



思科高管简报

2026 年 7 月

重塑关键基础设施运维模式

高管简报：AI 时代的网络防御

目录

- 迈向持续防御的转型趋势3
 - 重塑风险格局的两大动因3
 - 构建全新的运维节奏5
- 从理论到实践：机器规模的防御模式6
 - 思科先行：持续防御模式的落地成果7
- 重塑关键基础设施运维模式8
- 立即着手：三大优先事项9
 - 1. 升级运维模式，打造高韧性基础设施9
 - 2. 推进基础设施现代化升级9
 - 3. 全面提升安全态势10
- 衡量成效与落实预算11
- 前 90 天行动要点12
- 思科如何助您一臂之力13
- 后续行动14

迈向持续防御的转型趋势

前沿 AI 模型已从根本上改变威胁格局。如今，借助这些模型，攻击者能以机器速度发现漏洞、编写漏洞利用程序并借此打通攻击路径。这并非一个依靠补丁修复就能勉力支撑的临时阶段，而是一场关于企业和组织环境如何应对极速攻击的永久变革。

重塑风险格局的两大动因

01 补丁部署赶不上攻击速度

从漏洞披露到攻击爆发的时间窗口急剧缩短，而前沿 AI 更是将这一时间压缩至小时级。

02 攻击门槛已不复存在

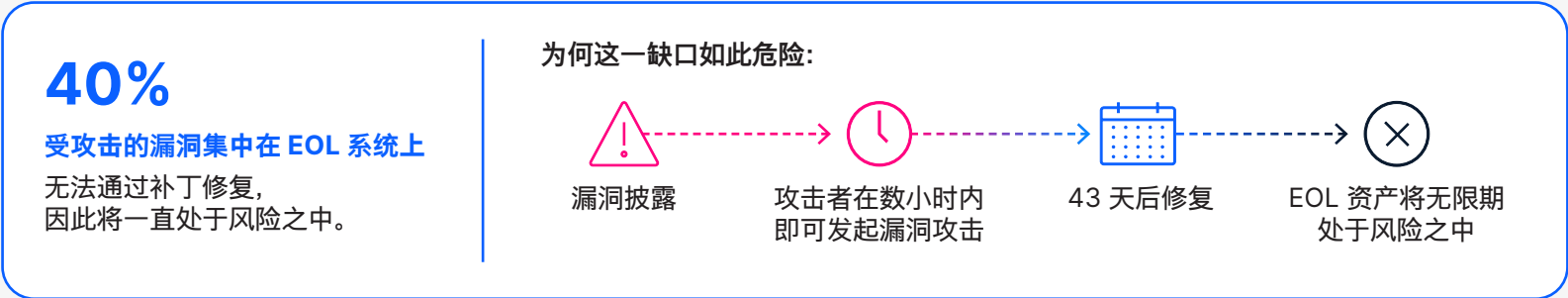
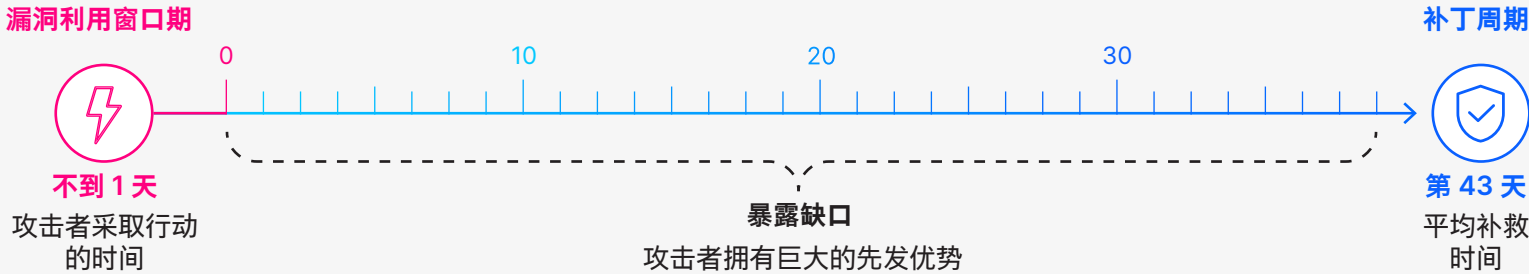
借助 AI，即便是技术薄弱的普通攻击者，也能发起以往需要国家级资源才能实施的复杂攻击。

多重因素叠加，威胁更加复杂：漏洞利用大幅提速，使得攻击者可渗透的漏洞范围持续扩大；与此同时，攻击门槛降低，具备攻击能力的主体数量相应暴涨。在这种形势下，可乘之机更多，攻击者数量激增，攻击速度也不断飙升。

企业和组织难以应对这种全新威胁形势，根源在于两大痛点：一是老旧基础设施无法通过修补或升级完成防护加固；二是传统安全流程仍采取人工操作来对基础设施进行定期防御。

长期沿用的“加固、验证和维护”传统模式，默认攻击者会受限于企业和组织的维护节奏，但事实并非如此。

数据揭示了传统方法的致命风险：2025 年，40% 最受攻击者青睐的漏洞都集中在生命周期已终止的系统上。修补一个严重漏洞的时间中位数高达 43 天。然而，漏洞利用窗口期（即从漏洞披露到被武器化的时间）如今已缩短至数小时。面对这一现实，43 天已不仅仅是延误，而是致命的败局。



来源： [《Talos 年度回顾》](#) 和 [《2026 年 Verizon 数据泄露调查报告》](#)

构建全新的运维节奏

依靠陈旧的流程或技术，根本无法应对 AI 时代的威胁。企业和组织需要建立一种持续不断的运维节奏：保持高频且可预测的修复和升级，淘汰那些无法有效保护的资产，全年无休地持续减少风险敞口。

本高管简报概述了 AI 时代保护企业和组织安全的实用措施，涵盖三大方向：升级运维模式，推进基础设施现代化升级，以及全面提升安全态势。请务必与安全和网络负责人共同审视这些措施，任何单点应对都会徒增不必要的风险敞口。

当您准备采取行动时，思科客户团队可分享一份详细的行动指南，为您的网络和安全团队提供针对本简报所分享信息的、更深层次的实战级指导。

从理论到实践：机器规模的防御模式

前沿 AI 正在改变安全领域的攻防格局，但两者所受的影响程度并不对等。正如云安全联盟首席分析师 Rich Mogull 在[最近的一份报告](#)中所述，攻击者占据着数学上的概率优势：他们只需找到一个漏洞加以利用即可，而防御者必须保护每项资源，抵御每个攻击者的每次攻击，才不至于功亏一篑。依靠陈旧的流程，您将无法破解这道数学难题。为了夺回优势，您需要一种能够帮助强化代码、加快补丁修复速度，且能实现大规模持续防御的运维模式。

思科先行：持续防御模式的落地成果



仅用 8 周时间，我们就对涵盖思科全线产品组合的 18 亿行代码完成了全面扫描。而在过去，即使由我们的安全研究团队主导，这项工作也需要 8 年才能完成。而这，仅仅是个开始。”

Anthony Grieco
思科高级副总裁兼首席安全与信任官

防御者需要的不仅仅是强大的 AI 模型，他们还需要具备相应的专业能力和运维模式，将 AI 的速度和规模转化为可重复的安全成果。思科安全和信任组织首先在内部环境中验证了这一方法，通过将前沿 AI 与安全专业能力及专项资源相结合，不仅提升了发现和修复漏洞的速度，还实现了评估的可重复性，并将安全防护转移到上游。

- **加速漏洞的发现与修复：**通过早期参与 Anthropic 的 [Project Glasswing](#) 和 OpenAI 的 [Trusted Access for Cyber](#) (TAC) 计划，思科将前沿 AI 模型应用于自身产品组合，在短短八周内分析了以超过 25 种编程语言编写的 18 亿行代码。这项工作充分展示了防御者如何利用 AI 的规模和速度优势，在真实的企业代码中加速漏洞的发现与修复。
- **实现评估的可重复性：**基于内部安全工程实践，思科开源了 [Foundry Security Spec](#)。这是一套久经实战考验的规范，用于构建智能体驱动的安全评估系统。该规范为防御者提供了一套独立于模型和技术栈的方法，将海量嘈杂的告警转化为界限清晰、优先级明确且可验证的评估结果。
- **将安全防护转移到上游：**思科构建并开源了 [Project CodeGuard](#)，旨在将“默认安全”规则融入 AI 编码工作流程。当它与 Foundry Security Spec 结合使用时，已确认的漏洞可转化为可重用的规则，从而有助于在已知的漏洞进入生产环境之前就将其拦截。

重塑关键基础设施运维模式

我们认为，企业和组织需要转向涵盖三个维度的持续防御：更新节奏、现代化升级和安全态势。

这种持续模式将改变您的运维方式：补丁修复变成了一种持续措施，而非临时救急；现代化升级旨在消除风险，而不仅仅是更新硬件；动态的安全态势则能缩小任何违规行为的影响范围。

	传统防御模式 强化防护，验证安全，避免变更	后 Mythos 时代的防御模式 强化防护，验证安全， 以机器级速度开展持续防御
更新节奏	每 12 至 24 个月 进行一次重大升级	引入 CI/CD 理念，确保系统 持续具备随时可发布的能力
现代化升级	延用老旧设备、 协议和脚本	持续淘汰 无法保障安全的资产
安全态势	仅记录风险例外情况	持续缩小并遏制 风险敞口

立即着手： 三大优先事项

变革始于聚焦三大优先事项：构建高韧性基础设施以赋能业务，解决设施老化问题，并全面提升整体安全态势。以下是对这些优先领域的总结，以及您可以向团队提出的启动相关问题。

1. 升级运维模式，打造高韧性基础设施

补丁修复已不再是定期性的项目，而是一项持续性的能力。客观形势使得这种转变势在必行：待修复的漏洞数量不断攀升，而维护窗口却日益压缩，逐台设备手动执行操作的传统模式根本无法填补这一缺口，攻击者会利用这一时间差发起攻击。解决之道在于建立可预测、自动化的节奏，让自动化技术消化海量修复工作，从而使工程师能将精力集中在需要专业判断的决策上，而不必逐台设备执行操作。要确保这种节奏能够强制执行，需要根据风险敞口层级设定补救 SLA，确保在数天内消除面向互联网的风险敞口，并在下一个维护窗口内解决下一层级的风险。

向您的团队提问：

- 按风险敞口层级划分，我们目前从收到安全通告到验证修复完成的平均时间中位数是多少？
- 流程中还有哪些步骤仍依赖人工手动操作？

2. 推进基础设施现代化升级

不再受支持的资产潜藏着无法通过控制措施弥补的风险：一旦出现新的漏洞，将无补丁可用。对于供应商已停止维护的系统，您只能选择将其隔离或淘汰。因此，现代化升级不仅涉及设备更新，更重要的是规避风险。对于其价值的论证应基于风险敞口和生命周期数据，而非单纯依据设备的使用年限。务必统一架构标准，确保其具备可修补、可视、可分段及可验证的特性，然后将其作为安全要求进行投入，并优先针对风险敞口最高的资产分批次推进。

向您的团队提问：

- 有多少资产的支持服务已经或即将终止？
- 这些资产与哪些系统相连？若再维持一年，需要付出多大的代价？

3. 全面提升安全态势

AI 驱动的攻击者现在能够以机器速度串联漏洞，使您的基础设施面临风险。对此，您可以采取以下防御手段：通过保护存在风险的资产来减少受攻击面；对环境实施网络分段以遏制入侵扩散、限制影响范围；填补隐蔽的身份管理短板以防止威胁升级。当攻击速度远超人类团队的反应极限时，您的 SOC 唯有借助全面的可视性、自动化以及智能体 AI 工作流程，才能跟上节奏。

这些控制措施并非都是新概念，但却空前紧迫地需要尽快落地。及早部署这些措施，不仅能有效抵御当下少数的高级威胁发起者，更能从容应对不久的将来大量涌现的攻击者。

向您的团队提问：

- 如果攻击者今天侵入了系统，在我们将其遏制之前，他们能沿着攻击路径渗透多深？
- 我们要如何察觉？
- 我们的响应速度能有多快？

一旦确立了这三个优先事项，工作重心就应从技术战略转向业务执行与成效衡量。

衡量成效与落实预算

衡量关键指标，并围绕业务风险阐述投资价值，以争取预算支持。

衡量成效

- ✓ 跟踪从收到安全通告到修复完成的耗时。按风险敞口层级进行度量。
- ✓ 衡量资产的更新程度。跟踪环境中运行最新版本的百分比。
- ✓ 严格执行补救服务级别协议 (SLA)。重点关注基于层级的 SLA，而非单纯的漏洞数量。
- ✓ 保留随时可供董事会审查的证据。妥善保存合规记录、补救时间安排和资产状态，以备审计员和网络保险公司审查。
- ✓ 强制落实智能体工作的问责制。确保每一项重要操作均可审核且可逆，并指定明确的负责人。

为新模式争取资金

- ✓ 有序安排支出。优先针对风险敞口最高的资产，将每一轮现代化升级与预算周期挂钩。
- ✓ 使支出与时间节点相匹配。利用融资手段将不可预见的资本支出转化为可预测的付款。
- ✓ 将其定位为安全要求。威胁形势决定了截止期限。这是业务发展的当务之急，而非锦上添花的可选行动。
- ✓ 资助运维能力建设。预算应涵盖服务和合作伙伴费用，以便在不增加人员编制的情况下扩展团队的工作效能。

前 90 天行动要点

以下是您现在即可批准的五项行动。这些行动均无需等待完整的计划设计完成，且每一项都能为下一项的执行创造条件。

1. **启动风险敞口评估。**建立按优先级排序的当前视图，清晰展示现有资产、存在漏洞的环节、不再受支持的资产以及面临风险的部分。这将作为你们共同的真实信息来源。
2. **按风险敞口层级设定补救 SLA。**承诺在数天内消除面向互联网的风险敞口或高严重性风险，并在下一个窗口期解决次级风险，同时据此进行汇报。这是落实持续防御的关键政策决策。
3. **建立常态化节奏。**建立标准化变更窗口并预先批准模板，使补丁修复成为例行维护，而不再是例外情况。
4. **确定首批现代化升级目标。**识别风险敞口最高的不受支持资产，并优先投入资金进行更换，价值论证应基于风险敞口、生命周期数据和未来业务需求。现代化升级是打造更安全、面向未来的基础设施的良机。
5. **开展面向 AI 时代的响应模拟训练。**模拟攻击者利用边缘漏洞以机器速度进行横向移动，以此统一团队的响应行动。

思科如何助您一臂之力

思科携手值得信赖的合作伙伴，致力于协助您应对这一全新现实。依托合作伙伴，我们提供覆盖所有这些领域的专业服务以赋能企业和组织，其中包括思科[韧性基础设施服务](#)，该服务针对基础设施加固提供了一套三步走结构化方案。

升级运维模式，打造高韧性基础设施

自 2026 年 7 月起，思科将按固定时间安排发布更新，提前通知并实行错峰发布，避免任何团队同时面临两个重大更新窗口。我们会确定受每次安全公告影响的产品，依据风险敞口而非单一的严重性评分来确定优先级，并确保修复措施落实到位。当暂时无法部署补丁或升级时，运行时防护机制将在无需停机的情况下为资产提供保护。

推进基础设施现代化升级：

我们提供多种途径，助您识别哪些思科资产已不受支持且存在风险，并提供加固基础设施和启用额外安全保护的建议。在考虑引入现代化基础设施进行更新换代时，思科推荐采用安全网络架构，通过以身份为先的网络分段、统一策略和分布式执行，将安全能力深度融入网络本身。为助力这一转型过程，Cisco Capital 提供灵活的融资方案，助您从容应对计划外支出。

全面提升安全态势：

思科为完整的攻击路径实施安全防护：跨人类、机器和 AI 智能体实体进行统一身份治理，随着智能体数量的激增，这种差异化优势变得愈发关键；强制执行网络分段，以便在发生入侵时有效遏制横向移动；使检测与响应实现机器级提速，由 AI 消化海量修复工作，而安全分析师则专注于需要专业判断的决策。

后续行动

当您准备推进下一步时，请联系思科客户团队，他们将协助将本简报中的建议付诸实施。他们能够全程提供指导，针对企业和组织及其面临的挑战量身定制详细的计划与评估。

思科合作伙伴同样是宝贵的资源。鉴于各合作伙伴的专长各异，建议根据您的环境需求来选择匹配的合作伙伴。欢迎访问[思科合作伙伴中心](#)，寻找最适合您的合作伙伴。