以毒攻毒，确保网络安全

不同于以往的任何技术，生成式 AI 正在迅速颠覆商业和社会形态，迫使企业领导者刻不容缓地重新思考其假设、计划和战略。为了帮助 CEO 们掌握快速变化的形势，IBM 商业价值研究院 (IBM IBV) 发布了一系列有针对性、基于研究数据的生成式 AI 指南，涵盖数据网络安全、技术投资策略和客户体验等主题。

这是本指南的第七部分，重点关注“网络安全”。

生成式 AI 既加剧了风险，也增强了韧性

生成式 AI 催生了一系列新兴网络威胁。黑客获得了更多的机会来利用漏洞，也可以通过更多的方式来执行恶意活动。

幸运的是，反之亦然：生成式 AI 可以加强企业的防御能力。在短期内，生成式 AI 将让曾经一度繁重的安全流程变得更加高效。通过分析海量数据并识别模式和异常，生成式 AI 可以及时发生新出现的威胁。

随着恶意行为者不断采用新的攻击方式，网络安全团队也需要与时俱进，跟上最新的安全形势。在这场猫鼠游戏中，时刻保持警觉将是管理漏洞并保持领先一步的关键。

IBM 商业价值研究院甄别出了每位领导者都需要了解的三个要点：

1. 生成式 AI 引入全新的风险与威胁。
2. 如果缺乏安全的数据，实现值得信赖的生成式 AI 就无从谈起。
3. 生成式 AI 将成为网络安全的“倍增器”。

现在，每位领导者都需要采取以下三项行动：

1. 将生成式 AI 视为迫切需要加以保护的重要平台。
2. 让可信数据成为组织的支柱。
3. 围绕速度和规模重新调整网络安全投资。

1. 网络风险 + 生成式 AI

需要了解的事项

生成式 AI 引入全新的风险与威胁。

生成式 AI 为网络攻击者提供了全新的武器库。当今的黑客不再仅仅是伪造电子邮件，而是可以模仿声音、面孔，甚至个性来诱骗受害者。

而这还只是开始。

随着生成式 AI 在未来半年到一年内持续普及，专家们预计新型入侵攻击将达到前所未有的规模、速度、复杂性和精密性，各种新的威胁形式也会不断涌现。从可能性和潜在影响的角度来看，大规模发起的自主攻击将成为最重大的风险。不过，受访高管们预计，黑客伪造或冒充可信用户将对业务产生最大的影响，其次是创建恶意代码。

组织实施生成式 AI 的方式也可能会带来新的风险。事实上，47% 的受访高管担心在运营中采用生成式 AI 会引发针对其组织自主 AI 模型、数据或服务的新型攻击。几乎所有受访高管 (96%) 表示，采用生成式 AI 可能会在未来三年内导致其组织出现安全漏洞。

全球数据泄露的平均成本为 445 万美元，美国更是高达 948 万美元。在此形势下，许多企业正在加大投资力度，以应对新兴网络安全风险。受访高管表示，其组织 2023 年的 AI 网络安全预算相比 2021 年增加了 51%。而且，他们预计到 2025 年，这一预算将再增加 43%。

受访高管们表示其组织 2023 年的 AI 网络安全预算相比 2021 年**增加了 51%**。

而且，他们预计到 2025 年这一预算将**再增加 43%**。

1. 网络风险 + 生成式 AI

需要采取的行动

将生成式 AI 视为迫切需要加以保护的重要平台。

敦促网络安全领导者紧急行动，即刻着手应对生成式 AI 的风险，而不是采取分步措施。

理解当前的 AI 风险状况。举办董事会级会议，召集网络安全、技术、数据和运营领导者共同讨论不断演化的风险，包括生成式 AI 的哪些使用方式有可能暴露敏感数据，并允许以未经授权的形式访问系统。让每个人都了解新兴的“对抗性”人工智能 — 即便是在核心数据集中引入几乎察觉不到的细微变化也可能会导致恶意结果。

确保整个 AI 管道安全无虞。专注于对用于训练和调优 AI 模型的数据进行保护和加密。在模型开发过程中持续扫描漏洞、恶意软件和损坏，并在模型部署后监控特定于 AI 的攻击（例如数据污染和模型盗窃）。

投资部署专为保护 AI 而设计的新型防御措施。尽管可以通过扩展现有的安全控制和专业知识来保护支持 AI 系统的基础架构和数据，但检测和阻止针对 AI 的对抗性攻击就需要采用全新的方法。

2. 数据 + 生成式 AI

需要了解的事项

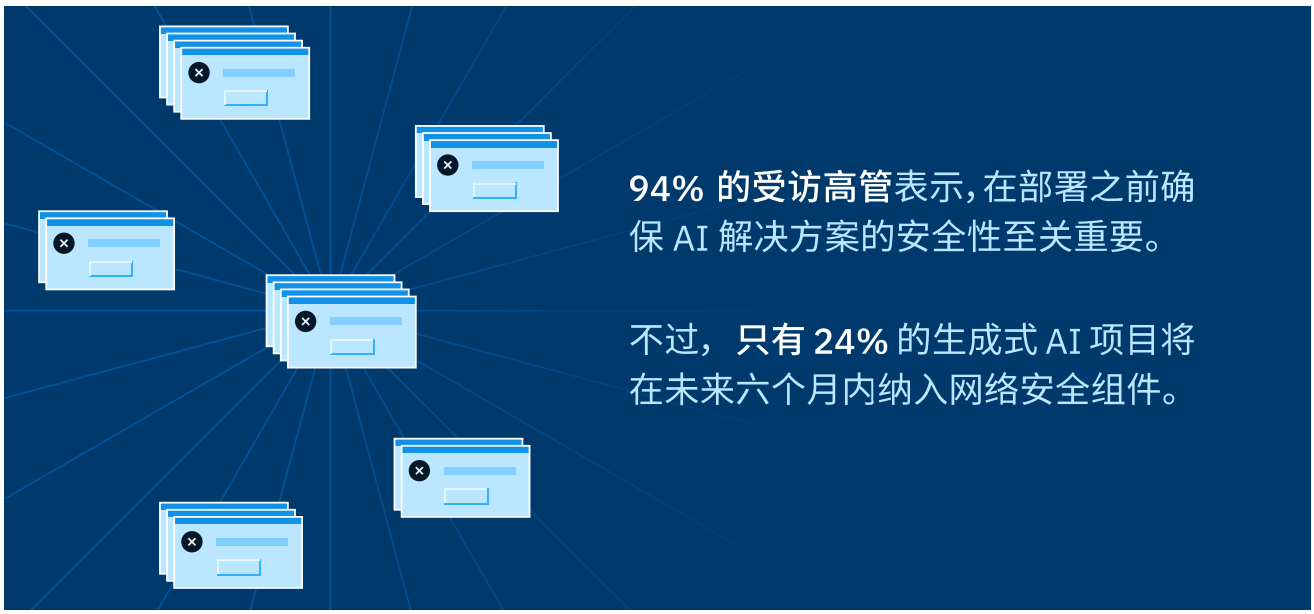
如果缺乏安全的数据，实现值得信赖的生成式 AI 就无从谈起。

数据是生成式 AI 的命脉。所有模型都依靠数据来回答查询并提供见解，也正是因此，训练数据成为了网络攻击的主要目标。黑客仍然希望窃取数据并高价出售，但数据渗透提供了一条获取非法利润的新途径。如果黑客可以更改驱动组织生成式 AI 模型的数据，就可以通过有针对性的操纵或错误信息来影响业务决策。这种不断演变的威胁带来了一系列新的法律、安全和隐私问题，而 CEO 则需要在整个企业范围内管理这些问题。

高管们看到了问题的严重性。在采用生成式 AI 方面，受访高管预计会出现各种各样的风险 — 84% 的受访高管担心广泛或灾难性的网络安全攻击有可能会引发新的漏洞。三分之一的受访高管表示，如果没有全新的治理形式，例如全面的监管框架和独立的第三方审计，就无法管理这些风险。

总体而言，94% 的受访高管表示，在部署之前确保 AI 解决方案的安全性至关重要。不过，只有 24% 的生成式 AI 项目将在未来六个月内纳入网络安全组件。而且，69% 的受访高管表示，在部署生成式 AI 方面，创新优先于网络安全。

这表明对生成式 AI 网络安全需求的理解与网络安全措施的实施之间存在明显脱节。为了规避代价高昂且不必要的后果，CEO 需要采取有力举措来应对数据网络安全和数据溯源问题，包括投资部署数据保护措施（如加密和匿名化），以及建立数据跟踪与溯源系统，为生成式 AI 模型所使用的数据提供更好的完整性保障。



2. 数据 + 生成式 AI

需要采取的行动 →

让可信数据成为组织的支柱。

持续迭代网络安全实践，全面考虑多种生成式 AI 模型和数据服务的要求。

在 AI 应用中建立信任与安全性。优先实施以安全、隐私、治理和合规性为中心的数据策略与控制。传达透明度和问责制对于在管理风险方面对于防止偏见、幻觉和其他问题的重要性。

保护为 AI 提供动力的数据。让首席信息安全官负责发现训练或调优中使用的敏感数据并对其进行分类，同时实施数据丢失预防技术，以防止通过提示发生数据泄漏。围绕机器学习数据集实施访问策略与控制。扩展威胁建模以涵盖生成式人工智能特定的威胁，例如数据污染、包含敏感数据以及输出不适当的内容。

将网络安全视为一种产品，并将利益相关方视为客户。网络安全对于保障 AI 计划顺利推进并推动收入增长至关重要。为了确保在产品中安全地使用 AI，请让您的团队了解生成式 AI 带来的网络安全威胁。强调改变行为以改善数据和安全卫生的价值。确保网络安全成效与业务成效相一致，从而鼓励采用。

3. 网络韧性 + 生成式 AI

需要了解的事项 →

生成式 AI 将成为网络安全的“倍增器”。

如果应用于网络安全领域，生成式 AI 可以成为业务加速器。生成式 AI 可以自动执行重复且耗时的任务，让团队专注于处理更复杂、更具战略性的安全事务。生成式 AI 还可以检测和调查威胁，并从过往事件中学习，以实时调整组织的应对策略。

由于收益显著，CEO 面临着迅速广泛引入生成式 AI 的压力。但为了避免增长结构倒塌，企业高管迫切需要利用生成式 AI 来增强韧性。这样一来，高管们不仅可以规避生成式 AI 的风险，还可以借生成式 AI 之力，让组织变得更强大。

超过一半的受访高管 (52%) 表示，生成式 AI 将帮助他们更好地分配资源、能力、人才或技能；而 92% 的受访高管表示，在采用生成式 AI 之后，这项技术更有可能增强或提升而不是取代其网络安全人员。

这些新兴技术工具可以帮助团队降低复杂性并专注于最重要的任务，或许也正是因此，84% 的受访高管计划优先部署生成式 AI 网络安全解决方案，而不是传统的网络安全解决方案。

在网络安全领域使用生成式 AI 有助于在整个企业生态系统中实现“倍增效应”。84% 的受访高管表示，开放创新的生态系统对于其组织未来的增长战略非常重要。由于企业高管希望建立支持创新和增长的合作关系，大多数受访高管预计生成式 AI 功能将影响其组织在未来两年内对云计算 (59%) 和整个业务 (62%) 的生态系统合作伙伴的选择。

随着技术的日益成熟，生成式 AI 在降低风险和创造价值方面的潜力会不断增长。建立广泛风险管理和韧性能力的企业将能够利用这项新技术抢占先机，取得“行稳致远”的发展，并更有效地为未来的增长保驾护航。

84% 的受访高管计划优先部署生成式 AI 网络安全解决方案，而不是传统网络安全解决方案。

3. 网络韧性 + 生成式 AI

需要采取的行动

围绕速度和规模重新调整网络安全投资。

让 AI 成为加强安全防御的重要工具。鼓励网络安全领导者将生成式 AI 和自动化嵌入到其工具包中，以便快速、大规模地应对安全风险与事件。这将大幅提高生产力，并让网络安全成为业务增长的推动力。

运用 AI 加速实现安全成效。自动处理不需要人类专业知识和判断力的日常任务。运用生成式 AI 简化人类与技术协同合作的任务，例如安全策略生成、威胁搜寻和事件响应。

部署 AI 来检测新威胁。更新工具和技术，使您的团队在速度、规模、精度和复杂性上能够跟上攻击者的步伐。运用生成式 AI 更迅速地识别模式和异常，让团队能够及时发现新的威胁向量，从而防患于未然。

发挥合作的力量。与值得信赖的合作伙伴携手合作，共同定义 AI 安全成熟度，并实施全面的生成式 AI 战略，以推动整个组织创造价值。

IBM 商业价值研究院

CEO 生成式 AI 行动指南

网络安全

本页分析所依据的统计数据来自 IBM 商业价值研究院联合牛津经济研究院开展的四次专项调查，以及来自 2023 年 IBM *数据泄露成本报告*中的一项参考资料和来自*打开创新之门 (2022)* 的一项参考资料。2023 年 9 月至 10 月，针对 200 名美国高管开展了第一项调查，主题是生成式 AI 对网络安全的影响。2023 年 5 月至 6 月，针对 414 名美国高管开展了第二项调查，主题是生成式 AI 对混合云的影响。2023 年 8 月至 9 月，针对 200 名美国高管开展了第三次调查，主题是生成式 AI 和 AI 伦理。2023 年 5 月，针对 300 名美国高管开展了第四次调查，主题生成式 AI 对劳动力的影响。

IBM 商业价值研究院

IBM 商业价值研究院 (IBM IBV) 创立二十年来，凭借 IBM 在商业、技术和社会交叉领域的独特地位，我们每年都会针对成千上万高管、消费者和专家展开调研、访谈和互动，将他们的观点综合成可信赖的、振奋人心和切实可行的洞察。

需要 IBV 最新研究成果，请在 ibm.com/ibv 上注册以接收 IBV 的电子邮件通讯。您可以在 Twitter 上关注 @IBMIBV，或通过 https://ibm.co/ibv-linkedin 在 LinkedIn 上联系我们。

访问 IBM 商业价值研究院中国官网，免费下载研究报告：https://www.ibm.com/ibv/cn

扫码关注 IBM 商业价值研究院

官网　微博　微信公众号　微信小程序

国际商业机器 (中国) 有限公司
北京市朝阳区金和东路 20 号院 3 号楼
正大中心南塔 12 层
邮编：100020

美国出品 | 2023 年 11 月

DBMQB8RE-ZHCN-00