Gartner

# 聚焦2027：九大网络安全趋势前瞻

筑牢新兴领域安全防线

革新治理体系

实现AI应用常态化

1 CISO 拓展软件供应链安全边界，应对 AI 增强型威胁

2 组织应对滞后，量子解密威胁加剧

3 IAM需升级转型，保障AI智能体安全并赋能其应用

4 代理型AI需纳入项目级统筹监管

5 AI与网络韧性重塑CISO的职责边界

6 技术债务阻碍AI目标的达成

7 AI颠覆传统网络安全意识培训模式

8 AI驱动的SOC解决方案颠覆运营常态

9 前沿AI模型变革漏洞管理

## 筑牢新兴领域安全防线

### 1 CISO 拓展软件供应链安全边界，应对 AI 增强型威胁

59%的CISO将第三方及供应链攻击视为未来12个月的五大威胁之一。原因在于，业务方要求快速交付AI系统，迫使组织在未充分验证安全性的情况下，采用开放权重模型、前沿模型以及集成这些模型的第三方组件。

### 2 组织应对滞后，量子解密威胁加剧

预计到2029至2030年，量子计算将威胁传统非对称加密的安全性。鉴于改造迁移耗时数年，网络安全领导者应尽快评估并部署后量子密码（PQC）解决方案。

### 3 IAM需升级转型，保障AI智能体安全并赋能其应用

机器身份的数量正以空前速度增长——94%的组织报告其规模持续扩大，而AI/机器学习的应用（52%）和自主智能体的发展（35%）是推动这一增长的主要因素。这类非人类身份现已成为攻击者的重点目标。58%的组织遭遇过与AI相关的机器身份失陷事件，其中42%造成中度至重大业务中断，36%带来财务损失，32%导致声誉受损。

## 革新治理体系

### 4 代理型AI需纳入项目级统筹监管

在CEO和CIO为保持竞争力而积极推动AI应用的大环境下，CISO难以放缓相关项目的推进。一方面，业务部门采购AI智能体的需求迫切；另一方面，“氛围编程”（vibe-coding）工具大幅降低了使用门槛，组织很难抵抗这种诱惑。然而，真正落实员工使用第三方AI应用审批与管控流程的企业仅占16%。结果是，“失控自动化”流程在无人监管的情况下被授予过高权限并持续运行。

### 5 AI与网络韧性重塑CISO的职责边界

两股颠覆性力量正在重塑CISO的职责边界。其一是从网络防护向网络韧性的战略转变，其二是引入AI并保障其安全的迫切需求。职责范围随之扩大，通常延伸至数据治理、AI治理、隐私保护和业务连续性等领域——但对大多数CISO而言，这并不代表其需要直接承担这些领域的管理职责。

### 6 技术债务阻碍AI目标的达成

49%的网络安全领导者将技术债务视为阻碍其核心工作推进的主要瓶颈。面对高管层加速部署AI的压力，企业不得不转向那些缺乏充分安全治理和AI适配管控的非结构化数据仓库，由此引发数据过度共享与越权访问等问题。

## 实现AI应用常态化

### 7 AI颠覆传统网络安全意识培训模式

在AI快速普及的背景下，现有的网络安全意识培训未能有效降低企业面临的安全风险。60%的数据泄露仍与人为因素相关，而86%的组织已在局部或全面使用独立的公有SaaS生成式AI应用。

### 8 AI驱动的SOC解决方案颠覆运营常态

受降本要求和市场过高预期的影响，AI驱动的安全运营中心（SOC）的发展前景充满不确定性。CISO本意是借助AI强化告警分流和调查能力，却不得不应对人员配置、技能重塑压力以及AI工具成本难以预测等现实困境。

### 9 前沿AI模型变革漏洞管理

传统的漏洞管理以漏洞数量作为优先级依据，这种模式本就与攻击者的实际节奏脱节。如今，前沿AI又带来了前所未有的供给端冲击：供应商和开源项目纷纷借助AI发现隐藏漏洞，导致安全补丁的发布数量与频率急剧上升，组织面临的更新压力陡增。

免责声明：以上趋势排名不分先后。

## 客观、可执行的洞见

布局未来，助力企业抢占成功先机。探索为网络安全领导者提供的其他免费资源与工具：

**会议**

**网络安全会议与活动**

与Gartner分析师及同行共同探讨最新网络安全动态。

查看日程↗

**路线图**

**构建企业级弹性网络安全路线图**

构建具备韧性、可扩展性与敏捷性的网络安全路线图。

即刻下载↗

**洞察报告**

**网络安全与AI：管理风险，实现安全保障**

就网络安全领域而言，AI市场热潮与前景也伴随着担忧与风险。Gartner助您厘清重点关注领域。

了解更多↗

**网络研讨会**

**AI智能体与OpenClaw的安全风险与防御策略**

解析 AI 智能体与 OpenClaw 带来的安全挑战，并分享实现 AI 自动化安全治理的实践方法。

立即观看↗

成为客户

已是Gartner客户？
登录客户门户网站，获取更多资源。登录↗

点击了解更多关于Gartner网络安全领导者服务的相关信息↗

来源：Gartner

© 2026 Gartner, Inc.及/或其关联公司版权所有。保留所有权利。CM_GTS_ 5333150

Gartner