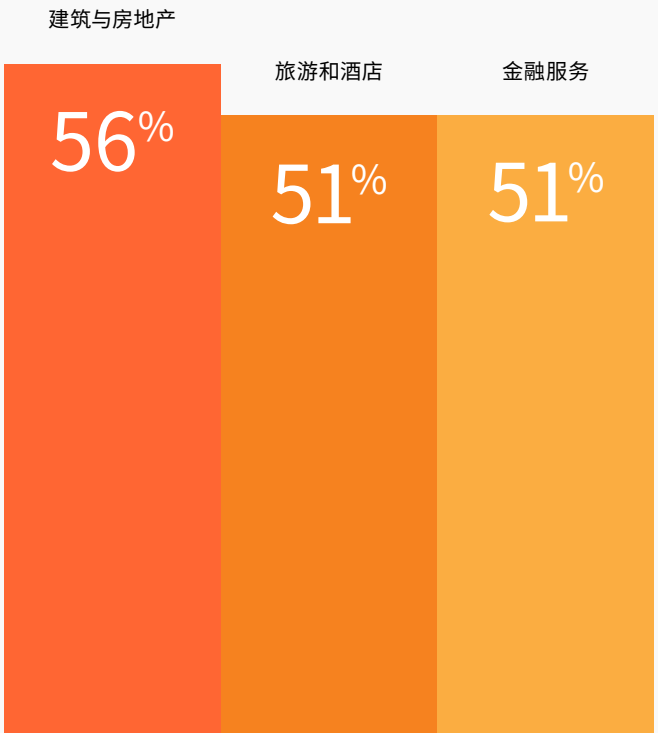
1.数据泄露是指攻击者未经授权访问组织的应用、数据和网络的事件，这些事件是可能危及到系统完整性的行为。

报告在过去 12 个月发生网络安全事件的受访者比例 %

按组织规模



最常成为攻击目标的行业



51% 的受访者报告数据泄露造成的总损失超过 100 万美元，其中 27% 的受访者报告损失超过 200 万美元。财务损失绝不是受影响组织面临的唯一影响。对于经历过数据丢失的组织而言，客户数据最常成为攻击目标，67% 的受访者表示此类数据被盗。同样，用户访问凭据 (58%) 和财务数据 (55%) 也经常被盗。

对于那些遭受数据泄露的组织，产生的财务损失还包括网络安全保险单不涵盖的额外费用，以及保费同比上涨的财务负担。中型组织 (可能没有购置稳健的保单) 也成为了复杂攻击的目标，往往承担了大部分额外开支。

Web 攻击、恶意软件 (病毒、蠕虫、特洛伊木马等) 和网络钓鱼继续成为过去一年中导致数据泄露的最常见攻击手段。

年度保费增长 (美元)

小型组织	中型组织	大型组织
80,381	566,107	437,865

最近一次数据泄露产生的额外支出 (美元)

小型组织	中型组织	大型组织
103,361	705,610	152,674

五种最常见的网络攻击手段

网络攻击 57%

恶意软件 49%

网络钓鱼 44%

供应链攻击 35%

企业电子邮件破坏 33%

几乎所有 (92%) 组织在遭受数据泄露后都面临着进一步的业务影响，主要包括监管行动 (26%)、利用数据的进一步攻击 (17%) 和声誉损害 (16%)。

根据 Cloudflare 第二季度 DDoS 威胁报告，分布式拒绝服务 (DDoS) 攻击同比增长了 20% ，达到 400 万次，其中 55% 是第 3/4 层 DDoS 攻击。我们的数据反映了这一现状，67% 的受访者表示，他们的组织曾遭受过 DDoS 攻击。其中大多数攻击是第 4 层 (47%) 或第 3 层 (41%)，API 或第 7 层攻击分别仅占攻击数目的 26% 和 18%。DDoS 攻击的主要影响是财务损失 (55%) 和服务中断 (54%)。

另一个可能让许多 IT 领导者担忧的因素是响应时间。76% 的受访者表示，他们的组织平均需要超过 12 小时才能识别数据泄露，而 74% 的组织需要超过半天的时间来控制事件。

因此，不足为奇的是，只有 27% 的受访者目前认为他们的组织做好了预防数据泄露的充分准备。

AI 正在改变威胁格局

近年来，人工智能 (AI) 在各行各业的讨论中占据了主导地位。然而，在网络安全领域，我们的受访者表达了一种以负面为主的看法，87% 的受访者认为 AI 要么导致攻击更频繁，要么使攻击者变得更高明。

尽管普遍担心 AI 对网络安全的影响，但对于跟上威胁步伐的信心却很高，83% 的受访者表示，他们的网络安全团队能够在未来领先于利用 AI 发动网络攻击的威胁行为者。然而，如果一个组织成为 AI 驱动的数据泄露的目标，只有 28% 的受访者认为他们的组织做好了充分准备，这凸显了信心与实际就绪程度之间的差距——直到进行了关键能力升级为止。

工程和汽车 (45%) 以及 IT 和科技 (42%) 行业的受访者认为自己为防止这些类型的数据泄露做好了最充分准备。与此形成鲜明对比的是，法律和法律服务 (25%) 以及教育 (21%) 行业的信心程度较低。

展望未来，我们的受访者认为，随着威胁行为者研究如何更有效地使用 AI 技术，来自 AI 的威胁将会增加。具体而言，50% 的受访者预计 AI 将被用于破解密码或加密代码。此外，47% 的受访者认为它将增强网络钓鱼攻击和社会工程学技术，44% 的受访者认为 AI 将促进 DDoS 攻击的发展。最后，40% 的受访者认为 AI 将在制造深度伪造和促进隐私泄露方面发挥作用。

由于这些新型、多样化的威胁，70% 的受访者表示他们的组织正在改变工作方式。最有可能受到 AI 所致变化影响的行业是治理和监管合规 (40%)、网络安全团队的战略方向 (39%) 以及供应商合作 (36%)。

网络安全领导者也在加强自身能力，以抗击 AI 带来的威胁。每位受访者都预计在未来部署至少一种新的 AI 相关安全工具、技术或措施。雇用生成式 AI 分析师 (45%)、进一步投资威胁检测和响应系统，以及安全信息和事件管理 (SIEM) 系统 (均为40%) 被列为未来的首要措施。IT 供应商将继续发挥重要作用，因为 66% 的受访者已经向他们寻求 AI 相关解决方案。

因支付赎金证明无济于事，应对勒索软件攻击的方式不断演变

全球范围内，勒索软件及其后续赎金要求不断增加，亚太地区也不例外。

我们的调查显示，在所有经历过数据泄露的受访者中，有 22% 成为勒索软件攻击的目标。在受影响的组织中，62% 最终支付了赎金。普遍支付赎金的现象与 70% 受影响组织曾承诺不支付赎金的事实形成了鲜明对比。

然而，不同国家/地区之间存在显著的差异，印度 (69%)、中国香港 (67%)、马来西亚 (50%) 和印度尼西亚 (50%) 的组织最有可能支付赎金，而韩国 (19%)、日本 (19%) 和新西兰 (22%) 最不可能屈服于赎金要求。

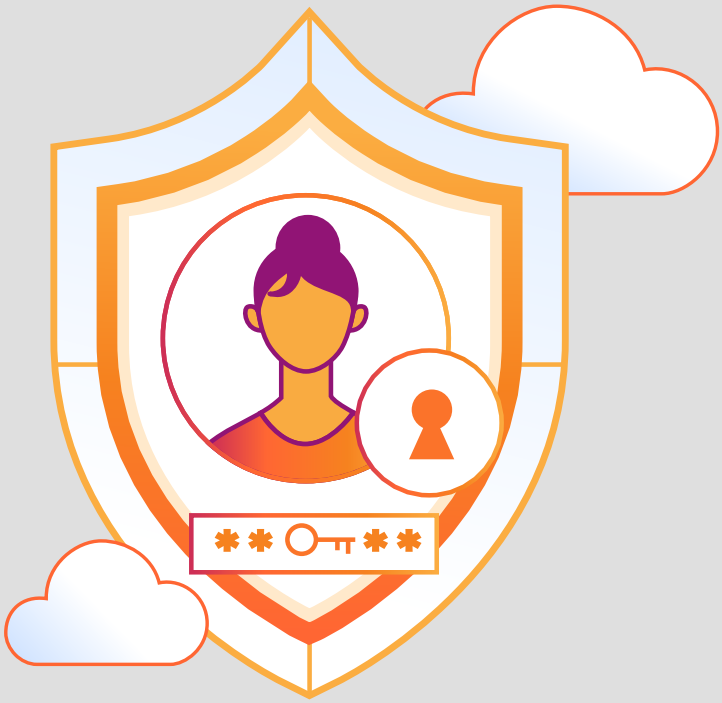
屈服于勒索要求的因素有很多，但最常见的是担心数据丢失的法律后果 (39%)、轻松恢复数据的好处 (25%)、担心长时间宕机 (22%) 和道德影响 (13%)。

几乎每个最终支付赎金的组织都为之后悔，96% 支付赎金的受访者发现其决定产生了一个或多个后果：

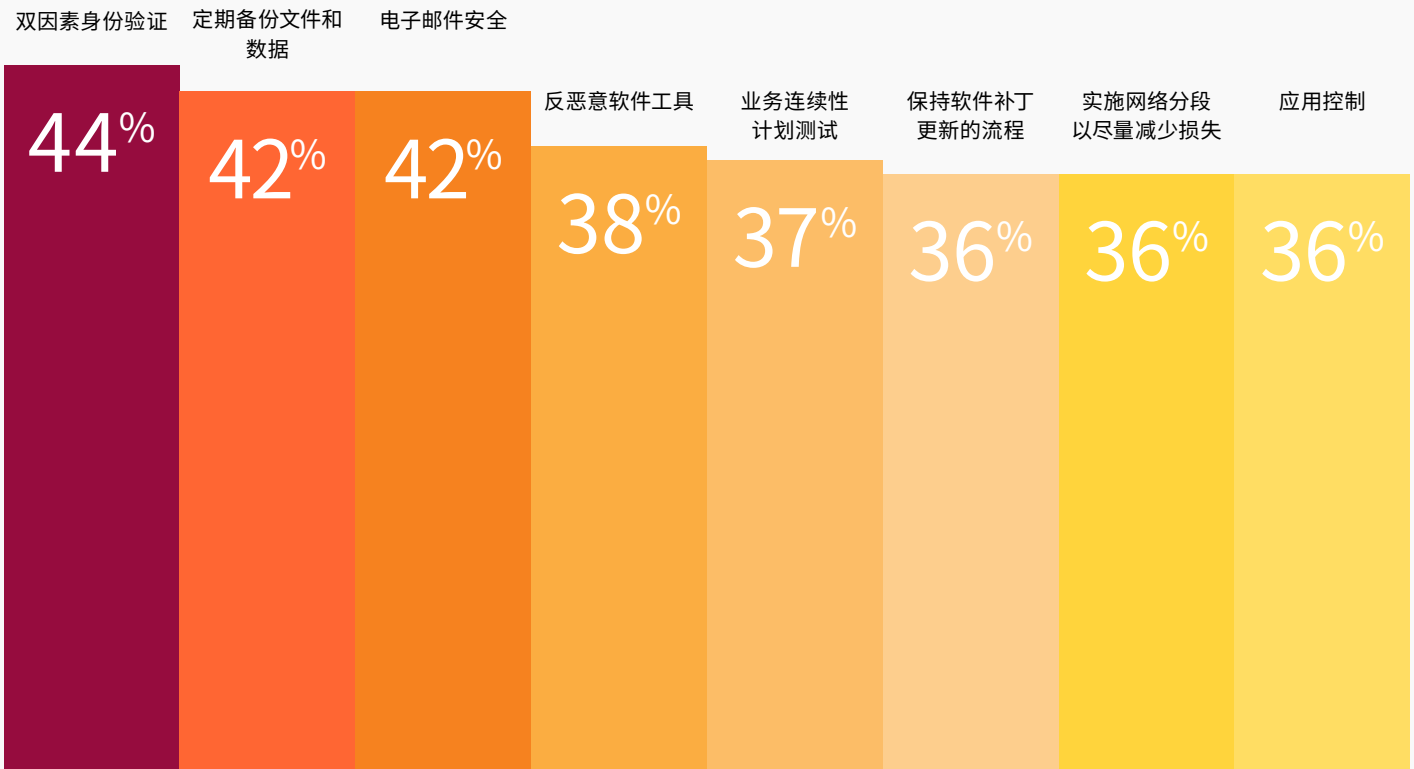
- 支付赎金的消息公开后，来自新来源的勒索攻击有所增加 (63%)
- 攻击者并没有删除窃取的数据，或在日后予以出售/披露 (56%)
- 攻击者没有履行恢复系统和归还数据的协议 (53%)
- 仅部分被盗数据得到恢复 (50%)
- 同一批攻击者卷土重来，提出进一步的赎金要求 (46%)

根据我们的受访者反馈，这些攻击最常见的入口点是被攻破的远程桌面协议或 VPN 服务器。这种情况占所有勒索软件攻击的 47%，但对中型公司而言是尤其严重，占 61%。第二个最常见的入口点是 Web 应用或服务器中未修补的漏洞 (39%)。

鉴于这些漏洞，受访者重点关注可用于防范勒索软件攻击的措施。Zero Trust 架构的常见原则（例如网络分段和定期数据备份）可以限制勒索软件攻击者的手段，但我们的数据显示在这些方面还有很大的改进空间。



部署“非常成熟的”(76-100%) 反勒索软件措施的受访者比例 %

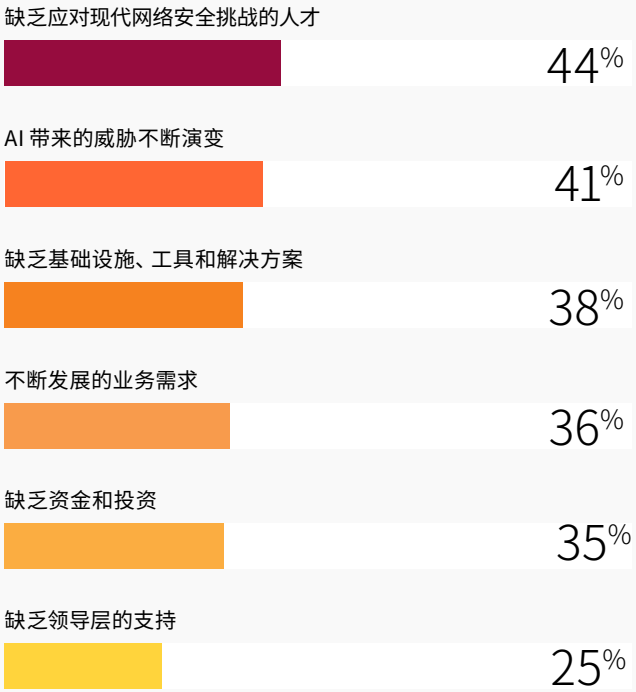


网络安全团队被要求承担更多责任，但可用投资减少了

仅 21% 的受访者认为他们所在组织的网络安全态势非常成熟，多个关键因素正在阻碍组织的发展。

缺乏人才仍然是最紧迫的挑战 (44%)，同时只有 33% 的组织投资于领导团队的网络安全培训。大多数 (83%) 受访者在网络安全准备方面面临至少以下两项挑战。

将以下至少两项列为其三大网络安全挑战之一的受访者百分比 %：



不断扩大的数据泄露威胁已成为许多高层领导团队的重要议程之一，80% 的受访者表示他们至少每月需要向董事会汇报数据泄露情况，而 22% 的受访者需要每周汇报。

在预算分配方面，84% 的受访者表示，在过去 12 个月里，他们所在的组织将总 IT 预算的 10% 以上用于网络安全，而 30% 的组织在这方面的支出超过了 20%。尽管亚太地区市场环境充满挑战，但预计来年的预算将保持相对稳定。

鉴于网络安全领导者努力应对人才短缺问题，这一点将至关重要。许多人认识到寻找新员工是一项挑战，因此正在投资提升团队成员的技能 (48%)。类似比例 (45%) 的受访者正投资于团队和流程重组，36% 将网络安全功能外包给托管服务提供商 (MSP)。虽说承认应对网络安全威胁方面存在人才短缺问题，但只有 31% 的受访者承认应对网络安全威胁方面存在人才短缺问题，但并未完全排除招聘新员工的可能。

更多的解决方案并不能使组织更安全

疫情带来的快速数字化和数字转型努力中产生了一些问题，持续至今。值得注意的是，许多产品和解决方案是在团队努力应对管理大量远程员工的复杂性之际匆忙实施的。

总体而言，在报告多种解决方案和 IT 供应商带来复杂性的受访者中，86% 称这种复杂性导致他们的组织更容易受到攻击。除了防御攻击的困难之外，网络安全架构的复杂性还导致人才过度紧张，以及处理成功的攻击时存在延迟。

管理多家 IT 供应商带来的挑战

人才挑战（现有人力过度紧张、人力不足、人力过多）	52%
与现有其他解决方案/软件集成的挑战	49%
在重复性任务/非关键网络安全功能上花费过多时间	49%
补救网络攻击需要操作太多解决方案	48%
补救网络攻击需要更长时间	47%
功能重叠意味着某些解决方案成为冗余	46%
需要遵守太多严格的协议和流程	44%

管理多家 IT 供应商带来的挑战

	过去 12 个月经历 30 次以上的数据泄露（占经历过数据泄露的组织的比例）
拥有不到 10 家 IT 供应商的组织	4%
拥有 11-20 家 IT 供应商的组织	6%
拥有 21-30 家 IT 供应商的组织	24%
拥有超过 30 家 IT 供应商的组织	45%

几乎所有受访者 (92%) 都至少经历过其中两个问题，67% 的受访者表示其组织从 10 家以上的 IT 供应商购买了解决方案，40% 的组织由 20 家以上的 IT 供应商提供服务。尽管如此，供应商数量仍有增无减，82%的受访者表示，在过去两年中，他们合作的 IT 供应商数量有所增加。

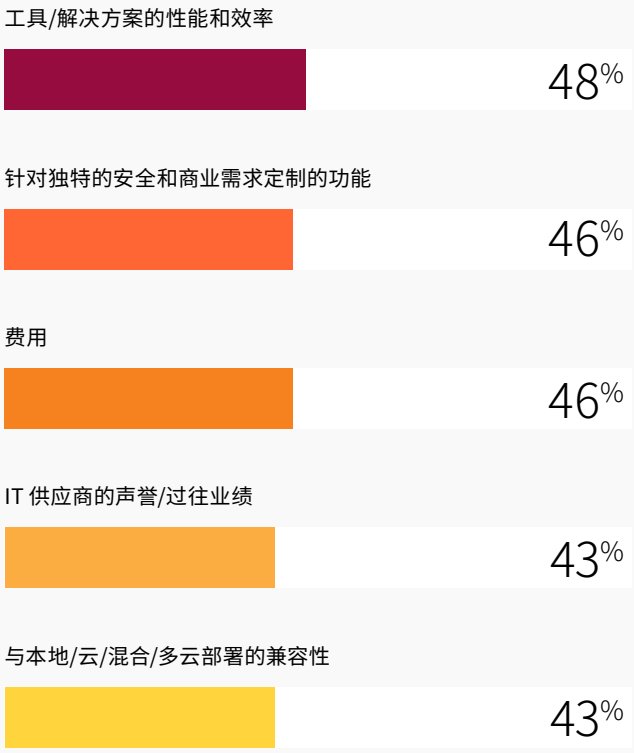
从众多 IT 供应商处购买解决方案并不会让组织变得更安全。IT 供应商较少的组织受到攻击的可能性更低。在拥有少于 10 家 IT 供应商的组织中，只有 4% 在过去一年经历了 30 次以上的数据泄露，而拥有超过 30 家 IT 供应商的组织中，这个比例达到 45%。

IT供应商数量不断增加不但使维持组织安全的复杂性增加，还导致了成本飙升。我们的调查显示，IT 供应商的数量和预算分配之间存在直接联系。拥有 30 家或更多 IT 供应商的组织中，有 22% 将 30% 以上的 IT 预算用于网络安全，而在拥有少于 10 家 IT 供应商的组织中，只有 5% 将 IT 预算的这一比例用于网络安全。

从更广泛的角度来看 IT 供应商数量增加带来的财务影响，我们的受访者报告称，平均而言，用于工具和解决方案的支出增加了 18%。那些减少了 IT 供应商数量的受访者发现成本仅增加了 6%。

由于可供选择的解决方案如此之多，网络安全决策者必须制定各种评估标准，以确保他们在做出选择时不仅仅基于成本。或许并不意外的是，受访者告诉我们，性能和效率是最重要的，紧随其后的是定制解决方案和成本。

选择新解决方案的因素



要求 IT 供应商展示投资回报率的计算项目

采用集中式威胁检测和响应后，数据泄露响应时间缩短	64%
管理更少解决方案所节省的时间带来的成本节约	64%
将多个订阅替换为其他解决方案所带来的成本节省	52%
降低由孤立解决方案和人为错误导致的安全漏洞风险	50%
自动化、简化网络安全流程	31%

整合解决方案或 IT 供应商的数量对组织有明显的优势，其中最重要的是能够获得更好的安全成果。随着企业日益认识到这一现实，他们正在对所选的 IT 供应商施加压力，以推动整合。左表显示对 IT 供应商提出的前五大要求，从节省的工时到事件响应时间。

组织评估选择部署工具的有效性的方式也发生了变化，重点关注性能而非数据泄露的影响。

选择新网络安全工具和解决方案时的首要因素

56% 响应网络攻击所需时间	55% 检测网络攻击所需时间	55% 检测高级威胁的效果
46% 丢失数据的量	44% 造成的经济损失	43% 升级之间的时间

Zero Trust 解决方案对网络安全至关重要

在威胁形势日益严峻的情况下，Zero Trust 越来越受重视。

大约 88% 的受访者已经投资或计划投资于 Zero Trust 解决方案。在已经部署这些解决方案的受访者中，33% 已全面部署，42% 部分部署，侧重于数据加密和多因素认证 (MFA)。此外，80% 的受访者表示至少部分部署了安全 Web 网关和防火墙即服务。推动向 Zero Trust 架构转变的几个关键原因：

- 通过实施多因素身份验证，减少用户凭据盗窃和网络钓鱼的影响；
- 通过分隔用户访问，Zero Trust 可确保用户只能访问特定资源，而不会暴露整个网络。这种方法对于限制勒索软件攻击的严重程度至关重要；
- Zero Trust 框架可降低易受攻击的 IoT（物联网）设备带来的风险，而这些设备通常难以保护和更新；
- 并为连接的用户和设备进行持续监控和验证。

对于已迁移到 Zero Trust 受访者被问及给组织流程带来的效率提升时，84% 的受访者表示，通过 VPN 替代或增强缓解了远程办公人员的瓶颈。相反，新员工入职带来的效率提升最小。

然而，迁移到 Zero Trust 框架并不是一个简单直接的过程。83% 的受访者表示，迁移到使用 SASE 模型的 Zero Trust 架构是一项“复杂”(65%) 或“高度复杂”(18%) 的挑战。这一变化还必须从人员的角度进行管理，因为 23% 的最终用户不支持此举。鉴于其专业知识，网络安全团队几乎普遍 (89%) 支持。

88% 的受访者表示，在准备向 Zero Trust 转变时，最具挑战性的任务是梳理所有需要访问敏感数据存储、必要系统和应用的任务的事务流程。

监管加码成为核心问题

网络安全团队面临着日益增多的监管要求，需要耗费大量时间和资源来管理。我们的调查显示，43% 的受访者将组织 5% 以上的 IT 预算用于合规和认证事务。

48% 的受访者每周工作时间的 10% 或更多的（半天）用于跟上不断变化的监管和认证要求。这一挑战在游戏行业最为明显，62% 的组织在监管合规方面花费了更多时间。

几乎所有组织 (99%) 发现在过去两年中，在监管合规上需要投入更多时间，其中 47% 的组织报告，每周在这方面花费的时间增加了 20% 或更多。

在过去两年中，地方网络安全法规最可能导致组织网络安全架构的复杂性增加。这解释了所花费时间的增加 (64%)，而国际数据隐私法规 (57%)、本地数据隐私法规 (55%) 和国际网络安全法规 (49%) 则是解释了在其他形式监管上花费的时间。

中国香港 (75%)、台湾地区 (70%) 和印度尼西亚 (70%) 的受访者最有可能报告本地网络安全法规导致复杂性增加，而受影响最大的行业是交通运输 (73%) 以及能源，公共事业和自然资源 (72%)，可能是因为这些行业与公共部门的联系非常密切。

在过去两年里，遵守更多监管和合规变化所带来了切实的影响。每一位受访者都至少经历过一个以下问题，77% 受访者经历过至少两个问题：

- 影响了组织向客户提供技术和数据的能力：46%
- 影响了网络安全团队实现业务目标的能力：46%
- 影响了网络安全团队向 CIO 和 CISO 交付成果的能力：44%
- 影响了企业的整体运作：40%
- 迫使企业在每个市场部署实体 IT 设备：39%
- 禁止使用未经认证的 IT 供应商：37%

监管要求增强带来负面影响的同时，受访者也指出了一些积极的方面。所有的受访者都表示他们至少看到了以下一项，而 79% 的受访者至少看到了两项：

- 改善组织的基线隐私和/或安全水平：59%
- 提高组织的技术和数据的完整性：57%
- 改善组织的声誉和品牌：53%
- 增加私营部门销售机会：42%
- 增加公共部门销售机会：39%

对于更严格的认证是否能为遵守它们所花费的时间带来积极回报存在质疑。只有少数受访者认为，常见的认证对他们组织的安全、品牌或商业机会产生了积极影响，其中对美国联邦风险与授权管理计划 (FedRAMP) 的评价最为积极，达到 42%。

然而,这并非是普遍的情况,某些市场欢迎更高程度的审查：越南 (62%)、菲律宾 (58%) 和泰国 (57%) 的受访者欢迎 FedRAMP，并认为其具有积极影响。

在处理客户信用卡数据的组织中，66% 完全遵守新的支付卡行业数据安全标准 4.0 (PCI DDS 4.0) 框架，另有三分之一 (31%) 部分合规。与框架的其他领域相比，受访组织在加密和数据保护方面似乎更加成熟 (71%)。

建议

网络安全团队面临着日益复杂的威胁形势，包括潜在的 AI 驱动攻击。与此同时，领导者还要平衡预算限制、应对监管要求并继续争夺顶级安全人才。传统解决方案涉及多家供应商，这种复杂性加剧了当前动态环境的挑战。

我们可以提出哪些建议来支持 CISO 取得成功？

1. **精简解决方案以降低复杂性：**在去年的报告中，我们建议通过SASE简化安全架构。今年，这一建议不仅仍然有效，而且证据显而易见：更多解决方案和 IT 供应商与风险减少并不相关。组织应该考虑采取更加审慎的方法，以尽量减少部署的解决方案数量，并整合提供解决方案的 IT 供应商。

2. **加强链条中最薄弱的环节：**在当今全球化和万物互连的环境中，每个组织都依赖软件供应链。应用基于开源代码、API 和第三方集成构建，这些都是不断扩大的攻击面。鉴于我们的攻击面不断扩大，选择一个新合作伙伴意味着信任其整个开发生态系统，而不仅仅是工具本身。从基于边界的安全模型转向 Zero Trust 模型可以降低供应链入侵的风险，因为后者不信任任何人，并假设攻击者已在网络之中，根据身份和上下文评估用户、设备和工作负载。寻找致力于安全设计原则的合作伙伴。

3. **限制勒索软件攻击者的筹码并制定应对勒索要求的计划：**勒索软件攻击呈增长趋势，CISO 及其董事会需要制定应对方案。根据本项研究的证据，这个方案不应包括支付赎金，因为几乎在每个案例中，选择支付赎金的组织都对其行动感到后悔。我们建议采取的策略是利用 Zero Trust 模型的能力，最大程度减少发生入侵时攻击者进行横向移动的风险。此外，强大的恢复计划将降低攻击者要求的筹码。保障措施始于对最关键的系统和数据进行定期备份，并经过测试以确保其有效性和完整性。定期进行灾难恢复测试对于识别漏洞、增强恢复运营的能力以及减少影响至关重要。

4. **做好应对 AI 助长攻击倍增和加剧的准备：**AI 将被攻击者加以利用，CISO 需要实施适当的 AI 防御策略。网络安全领导者应谨慎对待简单地将问题外包的做法，但确实有必要审视人才模式、治理框架、合规要求和使用监控。现在所有组织都可以采取的一个关键行动是：审查与第三方供应商的合作条款，以确保了解他们在其 AI 模型中如何使用您的数据，且符合您的要求。您当前的安全工具如何应对 AI 攻击的增长？许多 Cloudflare 产品利用我们庞大的全球威胁情报网络来主动抗击新威胁。

5. **将投资从资本转移到运营支出：**大多数组织的预算都面临压力，网络安全领导者需要成为优秀的财务管理者。考虑提升现有团队成员的技能，以符合未来的发展方向，减少复杂性并精简流程。探索重新组织角色的机会，以最大限度地提高效率，同时减少滞后时间。值得考虑的是将一些功能外包给 MSP，将投资从资本支出转移到运营支出。

6. **习惯更多的审查：**网络安全领导者面临着越来越多来自组织内外的审查，对他们本已不小的压力而言犹如雪上加霜。这种审查将持续，CISO 需要努力寻找机会，以遵守不断变化的（本地或国际）法规，并能够满足董事会成员的需求。确保你的审计承诺经过协商，设定明确的范围和时间表，以减少那些对客户没有价值或不能降低风险的任务。

迁移到全球连通云

Cloudflare 提供一种名为“全球连通云”的全新服务，用于连接和保护企业的人员、应用和网络，在提供无处不在的安全方面发挥着至关重要的作用。借助 Cloudflare 广泛的安全产品组合，例如应用、API 和网络安全、Zero Trust 以及全球威胁情报，组织能够加强其数字基础设施防御网络攻击的能力。组织能够确保其在线数据和知识产权的安全，并保护其品牌的完整性。

这些安全服务基于 Cloudflare 的可编程全球云网络服务的统一平台构建。这个平台连接和保护着庞大比例的全球互联网流量，平均每天阻止 1820 亿次威胁。这个全球云网络提供针对网络中断和基础设施故障的冗余和恢复能力，从而最大程度地降低宕机风险并确保高可用性。

如需进一步了解 Cloudflare 解决方案平台，寻求销售代表提供演示，请访问：

cloudflare.com

我们将评估您的当前安全态势，并制定为您的人员、应用、设备、网络和数据加强网络安全的行动计划。

010 8524 1783 | enterprise@cloudflare.com | cloudflare.com/zh-cn