CLOUDFLARE

2025 年

Cloudflare 信号报告

规模化韧性

前言 | MICHELLE ZATLYN

我们生活在一个前所未有的时代。科技正在以令人眼花缭乱的速度进步。

从生成式 AI 的爆炸性崛起——同时带来希望和威胁——到日益无处不在的网络威胁，从高度互联的世界这个新悖论，到给本地社区和全球经济带来的影响，唯一不变的似乎就是变化本身。游戏规则不断变化着，如果我们的应对策略未能持续完善，很快就会过时。

因此，我郑重宣布第一版 ***Cloudflare 信号报告***。该年度报告全面梳理网络安全趋势和关键发现，旨在帮助您制定适合自身需求的战略规划。

Cloudflare 保护着全球 20% 的网站，平均每天阻止超过 2270 亿次网络威胁。这为我们提供了一个非常独特的观察视角。我们看到的不仅仅是数据——我们能够识别出模式、行为和拐点，从中发现未来发展方向。

我们已知的事实：AI 驱动的威胁需要 AI 驱动的防御。Zero Trust 必须成为标准。后量子就绪不是明天的问题，今天就需要得到解决。而且，所有这些都需要高管的参与和支持。**韧性不是可选项：而是不可或缺的。**

Cloudflare 信号报告旨在深入剖析塑造安全格局的各种力量，帮助全球各类规模的企业、政府和个人做出优化韧性的明智决策。

我们的使命是帮助构建更好的互联网，而这从帮助您取得成功开始。

Michelle Zatlyn
联合创始人兼总裁，
Cloudflare

内容摘要

2025年，规模化韧性已不再是可选项——而是衡量领导力的决定性考验。

随着数字威胁日益复杂，地缘政治局势动荡加剧，企业的各个方面——财务、运营、合规和声誉——都面临着更高的风险暴露。AI 驱动的攻击，不断变化的监管框架，以及日益臃肿的数字生态系统，要求高管团队以协调一致的方式做出响应。

《2025 年 Cloudflare 信号报告》重点介绍了必须内置（而非附加）韧性的五个关键脆弱点。它们共同揭示了执行团队面临的新使命：规模化地将韧性嵌入到企业运营、创新和增长的核心中。

精明的企业领导者观察到一个明确的转变：韧性不再是单一职能部门的责任——而是成为整个高管团队共同承担的战略重点。领先企业正在从被动防御转向主动的、情报驱动的和可扩展的技术环境，实现跨业务集成。如果企业将韧性视为高管团队的共同责任和增长驱动力，而非仅仅是保障措施，就将在日益动荡的世界中处于领先地位。

本报告强调了 Cloudflare 的承诺：构建一个安全、高性能和具有韧性的数字生态系统，使各种规模的企业能够承受中断，在全球范围内自信地进行业务运营。

五个关键脆弱点

韧性必须内建于架构之中，而非后期附加。

1

AI 驱动的威胁和内部风险

需要首席技术官 (CTO) 的密切协作，因为攻击者现在利用 AI 来自动化和扩展攻击，其速度远超传统防御的响应能力。AI 驱动的威胁需要 AI 支持的防御，能够实时适应。自动化这些能力不仅可以扩大覆盖范围，还能使组织在不减慢业务步伐的同时扩展其防御能力。

2

Zero Trust、身份保护和云复杂性

需要 CIO 的领导，因为企业已经从基于边界的模型转向身份优先的框架。Zero Trust 已经成为可扩展、云原生风险管理的事实标准——确保跨分布式系统的可用性、可见性和控制。

3

韧性不再是可选项

对 CFO 和 CRO 而言。随着第三方风险增长和监管框架扩展，财务和风险领导者必须确保投资超越风险缓解，推动运营连续性、合规自动化和可扩展的治理。这一层面的韧性必须是主动、嵌入式和具有成本效益的——而非各种单点解决方案的拼凑组合。

4

数据隐私和后量子就绪性

需要 CPO 的早期参与。鉴于量子计算即将攻破传统加密，未来数据保护需要立即采取行动。领导者必须加速采用后量子加密技术，以保护长期数据安全并满足不断发展的监管预期。

5

地缘政治风险和针对性的网络攻击

要求 CEO 和董事会直接参与。随着国家支持的网络攻击行动越来越多地针对领导层、供应链和全球运营，韧性必须扩展到组织最高层——通过实时情报、高管就绪和跨境协调提供支持。

> “AI 驱动的攻击、不断变化的监管框架和日益庞大的数字生态系统，都要求**高管层以协调一致的方式进行应对。**”

内容

1

镜像对抗：在对抗性 AI 时代保护企业

镜像对抗：在对抗性 AI 时代保护企业

AI 驱动的网络威胁正在以前所未有的速度演变，传统安全方法变得毫无用处。现在，攻击者利用 AI 自动化攻击、逃避检测并以超过组织响应的速度利用漏洞。从被动防御转变为主动、AI 驱动的安全防护不再是可选项——而是不可或缺。

AI 驱动的攻击已经造成实际的业务影响。74% 的 IT 安全专业人员表示，AI 驱动的威胁正对其组织产生重大影响[1]。深度伪造诈骗（如虚假视频通话）已导致数百万美元损失，澳大利亚的一个案例甚至造成了 2500 万美元被盗[2]。AI 生成的钓鱼攻击变得更具说服力，而 AI 增强的恶意软件能够适应环境以规避传统防御。

除了直接攻击外，AI 还在助长虚假信息传播、数据投毒和模型操纵，这些都可能危及 AI 驱动的系统。

攻击者生产力提升给安全团队带来巨大压力

许多 AI 使能工具也许不能解锁突破性攻击技术，但这些工具可以帮助攻击者提高生产力、效率和攻击数量。这些工具可加快各种任务的执行速度，例如编写网络钓鱼电子邮件，以及使用“暗黑聊天机器人”来帮助编写恶意软件。

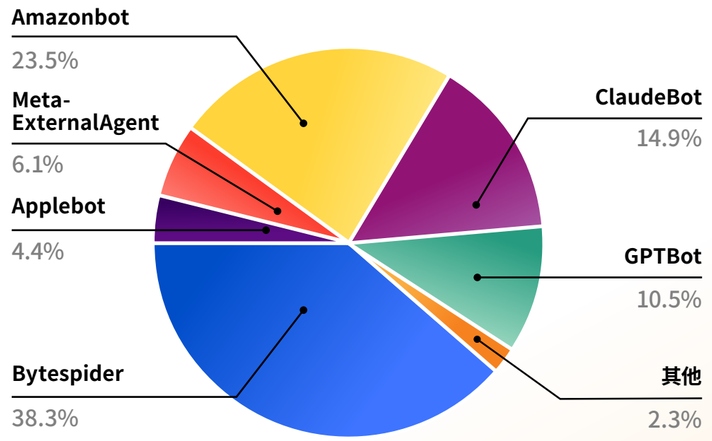
这意味着，组织将开始面临数量更多且更为复杂的攻击，而且这些攻击通常采用现代化的攻击手段。随着攻击数量增加，人工安全流程（如分类处理钓鱼邮件和手动调整检测机制以阻止最新威胁）必然会面临更大压力。

AI 抓取威胁数字内容创作者

AI 模型需要数据进行训练，许多 AI 公司通过自动化网络抓取来收集这些信息。事实上，Cloudflare 网络上处理的所有机器人流量中，AI 爬虫占比已经达到 2%[3]。

AI 衍生内容可能会分散网站的流量和互动，严重损害那些依赖在线内容和广告获取收入的组织。而且反对声音正在增强。2025 年 2 月，教育公司 Chegg 起诉 Google，指控其 AI 功能损害了他们的流量，同时英国创意产业发起了“Make It Fair”（确保公平）活动，反对在未经许可的情况下使用内容[4]。

主要 AI 爬虫在应用层流量中的占比



Cloudflare 在 2024 年观察到的 AI 爬虫流量中，几乎全部 **(98%) 来自 6 家公司**[5]。

对于高度依赖发布数字内容或数字广告的组织而言，**AI 内容抓取机器人是一种事关生存的威胁。**

合成身份欺诈扰乱关键行业

AI 正在助长合成身份欺诈 (SIF) 的兴起，犯罪分子通过混合真实和虚假数据创建高度逼真的身份，以绕过传统验证系统。AI 生成的个人详细信息、深度伪造和自动化凭据填充使这些身份更难被检测，对金融服务、医疗保健和政府机构等重点攻击目标行业构成重大风险。

与传统欺诈不同，合成身份欺诈由于没有立即产生受害者而往往不引人注目，让欺诈者能够建立信用记录并实施大规模诈骗。

AI 增强内部威胁

远程办公和云迁移扩大了内部威胁的攻击面，使其更难检测。超过一半的组织报告在过去一年中遭遇过内部威胁，其中 8% 的组织遭遇了超过 20 起事件[6]。

如今，AI 正在放大这一挑战，为内部人员提供逃避检测的强大工具。AI 支持的网络钓鱼、深度伪造诈骗和自动化社会工程学攻击可在几秒钟内生成令人信服的上下文感知消息，从而更容易实施欺骗，并更频繁地发动攻击[7]。

并非所有内部威胁都是蓄意攻击。Verizon 的 2024 年数据泄露调查报告发现，68% 的数据泄露是由人为因素造成的，例如个人被社会工程欺诈所欺骗或犯错误[8]。AI 辅助的鱼叉式钓鱼攻击利用了这些失误，几乎完美地模仿真实同事或高管，诱骗员工分享凭据、批准交易或泄露敏感数据。

组织必须部署行为分析、实时监控和异常检测，以便在风险升级前发现此类威胁。要在速度和规模上匹敌 AI 驱动的威胁，AI 驱动的安全自动化已经必不可少。

AI 驱动的机器人重塑网络安全格局

AI 驱动的机器人正在增加攻击的复杂性和风险暴露。2024 年，Cloudflare 观察到的所有应用流量中，有 28% 来自机器人，而且这个比例在过去四年里一直稳定在 30% 左右。虽然机器人可以服务合法的目的——如客户服务自动化和搜索引擎索引——但绝大多数 (93%) 未经验证，可能存在恶意[9]。

关键转变是AI驱动的机器人能够以前所未有的效率发动大规模自动化攻击。攻击者现在使用机器人进行凭据填充，发起分布式拒绝服务 (DDoS) 攻击，抓取敏感数据，并以机器速度实施欺诈。AI 模型能够生成逼真的钓鱼尝试、绕过传统验证码 (CAPTCHA) 并利用自适应行为逃避检测，显著增强了上述能力。

如今，要在速度和规模上与 AI 驱动的威胁相匹配，AI 驱动的安全自动化已经变得**不可或缺**。

28%

Cloudflare 观察到的所有应用流量中，有 28% **来自机器人**

高管层需要思考的问题

构建 AI 驱动的防御能力

为了领先于 AI 驱动的威胁，组织需要采取主动方法，以支持实时预防和缓解。**以下是高管可以提出的几个问题，用于评估其组织的就绪程度。**

Q1

我们是否正在使用 AI 驱动全面的安全可观察性？

我们是否正在将日志、分析、警报和取证统一到单一界面中，以识别风险及其根本原因？

Q2

我们是否在利用 AI 驱动的安全来实时检测并消除威胁？

我们是否拥有 AI 赋能的检测手段来分析庞大的数据集、识别异常并自动响应新兴威胁？

Q3

我们针对 AI 驱动的钓鱼攻击、深度伪造和恶意软件的防护程度如何？

我们是否正在部署基于 AI 的检测、防钓鱼身份验证和自适应安全控制来应对不断演变的攻击？

Q4

我们是否正在保护自有数据，防范 AI 数据爬取和自动化威胁？

我们是否实施了机器人管理、API 身份验证和数字水印来防止数据盗窃和利用？

Q5

我们是否在利用 AI 驱动的行为分析来实时检测内部威胁？

我们是否在持续分析用户行为，包括访问模式、权限升级和数据泄露尝试？

高管视角

AI 数据安全的新防护机制

Dane Knecht
Cloudflare
首席技术官

保护 AI 时代的数据：信任、访问权限和可见性

当今组织面临的最紧迫痛点是数据访问权限——具体而言，如何在 AI 工具日益普及的企业环境中管理和保护数据。随着生成式 AI 嵌入到工作流程，挑战不再局限于于应对威胁，还包括防止对敏感数据进行存在风险或未经授权的访问。

这在董事会和高管层面提出了一些紧迫的问题。如何安全地授予工具对企业数据的访问权限？如何确保一个看似无害的 AI 插件不会成为数据外泄的通道？业务和声誉后果切实存在，并在不断扩大。

我们的盲点：Shadow AI 和治理空白

AI 工具在企业内部无序扩散是一个重大盲点。员工远在正式政策出台之前就已经采用 AI，而且往往未意识到潜在风险。这些“影子 AI”部署绕过了传统审查，造成隐蔽的攻击面并引入新的合规风险。

罕有组织全面梳理过企业内部的 AI 使用情况。缺乏这种可见性，就几乎无法管理数据暴露风险，也难以有效响应安全事件。

未来展望：主动控制和强化监管审查

在未来 12 至 18 个月内，企业安全将从被动威胁检测转向针对 AI 访问和使用的主动治理。监管审查将加强——要求透明公开、实施运营监督并遵循严格的数据保护实践。

通过组建跨职能治理团队、制定 AI 使用政策，并为工具和用户实施访问控制，行动迅速的组织将有效降低风险，并树立行业领导地位。

未来的韧性不仅体现在威胁的识别上，更关乎对 AI 访问数据的方式和范围进行控制。

员工**远在正式政策出台之前就已经采用 AI**，而且往往未意识到潜在风险。

2

突破传统边界：Zero Trust、身份和安全新前沿

突破传统边界：Zero Trust、身份和安全新前沿

企业转向多云环境、SaaS 平台和 API 驱动的架构造成了碎片化的安全格局，错误配置、身份风险和影子 IT 使企业面临日益严峻的网络威胁。在这种环境中，Zero Trust 安全模型已经取代了基于边界的过时模型，通过以身份为中心的持续验证方法，成为保障云应用、工作负载和数据安全的基础。

为了跟上步伐，组织必须在云和 SaaS 平台中全面实施 Zero Trust 原则。

Zero Trust 取代传统 VPN

威胁行为者现正积极利用 zero-day 漏洞和暴力攻击手段瞄准 VPN 提供商，以获得网络访问权限[10]。随着网络边界瓦解，企业正在转向以身份为中心的安全模式，在云工作负载和 SaaS 应用中执行持续验证、最小特权访问和基于上下文的身份认证。

Zero Trust 网络访问 (ZTNA) 现已不可或缺，取代使企业易受凭据填充攻击、横向移动和内部威胁影响的传统 VPN。若不实施 Zero Trust，企业将面临未授权访问、凭据泄露和供应链安全漏洞等重大风险。

API：新兴的攻击手段

鉴于目前 60% 的互联网流量基于 API，未受保护的 API 已成为攻击者的主要目标[11]。许多组织未能有效追踪和保护 API，使其面临数据泄露、凭据滥用和注入攻击的风险。Cloudflare 基于机器学习的分析发现，组织报告的 API 端点数量仅为实际数量的四分之一，造成重大安全盲点[12]。

为了降低风险，企业必须采用自动化的 API 发现、身份验证实施和 AI 驱动的异常检测，以防止入侵和数据泄漏。

Cloudflare 基于机器学习的分析发现，**企业报告的 API 端点数量仅为实际数量的四分之一**

影子 IT 和未受管理的云服务加剧了风险

未经批准的云服务快速增加，使 IT 团队日益难以有效监控和保护云环境。员工频繁使用未经批准的协作工具，暴露敏感数据并绕过企业安全策略。

云访问安全代理 (CASB)、AI 驱动的发现工具和自动策略实施现在对于获得实时可见性、确保合规和防止未经授权的数据暴露变得至关重要。

以身份为中心的安全模式：密码时代的终结

随着网络威胁日益复杂，身份依然是主要攻击手段。在 2024 年第一季度，思科 25% 的安全事件响应服务与用户接受虚假多因素认证 (MFA) 推送通知有关[13]。泄露凭据也导致了重大安全入侵事件，例如包括 Santander Group、Ticketmaster 和 Advance Auto Parts 在内的至少 160 家 Snowflake 客户[14]。

网络犯罪分子越来越多地绕过 MFA、劫持活动会话并窃取凭据，使企业面临大规模的入侵和帐户接管风险。

Challenge:

- **凭据复用使企业面临风险**——所有人类登录尝试中，46% 涉及凭据泄露，企业中这一比例上升到 60%[15]。攻击者自动化凭据填充，即可轻松获得对企业系统的访问权限。
- **自动凭据填充攻击的规模正在迅速扩大**——使用泄露凭据的登录尝试中有 94% 来自机器人，每秒测试数千个被盗密码[16]。如果没有实时机器人缓解和自适应身份验证，组织仍然非常容易遭受大规模入侵。
- **密码已不再足够**——面对现代威胁——包括 MFA 绕过、会话劫持和防钓鱼凭据盗取，静态密码，甚至基本的 MFA 方法均越来越无效。为了应对这些风险，组织必须采用无密码身份验证，执行 Zero Trust 访问控制，并部署符合 FIDO2 标准的安全密钥来消除对静态凭据的依赖。

46%
的人类登录尝试涉及**泄露凭据**

94%
使用泄露凭据的登录尝试来自机器人，每秒测试数千个被盗密码

高管层需要思考的问题

保障云端安全，重新思考身份验证

随着云计算加速，组织必须重新思考安全和身份验证，以防范不断演变的威胁。Zero Trust 方法、AI 驱动的可见性和强大的身份保护对于保护云服务、SaaS 应用和 API 至关重要。**请考虑以下问题，确定贵组织在应对这些挑战方面的积极程度：**

Q1

我们是否对云服务、SaaS 应用和 API 实施了 Zero Trust 安全策略？

我们是否在所有环境实施了持续验证、最低特权访问和基于风险的身份验证？

Q2

我们是否对影子 IT 和未受管云服务有完全的可见性？

我们是否在使用 AI 驱动的发现工具来检测未经授权的应用并执行安全策略？

Q3

我们的 API 是否采取了安全措施来防止未授权访问和数据泄露？

我们是否实施了自动化 API 发现、身份认证控制和 AI 驱动的异常检测？

Q4

我们是否消除了身份验证策略中基于密码的漏洞？

我们是否采用了无密码身份验证、防网络钓鱼的 MFA 和自适应身份保护？

Q5

我们是否已准备好检测和应对自动化凭据填充攻击？

我们能否部署 AI 驱动的机器人缓解、行为分析和自动凭据撤销来防止未授权访问？

高管视角

Zero Trust 构建韧性未来

Corey Mahan
副总裁，产品管理，
Cloudflare

目前，组织面临的最大挑战是平衡安全性和可用性。混合办公将成为常态，云采用正在加速，用户期望无摩擦的访问——无论他们身在何处或使用什么设备。但传统架构已无法跟上这一步伐。我们发现太多的企业依赖于单点解决方案的拼凑组合，其难以扩展，导致中断、延迟和用户沮丧。

高管们提出了一个关键问题：我们如何在不降低业务效率的情况下提供安全访问？这种压力正推动 Zero Trust 成为焦点——不仅仅作为一种安全模型，更是业务使能器。

常见误区

许多组织初衷是正确的，但很快就陷入停滞。一个常见的误区是认为购买 “Zero Trust 解决方案” 就等同于实施一种战略。事实并非如此。Zero Trust 是一种思维方式和架构转变。

另一个问题是误认为统一就意味着集成——许多所谓的平台实际上只是简单拼凑起来的产品，互相之间不共享数据、策略，甚至后端系统。这会造成盲点，尤其是在云 API、DevOps 流水线和 AI 应用等现代环境中。

然后还有影子 IT 和影子 AI，员工在使用这些工具，但 IT 团队毫不知情，造成了严重的治理空白。

未来展望（12-18 个月）

在未来一年左右，我们将看到 Zero Trust 从孤立的控制措施演进为覆盖整个企业的基础性架构层。重点将从单纯的安全远程访问管理转变为统一所有环境的身份、数据和流量策略。企业领导者正在转向具有以下特征的平台：固有韧性、默认全球化、自动化响应，并提供实时可见性。这就是真正的价值所在：不仅仅降低风险，还赋予了敏捷性。

取得成功的组织将是那些将 Zero Trust 嵌入其数字基础中的组织，使其成为安全构建、扩展和创新的一部分。

一个**常见的误区**是认为购买‘Zero Trust 解决方案’就等同于实施一种战略。”

3

更强大，不仅更安全：扩展保护以覆盖基础设施、生态系统和监管

更强大，不仅更安全：扩展保护以覆盖基础设施、生态系统和监管

构建覆盖网络、供应链和合规框架的韧性，对于维持运营完整性和竞争优势至关重要。

然而，当今的网络威胁（如 DDoS 攻击）速度更快、规模更大、更复杂——传统防御措施已经无法应对。与此同时，数字供应链暴露了隐藏的漏洞，而监管环境变得要求更严格、更分散。

为了保持竞争力，组织必须将网络安全从 IT 问题重塑为业务韧性战略——覆盖基础设施、生态系统和监管。

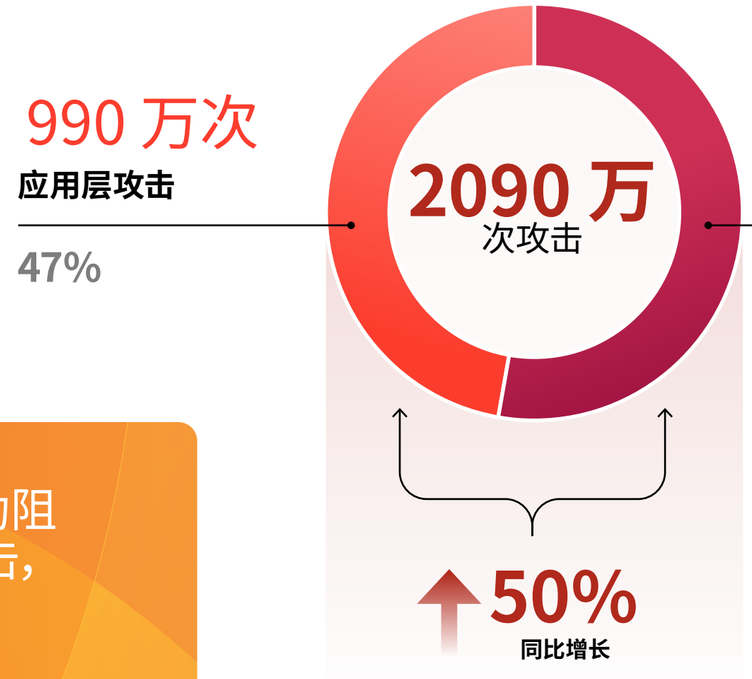
DDoS 攻击的规模和复杂性正在攀升

DDoS 攻击已演变为网络犯罪分子、黑客分子以及国家级攻击者用以扰乱业务运营、制造合规风险和声誉损害的精准工具。DDoS 攻击正在重创各行各业。2024 年，Cloudflare 成功阻止了 2090 万次 DDoS 攻击，较 2023 年增长 50%[17]。

DDoS 攻击的规模与复杂性持续升级，攻击者正利用僵尸网络、物联网 (IoT) 设备和 AI 驱动的自动化技术，对关键数字服务发起持续、高影响力的攻击。

2024 年，Cloudflare 成功阻止了 2090 万次 DDoS攻击，比 2023 年增长了 50%

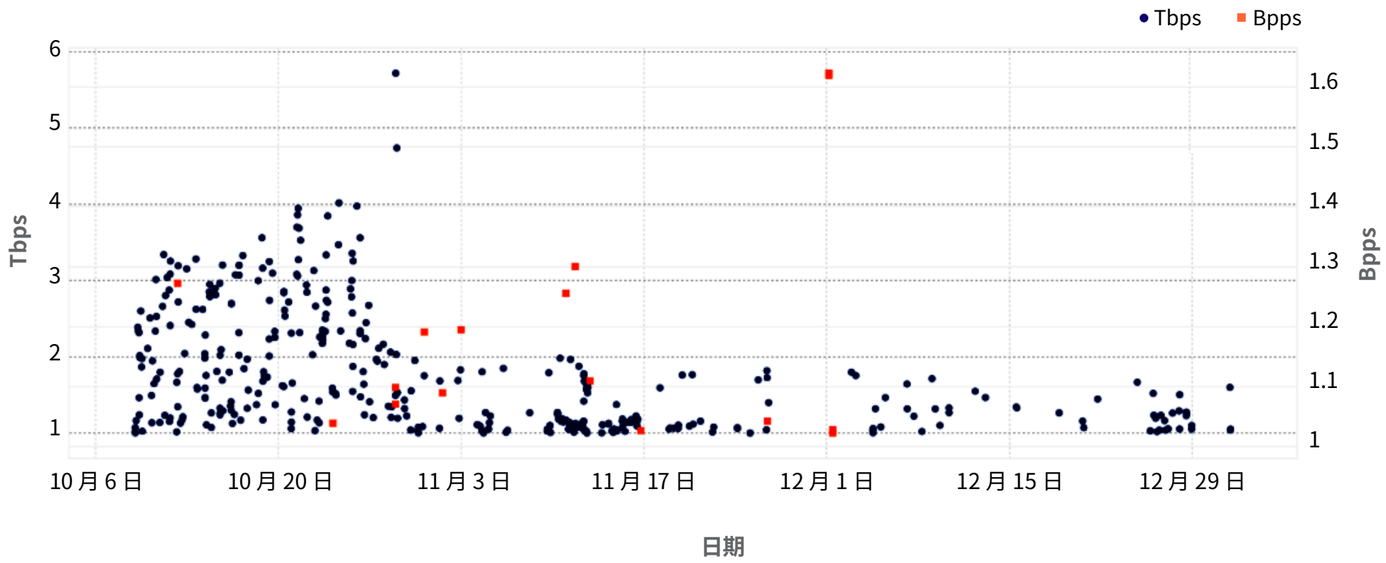
2024年 DDoS 攻击数量



超大容量 DDoS 攻击崛起

2024 年第四季度

2024 年第四季度，超大规模网络层攻击激增到前所未有的水平。超过 1 Tbps 的攻击数量环比激增 1885%，超过 1 亿 pps 的攻击环比增长 175%。值得注意的是，在超过 1 亿 pps 的攻击中，有 16% 也超过 10 亿 pps，凸显了现代 DDoS 威胁的强度和规模不断增长[18]。



Cloudflare 数据显示，平均每个企业和组织使用**至少 20 个第三方脚本**

供应链攻击不断升级

根据世界经济论坛的数据，54% 的大型企业认为第三方风险管理是他们的头号网络韧性挑战[19]。针对软件供应链、云平台和第三方集成的攻击急剧增加；在 2024 年，有 15% 的泄露涉及第三方[20]。

雪上加霜的是，风险正日益集中在少数几家占主导地位的云服务提供商中。这些提供商中的单一漏洞或服务中断可能会在各行业产生连锁反应——2024 年的重大 IT 服务中断就是明证，这些事件造成了数十亿美元的损失，并暴露了超互联数字生态系统的脆弱性。这些事件清楚地提醒我们，在当今相互依赖的环境中，一个单点故障就可能使整体运营陷入停滞。

一个特别脆弱的领域是客户端攻击，因为企业通常依赖第三方脚本来加速 Web 应用开发。这些脚本是嵌入的代码（通常是 JavaScript），来自外部服务器。

这些脚本提高效率的同时，也造成了重大的安全漏洞：每一个与外部函数的连接都会增加基于浏览器的供应链攻击的风险。

Cloudflare 的数据显示，平均每个企业组织至少使用 20 个第三方脚本，而有些组织更是不知不觉中使用了数以万计的脚本，每一个脚本都可能成为攻击者的潜在入口。

一家大型电子商务企业的网站挂载了超过 34 万个第三方脚本[21]。

欧盟的网络韧性法案和支付卡行业数据安全标准 (PCI DSS 4.0) 等法规有助于解决供应链安全问题，但执行仍然存在挑战。

网络安全法规不断增加

网络安全法规正以迅速的步伐扩张，对企业提出了更高的要求，以增强安全性、透明度和事件报告。美国证券交易委员会 (SEC) 现要求上市公司披露重大网络安全事件，并详细说明其风险管理策略。欧盟《通用数据保护条例》(GDPR) 仍然是最严格的数据隐私法之一，对违规行为处以最高全球收入 4% 的罚款。澳大利亚审慎监管局 (APRA) 的 CPS 234 要求金融机构维护强健的信息安全措施，而欧盟的数字运营韧性法案 (DORA) 则为金融行业制定了统一的网络安全标准。

换言之，合规性已不再是事后考虑的问题。要成功应对这一形势，组织需要将合规性嵌入其运营中，并利用自动化技术简化报告流程，确保持续符合不断发展的法规要求。

持续推进合规自动化

合规自动化正成为关键趋势，因为组织面临日益增加的监管复杂性和运营风险。仅在美国就有超过 52 项网络事件报告要求现已生效或处以提案阶段，而全球框架——如 GDPR、DORA 和 PCI DSS 4.0——正在扩大适用范围，因而人工合规流程已难以为继[22]。德勤的一项调查发现，62% 的全球组织计划增加对合规自动化的投资，主要原因包括监管碎片化以及对实时响应的需求[23]。

为满足司法辖区的数据要求且不影响性能，企业正采用战略性数据本地化方案，通过区域节点路由流量，并部署自动化审计工具以验证合规性。与此同时，合规与安全之间的界限正变得日益模糊——企业正在实施集成框架，以统一威胁检测、策略执行和审计就绪性。

这种融合使企业能够降低风险、更快响应监管变化，并实现跨境治理的扩展。实现合规自动化和运营化的组织将获得战略优势——加速进入受监管市场，增强客户信任，并最大程度降低财务和声誉风险。

不断发展的监管环境

网络安全和数据保护的全球监管框架持续快速演进，组织现在需要在多个司法辖区应对错综复杂的合规要求。

例如：

SEC 网络安全规则

美国证券交易委员会对上市公司实施了全面的网络安全披露要求。这些规则要求及时报告重大安全事件，并详细披露风险管理策略、治理和专业知识。

NIS2

欧盟的 NIS2 指令在 18 个关键领域设定了更严格的安全要求。它要求采取韧性、风险管理、事件响应和报告措施，并加强监督和对不合规行为的处罚。

APRA CPS 234

澳大利亚审慎监管局 (APRA) 的 CPS 234 信息安全标准要求金融机构保持与其信息资产规模和威胁程度相匹配的强健信息安全能力。

DORA

DORA 代表了欧洲在金融领域实现数字运营韧性的综合方法。它为支持金融实体运营的网络和信息系统的安全性提出了统一要求。

高管层需要思考的问题

重新定义连续性与合规性

在由大规模 DDoS 攻击、不透明的供应链和复杂的全球法规塑造的威胁环境中，真正的韧性已经超越防御。这意味着设计能在压力下持续运行的系统，并将合规视为既是保护盾，又是战略使能器。**这五个问题将帮助首席执行官评估组织应对和适应中断的就绪情况。**

Q1

我们的基础设施是否能够承受大规模 DDoS 攻击，并在压力下维持正常运行？

缓解能力应超过峰值合法流量和有记录的最大规模攻击。具有韧性的组织部署地理冗余基础设施，制定合规感知的故障转移方案，并定期测试恢复程序，以确保服务正常运行和监管合规性。

Q2

我们是否对最关键的第三方依赖关系拥有实时可见性？

供应链漏洞是导致安全事件的一个主要原因。具有前瞻性的组织持续监控外部供应商和服务，强制执行合同安全要求，并将第三方风险洞察整合到更广泛的治理流程中。

Q3

我们是否自动化了合规工作流程以跟上全球法规的步伐？

鉴于监管框架众多且发展迅速，手动合规方法无法扩展。高绩效企业采用自动化审计、实时监控和感知司法管辖区的数据路由，以实现持续合规并降低运营开销。

Q4

我们的安全和合规功能是否完全整合？

孤立的团队导致效率低下和漏洞。统一平台使威胁检测与监管报告保持一致，简化审计流程，改善可见性，并降低整体风险。

Q5

我们是否已全面测试了组织的韧性态势——从事件检测到恢复和报告的整个流程？

积极主动的组织制定将技术控制与法规要求相关联的行动手册，定期模拟中断场景，并调整合规架构以支持跨司法辖区的扩展。

高管视角

有关就绪度的新规则

Emily Hancock
首席隐私管，
Cloudflare

保障未来：监管、风险和就绪度

网络安全监管正在进入一个新时代，要求更严格、审查力度更大、问责更广泛。从 SEC 的强制事件披露要求，到 GDPR 严厉的隐私违规处罚，以及 DORA 和 APRA CPS 234 等新标准，全球监管机构正在提高对数据保护、运营连续性和透明度的期望。对高管团队而言，合规不再只是一项法律义务，而是一个战略优先事项。

与此同时，新兴技术和不断演变的威胁模式正在挑战传统的安全方法。随着创新加速，监管机构和利益相关者也更加关注长期风险管理，尤其是敏感数据方面。组织必须证明他们不仅能够保护当前的资产，还能保护将支撑未来数字信任的数据和系统。

我们的盲点：误解与被忽视的空白

许多组织机构仍将安全和合规视为孤立的职能，由技术团队管理，缺乏跨职能协同。这造成了盲点，尤其是在理解敏感数据存储位置、加密应用方式以及第三方系统中的漏洞分布方面。

若缺乏明确的资产清单和治理框架，企业将面临落后于监管机构和攻击者的风险。

另一个空白是数据最小化。企业往往留存不再需要的个人数据，这种做法增加了暴露风险，而没有带来任何业务价值。嵌入隐私设计原则——限制数据收集、自动删除和在架构级别内置控制——可降低风险并提升合规性。

未来展望：向嵌入式合规转变

在未来 12-18 个月内，我们预计监管机构和标准机构将更加重视主动、可验证的安全实践。这包括加强对数据治理、加密和第三方风险的控制。及早行动的企业——通过采用集成平台、自动化合规工作流程并将安全嵌入核心运营——将降低复杂性，避免代价高昂的补救，并将自身定位为值得信赖的领导者。

转变显而易见：合规、连续性和安全必须从一开始就纳入设计。内化这种思维方式的组织不仅能跟上监管步伐，还能领导一个要求问责、透明和信任的世界。

“若缺乏明确的资产清单和治理框架，**企业将面临落后于监管机构和攻击者的风险。**”

4

破解密码：量子时代面向未来的隐私保护

破解密码：量子时代面向未来的隐私保护

量子计算有望给科学和工业带来变革性进步，但它也对数字安全构成根本性威胁。一旦大规模量子系统成熟，将能够破解目前广泛用于保护互联网安全的公钥密码系统。其中包括 TLS 加密、VPN、代码签名和区块链系统。

这种威胁并非假设性的。威胁行为者现在已开始收集加密数据，押注未来的量子计算机将能够进行破解——这一策略被称为“现在收集，日后解密”。随着后量子密码学的采用加速，对密码系统的可见性、自动化策略执行以及明确的迁移路径将定义组织的安全就绪状态。

量子威胁已经成为现实

美国国家标准与技术研究院 (NIST) 警告，组织应立即行动，以避免措手不及[24]。国家级行为者和复杂的对手正在主动收集加密通信、知识产权和国家机密，意图在未来破解。需要长期 (十年或更长) 保密的通信——如医疗记录、军事情报和法律合同——如果未使用抗量子密钥协商方案，则已处于脆弱状态。

PQC 采用有所激增，但依然存在空白

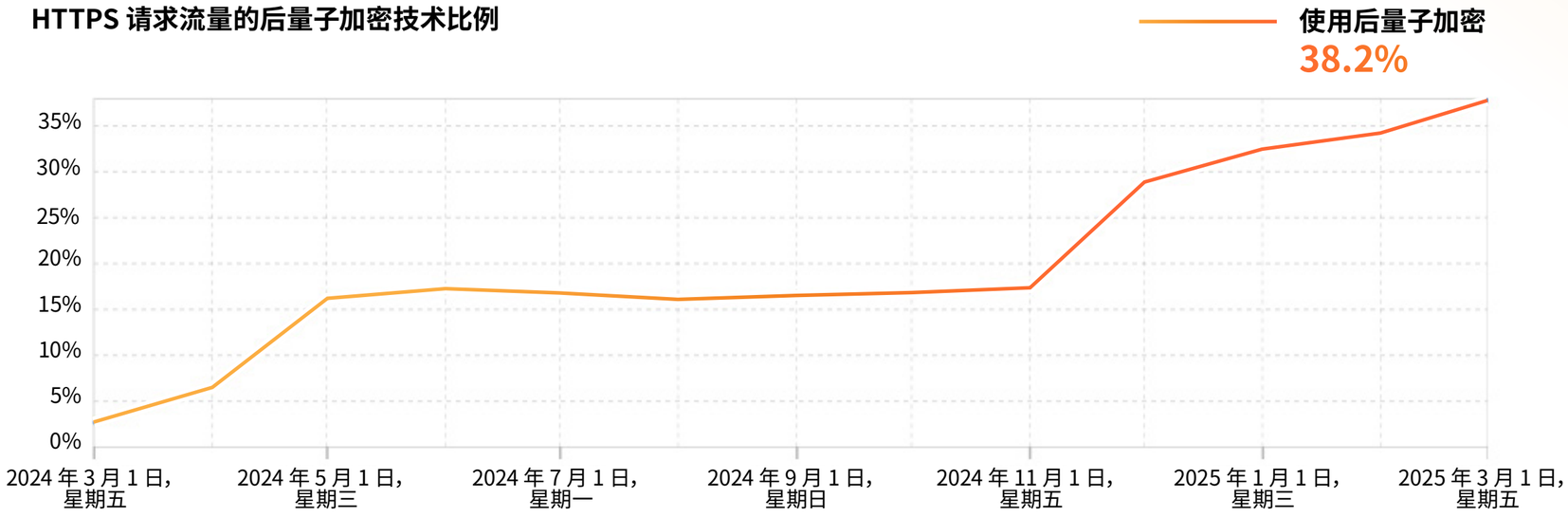
后量子加密(PQC) 已从理论研究进入生产实施。包括 Cloudflare 在内的主流科技公司在采用 PQC 方面处于领先地位。

2024 年初， Cloudflare报告称，只有 3% 的 HTTPS 流量是使用后量子算法加密的。到 2025 年 3 月，Cloudflare 推出默认混合后量子 TLS 以及得到 Chrome、Edge 和 Firefox 浏览器支持后，这个数字上升到 38%[25]。

尽管如此，采用情况并不平衡。大多数企业环境仍处于探索或试点阶段，密码系统无序扩张导致转型复杂化。如果企业未能优先考虑抗量子加密，就可能落后于监管要求，并使其数据暴露于长期漏洞。

后量子加密在全球的采用情况

HTTPS 请求流量的后量子加密技术比例



量子迁移战略规划

1

首先记录使用加密的所有地方。

创建迁移项目列表，并按风险和工作量进行优先级排序。

立即将后量子就绪性纳入供应商评估流程。

2

在采用最新标准方面，供应商之间存在差异。验证供应商的加密敏捷性，尤其是为企业网络流量提供隧道传输的 Zero Trust 供应商。

3

优先考虑密钥协商机制迁移。

鉴于“现在收集、日后解密”的威胁，确保当前密钥协商机制具备抗量子能力具有明确的优势。供应商已基本达成共识，即改造 TLS 1.3 以支持 X25519MLKEM768：传统椭圆曲线 X25519 与后量子 ML-KEM（基于模格的密钥封装机制标准，FIPS 203）的混合方案。

签名迁移应文档化，但目前暂不作为重点。

企业仍在努力就后量子签名迁移的最佳方案达成共识。幸运的是，后量子签名主要是防止主动式路径攻击，因此此类迁移的优先级较低。

4

加密可见性和 XDR 驱动的自动化将加速转型

量子迁移不仅仅是部署新算法，更在于了解密码学在不断日益臃肿的环境中的分布位置。其中包括嵌入式系统、云工作负载、传统应用、API 和 IoT 设备。使用具有深度网络和终端遥测能力的扩展检测与响应 (XDR) 平台的安全团队，能更好地发现过时的密码学、检测不安全的回退行为，并自动化补救工作流程。

供应商加密敏捷性将成为一个风险差异化因素

监管机构（如 NIST、BSI、ANSSI）开始推荐或强制要求密码学敏捷架构。企业将在招标文件和供应链审计中日益重视后量子就绪性评估。然而，并非所有供应商都取得同样的进展。未能支持混合加密或量子安全加密的供应商可能面临被淘汰的风险——尤其是在政府、金融服务和国防等领域。

高管层需要思考的问题

为防范量子风险做好准备

鉴于攻击者采用“现在收集、日后解密”的策略，切监管机构推进后量子强制要求，组织必须立即开始着手准备。提前启动这一转型的高管，不仅将为基础设施提供面向未来的保护，还将在信任、合规性和韧性方面获得战略优势。**回答以下问题，评估您在即将到来的量子风险时代的就绪情况：**

Q1

我们是否完全了解企业环境中使用加密的地方——从云和应用，到嵌入式系统和第三方工具？

加密系统往往是深度嵌入且缺乏文档支持。如果缺乏完全可见性，组织可能面临关键系统不受保护的风险，或在不知不觉中暴露于量子时代的威胁之中。

Q2

我们是否优先迁移到后量子密钥协商机制，特别是对于保护敏感或长期数据的系统？

“现在收集、日后解密”攻击的目标是必须保密多年的数据。迁移密钥交换机制（如 TLS 握手）是确保未来保密性的关键步骤，具有高影响力，且时间敏感。

Q3

我们的检测和资产监控工具是否能够识别企业中过时或易受量子攻击的加密技术？

XDR、SIEM 和资产发现平台应该帮助检测加密偏移、遗留库和回退协议。这对于防止错误配置和指导迁移优先事项至关重要。

Q4

作为采购和风险审查流程的一部分，我们是否评估了供应商和合作伙伴的加密敏捷性？

缺乏后量子就绪路线图的供应商可能会成为薄弱环节。将 PQC 一致性纳入尽职调查有助于减少下游风险，并确保长期韧性。

Q5

我们是否有一个分阶段的、基于风险的迁移策略，其中涵盖治理、自动化和高管可见性？

后量子迁移是一个复杂、跨越多年的过程。具有问责制的明确路线图、部署自动化以及进度实时指标，对于保持势头和董事会层面的信心至关重要。

高管视角

突破密码学迷障

Wesley Evans
高级产品经理，
Cloudflare

组织面临着加密复杂性激增的问题。这个领域曾经有数个定义明确的标准，如今已变成一个碎片化的算法和部署模型生态系统。这种快速演进，加之监管和运营方面要求采用量子安全加密的压力不断增加，已在企业层面造成了混乱。

领导者被告知要拥抱密码敏捷性并为量子韧性做准备，但大多数缺乏对密码技术使用位置和方式的明确清单。缺乏可见性，规划将沦为猜测。预算停滞。所有权界定不清晰。因此，即使在充分了解风险的情况下，高管也很容易降低行动的优先级。

常见误区

一个重大盲点是假设组织尚未遭到入侵。“现在收集、日后解密”攻击真实存在且活跃，尤其针对具有长期价值的数据，例如医疗记录、知识产权和国家安全信息。如果您的数据属于这些类别，则其可能已经落入威胁行为者手中，只待解密能力到位。

另一个误解是，量子风险将有一个明确的里程碑，例如 Shor 算法取得公开突破。但攻击者并不需要立即取得成果。

如果破解一个密钥需要数周或数月时间，而且回报很可观，他们就会进行这项投资。这种感知的滞后导致了一种危险的自满。

未来方向

两个转变正在迅速逼近。首先，量子纠错技术的进步将使量子解密的威胁从理论转变为现实。这将引发来自监管机构、董事会和公众的更大压力。其次，企业将开始推出加密敏捷系统。这意味着最终全面盘点加密的位置、使用方式和所有权归属。

这并非易事。大多数团队面对这一情况，犹如一次拖延已久地“就医”，预料将要经历不适、成本和意外挑战。但等待只会使情况变得更糟。当前的重点不是一夜之间更换所有系统，而是建立可见性、明确责任归属并启动升级过程。提前行动的组织将最有利地应对后量子时代的转型，在危机来临前做好准备。

“量子纠错的进步将使**量子解密威胁**从理论变成现实。”

5

改变平衡：
治理、地缘政治和伦理

改变平衡：治理、地缘政治和伦理

随着全球权力格局的变迁，网络安全、地缘政治和伦理的交叉领域正重新定义领导者的责任。如今，网络攻击已演变为地缘政治影响的工具，监管机构正追究高管个人责任，而人工智能 AI 引入的伦理困境正严峻挑战传统监管模式。

随着美国证券交易委员会 (SEC) 于 2023 年要求快速披露网络安全事件，以及国家支持的网络行动被广泛报道，企业领导者必须将健全的治理机制、透明的 AI 伦理和敏捷的风险管理融入其战略。

安全治理从指导转向问责

监管监督正在收紧。2023 年，美国证券交易委员会 (SEC) 要求上市公司在四日内披露网络事件，标志着向强制问责的转变。目前，近 72% 的公司在董事会优先考虑网络安全专业知识，71% 的企业在至少一位董事具有网络安全背景，而 2018 年这一比例仅为 34%[26]。董事会日益认识到，忽视网络安全可能导致严重的运营、法律和声誉后果。

地缘政治和网络战直接影响企业

国家行为者和黑客激进组织正日益将网络行动用作战略武器。近年来，国家支持的网络活动针对金融、能源和科技等关键行业，旨在破坏全球供应链并影响市场动态。例如，具有政治动机的威胁行为者 LameDuck 在一年内发起了超过 3.5 万次得到证实的 DDoS 攻击，导致包括 Microsoft、OpenAI 和斯堪的纳维亚航空 (Scandinavian Airlines) 等组织的运营中断[27]。即使是表面上中立的组织，也可能被卷入地缘政治冲突之中。

高管必须被视同攻击面对待

C 级高管面临直接的网络安全威胁。备受关注的深度伪造诈骗和高管身份冒充计谋呈指数级增长，据报道，数位首席执行官在旨在误导利益相关者的欺诈性音频和视频消息中被假冒[28]。

此类事件凸显了领导层在网络风险以及针对性的声誉和财务攻击面前是多么脆弱。

监管碎片化和供应链不确定性正在加剧

全球企业现正面临错综复杂的网络安全、AI 及数据主权法律环境。贸易限制和出口管制迫使企业重新评估供应商关系并重新配置供应链。例如，不断变化的关税和欧盟的 NIS2 指令破坏了既有供应链协议，增加了合规成本和运营延迟风险。

AI 伦理和影子 AI 需要规模化治理

生成式 AI 在工作场所中的爆炸式增长正在超出组织的控制。麦肯锡的报告指出， 现有 65% 的公司在至少一个业务职能中使用生成式 AI，而在 2023 年这一比例仅为三分之一[29]。Cloudflare 的 AI Gateway 在 2024 年 10 月至 2025 年 2 月期间处理了超过 50 亿个请求，短短五个月内增长了 60%[30]。采用速度非常快：2025 年 1 月，DeepSeek AI 跻身 Cloudflare Radar AI 服务排名的第三位，距离其 R1 模型发布仅九天[31]。

这种自发式采用加速了影子 AI 的兴起，即员工在缺乏监管的情况下使用未经授权的 AI 工具。这些工具带来严重风险：数据泄露，监管违规，以及将敏感信息暴露给公共 AI 模型。

为应对这一挑战，企业需要超越基本的政策声明。有效的治理需要建立明确的审批框架、提示词日志记录、URL 过滤以及使用情况监控。若无积极执行，AI 伦理和安全将沦为空谈。

国家行为者和黑客激进组织正日益将网络行动用作**战略武器**。

高管层需要思考的问题

应对道德和地缘政治风险

随着网络威胁日益政治化、AI 伦理日趋复杂以及监管预期收紧，高管团队必须超越技术性控制。**以下问题可帮助领导者评估其治理、情报和响应策略是否适应领导层本身已成为威胁面一部分的世界。**

Q1

我们是否已在董事会层面为安全和数字韧性明确了问责制，包括清晰度的职责分工和具备网络安全素养的领导层？

鉴于监管机构现在要求高管个人承担责任（正如美国证券交易委员会的快速披露要求所示），确保董事会具备网络安全专业知识对于降低法律和声誉风险至关重要。

Q2

我们是否持续监测地缘政治变动及其对威胁态势的影响，包括国家支持的网络攻击和黑客活动分子活动？

鉴于近期国家支持的网络攻击行动正在破坏供应链并瞄准关键市场领域，获取有关地缘政治风险的实时情报对于保护全球运营和领导层均至关重要。

Q3

我们是否已就针对高管的攻击（如深度伪造诈骗和身份冒充活动）制定了主动响应计划？

鉴于领导层面临来自 AI 驱动的虚假信息和身份冒充的风险日益增长，响应策略必须包括针对性的事件响应流程和持续的声誉管理措施。

Q4

我们的政策和安全控制措施是否足够完善，能够检测和管理员工队伍中未经授权使用 AI 的情况？

鉴于越来越多组织利用生成式 AI，且影子 AI 事件不断增加，精细化的监控和严格指南的执行对于防止数据泄露和确保合规性至关重要。

Q5

我们是否正在调整我们的网络安全和 AI 战略，以适应不断演变的数据主权和 AI 伦理相关地区法规，我们是否将这种一致性作为战略优势？

不同的监管框架——如欧盟 NIS2 指令和区域数据主权法律——要求安全策略既具有敏捷性，并有前瞻性。这种一致性既可降低法律风险，又可增强市场信任和竞争优势。

高管视角

多重危机世界中的治理和问责

Ramy Houssaini
首席网络解决方案官，
Cloudflare

企业和组织必须应对地缘政治、经济和技术风险交汇的多重危机格局。美国证券交易委员会的网络事件披露规则体现了从网络安全指导方针到高管问责制的转变。组织必须发展实时入侵检测和响应能力。违规可能面临严厉处罚，而声誉损失会损害利益相关者的信任。董事会必须融入网络安全专业知识和主动风险管理，以保持韧性。

盲点：地缘政治、AI 和供应链风险

一个关键盲点在于低估了地缘政治网络威胁。许多企业假设自身保持中立，然而国家支持的攻击正日益扰乱金融、科技和能源行业，使供应链处于脆弱状态。

另一个被忽视的风险是影子 AI，即在没有监督的情况下使用未经授权的 AI 工具。如果没有强大的监控，敏感数据可能面临暴露风险，导致监管处罚和竞争劣势。

此外，第四方和第五方供应商也会带来隐藏的漏洞。企业专注于直接供应商，而扩展供应商生态系统往往缺乏可见性，使企业容易遭受网络威胁和运营中断。

未来发展和战略准备

在未来 12-18 个月，组织应该预期：

- **监管扩张：** 欧盟的 NIS2 指令和类似框架将强化合规要求。企业领导者必须建立监管专项工作组以保持领先。
- **AI 治理加速：** 影子 AI 激增，监管机构将实施更严格控制。企业必须实施监控和治理框架以降低风险。
- **针对高管的攻击：** Deepfake 诈骗和冒充攻击将变得更加复杂，欺诈和错误信息的风险将增加。组织应部署 AI 驱动的检测系统，并加强高管安全培训。
- **供应链韧性：** 网络威胁和地缘政治不稳定将继续影响供应链。企业必须加强风险评估，履行安全义务，并改善供应商监控。

要在当前的多重危机时代取得成功，领导者必须将网络安全纳入治理，评估地缘政治风险，强化 AI 监管，并构建具有韧性的供应链。敏捷性和卓越的风险管理将对于应对不断演变的法规和确保长期稳定至关重要。

“董事会必须**融入网络安全专业知识和主动风险管理**，以保持韧性。”

总结

构建规模化韧性的高管团队举措

网络安全的性质已经发生了变化，其影响已渗透到企业的每个角落。在 2025 年，AI 驱动的攻击、地缘政治风险、监管复杂性和供应链相互依赖性要求采取协调、跨职能部门的响应。保障未来发展不仅仅意味着对威胁做出反应；它还意味着将韧性嵌入组织的运营、创新和增长方式中。这些行动号召旨在让 CXO 齐心协力，将韧性作为一种战略能力来打造。

1 使韧性成为共同的战略使命

通过确保高层管理团队在安全态势、资源分配和应急规划上达成共识，建立跨职能的网络安全责任体系。韧性不是一个团队的工作——它是一种企业能力，必须跨职能部门和地区扩展。

2 自动化和集成以确保可扩展性

人工合规流程和碎片化的防御无法及时应对 AI 驱动的威胁和不断扩大的监管要求。投资于针对威胁检测、合规工作流程和事件响应的自动化。集成合规、风险和安全工具，以消除孤岛并提升可见性。

3 将网络治理重新定位为竞争优势

随着高管问责制兴起，确保企业董事会和高管团队具备网络安全素养，并为数字风险监督设立正式岗位。将网络风险嵌入企业风险框架，把监管一致性视为竞争差异化因素。

4 立即构建面向未来的能力，不要推迟

立即开始您的后量子 (PQC) 加密迁移和 AI 治理准备。犹豫不决的领导者将面临“现在收集、日后解密”威胁，或者 AI 无序扩张。可见性、供应商加密敏捷性和分阶段迁移策略是关键。

5 规模化测试以寻找潜在故障

韧性不在于避免故障，而在于发生故障时维持运行。模拟现实世界的危机——从超大容量 DDoS 到内部滥用或针对高管的攻击——并对您的检测、遏制和恢复能力进行压力测试。在您的模拟场景中纳入合规、通信和供应链因素。

6 在攻防中整合 AI 技术

AI 不应再仅被视为是一种工具，而是高管团队的一种战略能力，推动整个企业的敏捷性、韧性和创新。通过利用 AI 驱动的洞察力，企业能够快速适应市场变化，预见风险，并优化实时决策。

AI 可自动化威胁检测、简化危机响应和强化网络安全态势，有效应对不断演变的风险，从而增强韧性。此外，通过发掘新的收入来源，加速研发进程，并大规模个性化客户体验，AI 有力推动了创新。随着 AI 深度集成到核心业务职能中，其将提升企业的适应能力并为未来做好准备，使领导者能够自信地应对复杂性。

这些行动号召旨在让高管团队**齐心协力将韧性作为一种战略能力来打造。**

保障未来发展不仅仅意味着对威胁做出反应，还需要积极应对。**这意味着将韧性嵌入组织的运营、创新和增长方式中。**

Resilience@ Cloudflare: 构建可扩展未来的基础

RESILIENCE@CLOUDFLARE

可编程的单一网络
与众不同

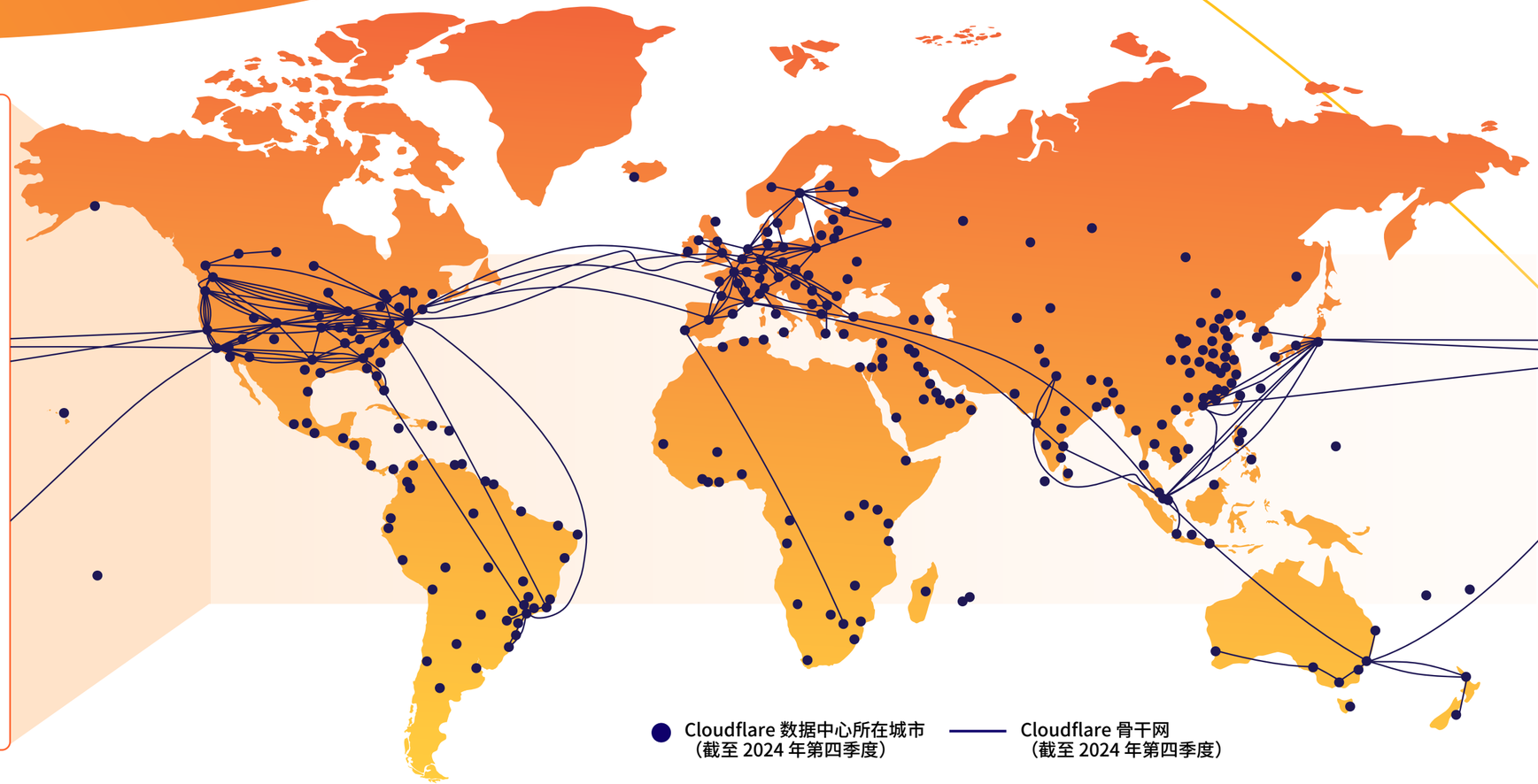
335+ 城市
遍布 125+ 国家/地区，包括中国大陆

↳ **其中 180+ 城市**
提供基于 GPU 的 AI 推理

~50 毫秒
触及全球 95% 互联网用户

约 1.3 万个网络
直连 Cloudflare，包括 ISP、云服务提供商和大型企业

348 Tbps
网络容量并在持续增长中



RESILIENCE@CLOUDFLARE

Cloudflare Workers

开发人员构建和扩展 AI 推理和智能体的最佳平台

成本和可扩展性

灵活扩展，可缩减至零

在 GPU 上运行 AI 模型，而无需提前数月为峰值期预置资源付费。仅需按使用量付费。

无计算 = 无使用费

基于计算的定价意味着，当函数空闲和等待 I/O 时，不会产生费用。（应用等待 I/O 的时间可能 **10 倍**于实际 CPU 使用时间。

性能

部署到全球

代码执行位置与全球约 95% 互联网人口之间的延迟不超过 50 毫秒

一站式编排和执行

Workers 能够在任何运行最高效的位置与 API、大语言模型 (LLM) 和外部或内部服务进行交互。

开发人员体验

您需要的所有产品

在单一平台上访问推理、状态管理、UI 部署或工作流。

从创意到生产部署仅需数秒时间

轻松简易的开发体验，包括本地开发和快速部署。

节省时间

无需调优。自动选择部署位置以提供最佳性能。

您只管编写代码，其他都交给我们。

RESILIENCE@CLOUDFLARE

一个安全平台。网络到云，应用到 AI，全面覆盖。

让组织能够：

- 重新控制运营
- 增强安全态势
- 加速供应商整合
- 增强用户体验，提高生产力
- 实现数据治理和合规

RESILIENCE@CLOUDFLARE

Cloudflare 专为未来打造

一个可组合的平台

统一的安全性
覆盖面向外部的系统和内部资源

任意连接
覆盖用户、应用、分支机构、数据中心和云

灵活性
可使用全栈开发人员工具定制平台

一个可编程的网络

更有效
简化连接和策略管理

更高效
确保在任何地方都提供快速、可靠和一致的用户体验

更敏捷
快速创新以满足不断变化的安全要求

RESILIENCE@CLOUDFLARE

在Workers AI 上运行推理任务。Workers AI 是首个全球分布式无服务器 AI 推理平台

部署到
全球

335+ 城市

遍布 125+ 国家/地区，包括中国大陆

代码执行位置与全球约 95% 互联网人口之间的延迟不超过 50 毫秒

190+ 城市

配备 GPU

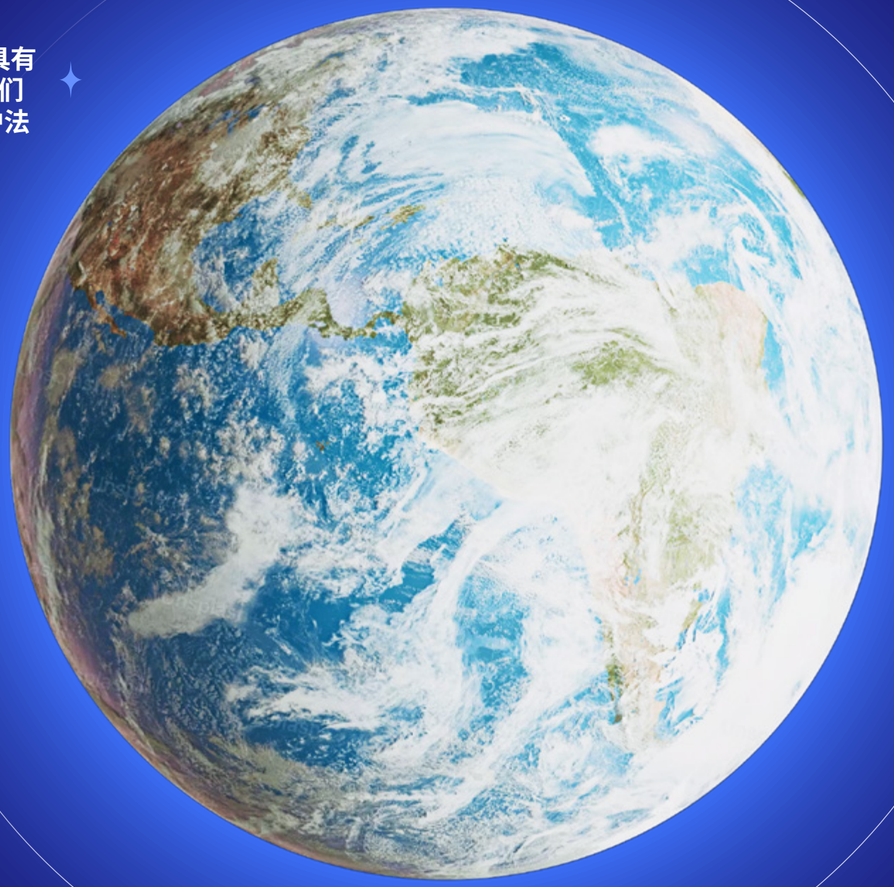
不断壮大的 AI 推理 GPU 算力城市集群

RESILIENCE@CLOUDFLARE

为开放的互联网而奋斗

互联网是一个奇迹。通过共同标准连接不同网络，使我们能够以具有韧性、互操作性和人人可访问的方式进行全球数据交换。如今，我们依赖互联网推动经济增长和创新，获取信息和自由表达言论，维护法治和民主原则。

作为支持互联网的全球社区一员，我们感到自豪。



- 倡导网络中立
- 监控互联网未开放的地方
- 保护人权与民主机构
- 部署改善数据隐私和安全性的标准
- 参与互联网标准开发
- 支持多利益相关者互联网治理

CLOUDFLARE

2025 年 Cloudflare 信号报告

了解更多

规模化韧性

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

REV:BDES-6966.2025APR24

尾注

本报告的发现主要基于 2023 年 1 月 2 日至 2024 年 12 月 31 日期间在 Cloudflare 全球网络上观察到的聚合流量模式。

1. https://www.darktrace.com/blog/survey-findings-ai-cyber-threats-are-a-reality-the-people-are-acting-now/
2. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
3. Cloudflare Radar 分析，2024 年
4. https://www.cnbc.com/2025/02/24/chegg-sues-google-for-hurting-traffic-as-it-considers-alternatives.html; https://www.theguardian.com/gnm-press-office/2025/feb/25/make-it-fair
5. Cloudflare Radar 分析，2024 年
6. https://nationalcioreview.com/wp-content/uploads/2024/07/2023_Insider_Threat_Report-16d8d8f7.pdf
7. https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai
8. https://www.verizon.com/business/resources/T1e3/reports/2024-dbir-data-breach-investigations-report.pdf
9. Cloudflare Radar 分析，2024 年。https://radar.cloudflare.com/bots
10. https://blog.talosintelligence.com/large-scale-brute-force-activity-targeting-vpns-ssh-services-with-commonly-used-login-credentials/; https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day
11. Cloudflare Radar 分析，2024 年
12. Cloudflare Radar 分析，2024 年
13. https://blog.talosintelligence.com/how-are-attackers-trying-to-bypass-mfa/
14. https://therecord.media/advance-auto-parts-data-breach-2million
15. Cloudflare Radar 分析，2024 年 10 月 12 日至 2024 年 12 月 31 日
16. Cloudflare Radar 分析，2024 年 10 月 12 日至 2024 年 12 月 31 日。https://radar.cloudflare.com/security/application-layer
17. Cloudflare Radar 分析，2024 年。https://blog.cloudflare.com/tag/ddos-reports/
18. Cloudflare Radar 分析，2024 年。https://radar.cloudflare.com/reports/ddos-2024-q4
19. https://reports.weforum.org/docs/WEF_Global_Cyber security_ Outlook_2025.pdf
20. https://www.verizon.com/business/resources/Tdd6/reports/2024-dbir-data-breach-investigations-report.pdf
21. Cloudflare Radar 分析，2024 年
22. https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf
23. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-survey-findings-on-esg-disclosure-and-preparedness.pdf
24. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
25. Cloudflare Radar 分析，2024 年。https://radar.cloudflare.com/adoption-and-usage
26. https://www.ey.com/en_us/board-matters/cyber-disclosure-trends
27. https://www.cloudflare.com/threat-intelligence/research/report/inside-lameduck-analyzing-anonymous-sudans-threat-operations/
28. https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam
29. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024
30. Cloudflare Radar 分析，2024 年 10 月至 2025 年 2 月
31. Cloudflare Radar 分析，2025 年 1 月。https://radar.cloudflare.com/ai-insights