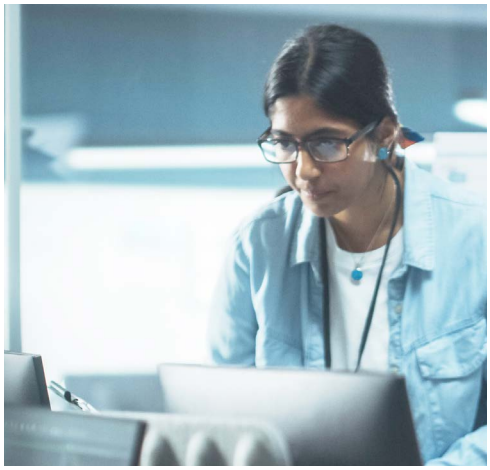
人工智能和自动化助力网络安全

领导者如何统筹技术和人才以取得成功

IBM

IBM 如何提供助力

IBM Security 致力于运用机器学习和自然语言处理等 AI 技术来助力安全运营分析师从容应对最新威胁、缩短响应时间以及降低成本。如需了解更多信息，请访问：ibm.com/security/artificial-intelligence



摘要

通过减轻日常任务负担，人工智能和自动化让网络安全团队能够将其稀缺专业知识应用于最迫切需要的环节。

安全事件快速增长，采用全新的安全运营方式已是势在必行

AI 和自动化有助于提高整个安全运营的可见性和生产力。领先的 AI 采用者正在监控 95% 的网络通信，并将事件检测时间缩短了三分之一。

AI 在安全领域的应用日益增长

根据调研，高管已在安全运营中广泛采用 AI。93% 的受访高管表示已经部署或正在考虑部署 AI。

采用安全 AI 的领导者正在改进关键成本绩效指标

绩优型组织将其安全投资回报率 (ROSI) 提高了 40% 或更多，并将数据泄露成本降低了至少 18%，从而腾出资金再投资于其网络安全团队。

快速变革加剧网络风险

现代数字运营一方面在创造价值，但另一方面也会产生新的漏洞。

2021 年，网络安全威胁事件大幅增长。美国 Colonial Pipeline 公司和一些水处理设施的系统就遭受了攻击。[1] 根据最近的一项研究报告，从 2020 年到 2021 年，勒索软件攻击事件增长了 105%，其中制造业是受攻击最多的行业。[2] 在过去的一年中还发生了一些迄今为止影响最大的供应链攻击事件。从 SolarWinds 漏洞利用、Microsoft Exchange Server 漏洞利用到 Apache Log4j 漏洞，各种重大网络攻击事件屡见报端，促使企业领导者及其客户增强警醒意识。[3]

是什么因素导致了当今形势剧变？

简而言之，新冠疫情加速了数字化转型，也放大了机遇和风险。[4] 如今，远程工作者的数量大幅增长。云用户和云服务的数量突飞猛进。许多基本系统都与第三方合作伙伴实现了集成。数量庞大的边缘设备正在将物联网数据传输到云端。各种设备互联互通，相互依存，实现高级连通性，创造价值的速度和规模均达到空前水平。

创新一方面创造了效益，但另一方面也是有代价的：新的设备、新的合作伙伴和新的集成大幅扩大了组织的整体受攻击面。各种新的威胁途径也层出不穷 — 从不知情的供应商到心怀不满的员工，从数据泄露、拒绝服务攻击到勒索软件。更复杂的是，威胁行为体在不断进化其策略、技术和程序，开始运用人工智能（AI）和自动化来探测弱点并发动更有效的攻击（见图 1）。[5]

最终结果是，许多高管都清楚认识到：当今的“不间断”数字化运营一方面在创造价值，但另一方面也会产生新的漏洞。尽管先进技术服务实现了效率提升，但许多组织正逐渐意识到其数字足迹充满了复杂性和未知数。除了形势变幻莫测以外，人手不足的安全团队也在疲于应对来自不同来源的海量数据（但往往缺乏洞察）和各种各样的工具。即使是知识丰富的安全专家，庞大、人才济济的网络安全运营团队，也往往无力应对上述挑战。

针对当前的运营现状，采用一种全新的安全方案势在必行

为了助力团队取得成功，网络安全领导者需要采用一种更加主动式和预防性的安全方案来保护核心业务运营。我们的研究表明，越来越多的组织开始采用前瞻性的威胁管理方法，利用 AI 驱动的自动化流程来改善洞察力、生产力和规模经济。

AI 技术可以通过四种关键方式推动安全转型：

- 机器学习功能有助于识别模式、盘点新资产和服务以及改进 AI 模型的性能。
- 推理功能有助于为数据分析提供信息、增强场景建模以及预测新的攻击途径。
- 自然语言处理可用于挖掘文本数据源、增强威胁情报以及充实知识资源。
- 自动化有助于协调时间密集型任务、加快响应速度以及减轻人类安全分析师的负担。

总的来说，这些功能可共同推动安全运营转型。

本报告展示了人工智能与自动化相结合将如何大幅改善速度、洞察力和灵活性。在实现这些绩效改进之后，网络安全团队可以专注于处理真正重要的事项，即主动防范、检测和响应威胁并从中恢复，同时降低成本和复杂性。

图 1

安全巅覆者

安全运营团队面临新的挑战

第 1 章

AI 在安全领域中的应用逐渐加速

为了解组织如何运用 AI 来支持安全运营并量化其对网络安全绩效的影响，IBM 商业价值研究院 (IBV) 与美国生产力和质量中心 (APQC) 开展合作，对 1000 位全面负责组织信息技术 (IT) 与运营技术 (OT) 网络安全的企业高管进行了调研。这些高管来自全球 5 个地区的 16 个行业 (参见第 32 页的 “研究和分析方法”) 。

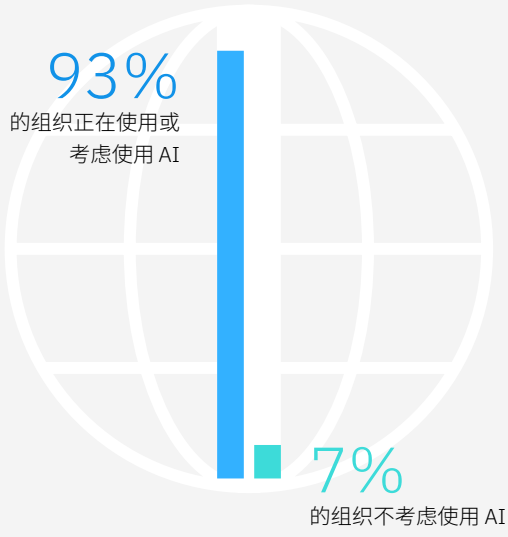
我们请求受访高管提供其组织安全部门绩效的相关信息以及他们在多大程度上运用 AI 和自动化来管理网络风险和合规性。他们还描述了如何运用 AI 来支持保护和预防流程以及检测和响应流程的安全运营。我们利用这些洞察来评估 AI 对网络安全绩效的影响，主要包括生产力、弹性和相关业务收益。

总体而言，我们发现全球范围内各个行业的大多数企业正在考虑或正在其安全部门中采用 AI 和自动化。64% 的受访高管表示已在至少一个安全生命周期流程中实施了 AI 来支持安全功能，而 29% 的受访高管表示正在考虑实施 AI。换句话说，基于 AI 的安全功能可能很快成为一种近乎普遍的能力 (见图 2) 。其余 7% 的受访高管表示并不考虑将 AI 和自动化应用于安全运营，他们正将自己置于危墙之下，非常有可能会无力应对快速增长的安全事件。

图 2

广泛采用

只有少数组织未考虑在安全运营中使用 AI



目前，64% 的受访组织正在试用、实施、运营或优化 AI 安全解决方案。我们将这部分组织称为“AI 采用者”。尽管 AI 在安全领域中的应用仍处于初期阶段（大多数组织应用 AI 不超过 2 年时间，也仍在使用传统环境），但预计未来会迅速普及。就 AI 的具体应用而言，在保护和预防功能中应用 AI 的 AI 采用者比例预计在未来三年内平均将增长约 40%，而在检测和响应功能中应用 AI 的 AI 采用者比例预计也将实现相同的增长。

与其他调研的结果相一致， 本次调研预计 AI 在安全领域的应用也将加速增长。我们近期的研究预测，在 2027 年之前，与网络安全相关的人工智能支出将保持 24% 的复合年增长率。到 2027 年，这一支出将达到 460 亿美元。[6]

技术和人才发挥积极成效

AI 采用者认识到 AI 驱动的洞察和 AI 驱动的自动化可为其安全主题专家的专业级识别和响应能力提供有力补充。他们发现，安全 AI 系统能够有效识别异常行为、动态评估漏洞以及标记异常活动（表示可能存在新威胁），其能力丝毫不亚于经验丰富的安全分析师。65% 的 AI 采用者表示，AI 的应用对其安全运营产生了重大积极影响（参见第 7 页的图 3）。但与人类安全分析师不同的是，安全 AI 可以运用机器学习和自动化来满足混合多云运营对于超高速度和超大规模的要求 — 其一致性和深度要远远超出顶级资深安全专家的能力。（参见观点：“安全 AI 为何如此有效？”）

例如，组织可以应用 AI 来跟踪正常行为以及实现模型构建自动化。为此，AI 安全解决方案会标记与预期行为的差异，并分析异常路径的威胁影响。57% 的 AI 采用者认为增强威胁响应以自动遏制威胁以及优化业务连续性可发挥最重大的影响力。通过理解上下文中的异常活动，AI 安全解决方案可以确定哪些安全策略和控制存在风险，运用相关洞察作为预警的强力补充，然后启动规范化补救措施。

这种为人类专家充当“网络助手”的方式突显了安全 AI 最重要的一项优势：减轻面临技能和资源持续短缺的安全团队的压力。60% 的 AI 采用者表示，自动化数据充实和第二屏功能可帮助安全分析师提高运营效率，从而大幅增强安全部门的效能。AI 威胁模型可以参考较长时间范围内和各种运行状况下的更多事件，因此可以引入专家级功能来应对让人类分析人员束手无策的威胁。

借助 AI 生成的洞察，AI 驱动的自动化功能可以按用户、设备或位置隔离威胁，然后发出适当通知并启动适当上报措施，并由人类专家来确定最佳调查和补救方案。对于已经开发这些功能的组织，网络安全分析师可以开始专注于真正重要的事项：不断提升技能和专业知识以解决更复杂、只有人类能够做出判断的问题。

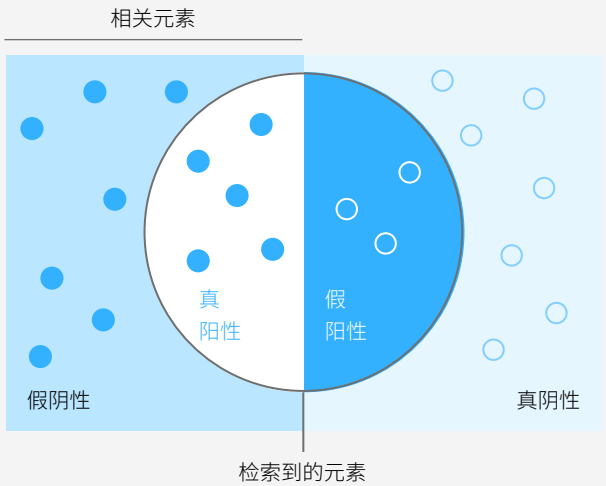
观点

安全 AI 为何如此有效?

为了防御不断扩大的受攻击面以及应对大幅增长的安全事件，安全 AI 和自动化正迅速成为必备能力。AI 为何如此有效？简而言之，这得益于迭代机器学习与分析模型调优的融合。

调优是优化分析模型性能的过程，但不会过度依赖于在不同情形中会发生变化的变量。在后台，机器学习算法运用无数样本来识别模式并学习如何有效响应不同的变量。此训练过程是改进 AI 模型性能效果的关键。

通过机器学习提高模型精确率和召回率，AI 安全解决方案可以有效区分实际安全威胁（真阳性）与普通事件（假阳性和真阴性），从而帮助安全分析师减轻预警疲劳（见下图）。这些解决方案可以对大多数安全事件进行鉴别分类，利用上下文数据洞察作为这些事件的补充，然后为安全分析师的检查和调查活动提供支持。通过利用 AI 来提高信噪比，安全分析师可以专注于处理构成最大风险的实际威胁。



信息来源：改编自 https://en.wikipedia.org/wiki/F-score

人工智能和自动化让安全分析师能够重新关注需要人工判断的复杂问题，从而创造更加充实和丰富的工作环境。

AI 可以分析非结构化和结构化数据源（利用威胁情报服务和开源网络情报 (OSINT) 整合内部和外部数据），因此可以提供情境化变量和情境化威胁的全面画像。对于网络安全分析人员来说，这有助于减少检测、响应和从事件中恢复所需的时间。

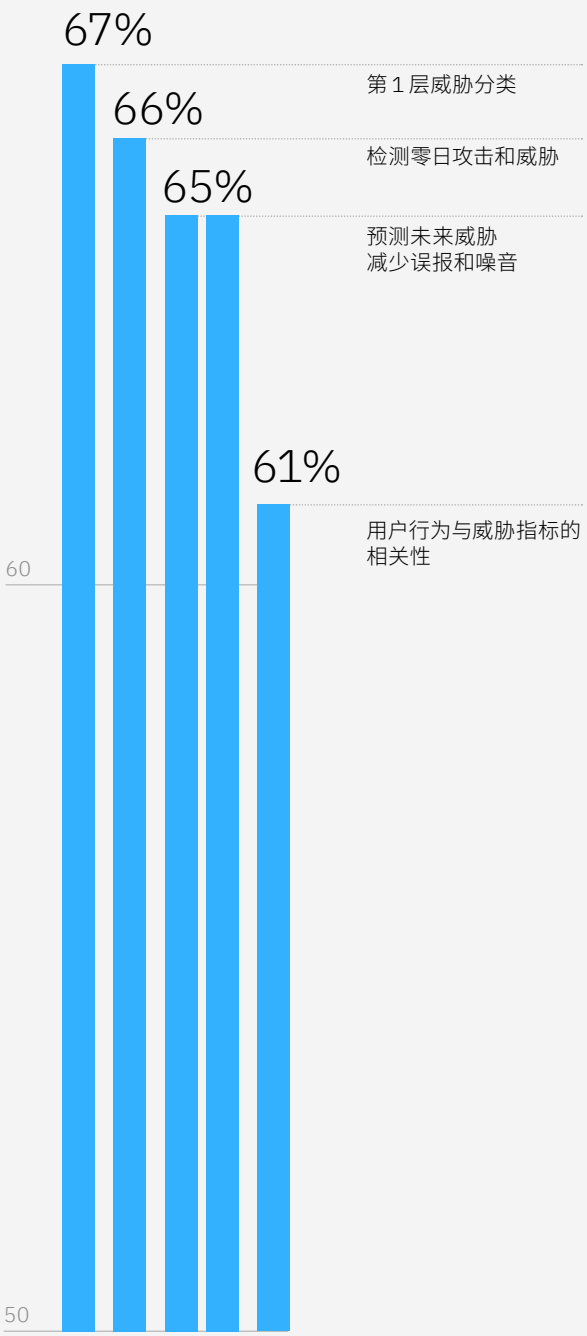
通过实现更加高效的上报、审查和补救程序，AI 可有效增强安全治理和合规性。通过自动处理耗时的重复性任务，AI 可以帮助分析人员减轻疲劳并做出更加合理和明智的决策 — 速度更快且错误更少。安全 AI 和自动化解决方案可以分发大量事件，从而让领导者能够充分利用优秀人类分析师的稀缺性技能。这最终将打造一个更加充实、丰富和令人满意的工作环境，从而在吸引和留住稀缺性网络安全人才方面发挥重要影响力。

成功融合 AI 洞察、自动化与员工专业能力的 AI 采用者指出，AI 应用对其安全成效产生了更加积极的影响（参见图 3）。67% 的受访高管表示，更有效地对第 1 层威胁进行鉴别分类有助于消除与基本检测相关的成本和时间。另有 65% 的受访高管表示，减少误报和噪音减少了人类安全分析师的检测工作量。65% 的受访高管表示，应用行为分析可有效支持预测未来威胁，这是提高主动性的重要步骤。

图 3

AI 的优势

AI 采用者利用 AI 解决方案来支持关键功能，从而改善绩效



问：以下哪项 AI 应用对您组织的安全运营具有最大影响力（选择前 5 项）？

AI 投资回报可观

据估计，到 2025 年，网络犯罪给全球经济造成的损失将达到平均每年 10.5 万亿美元。[7] 根据 Ponemon Institute 和 IBM 发布的《2021 年数据泄露成本报告》，数据泄露的年度平均成本达到历史新高水平，同时数据泄露事件的数量迅猛增长了 68%，从而进一步增加了这些成本。[8]

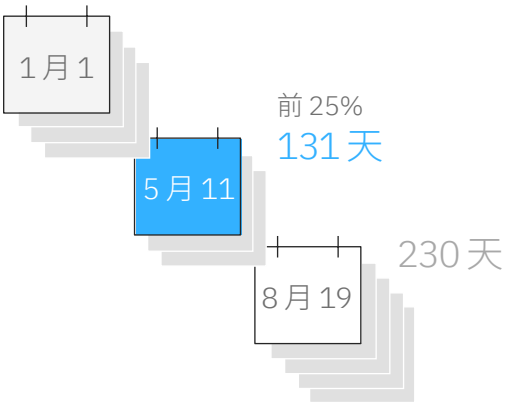
我们的研究结果表明，整个安全生命周期中的初始 AI 投资正在帮助组织更有效地打击网络犯罪，这一趋势已反映在安全成本绩效指标上。事实上，前 25% 的 AI 采用者（各项指标以第 25 分位或第 75 分位为界）认为 AI 和自动化显著改善了三项关键绩效指标，从而大幅改善了其安全部门的绩效和效能。（有关绩优采用者绩效衡量的更多信息，请参阅第 32 页的“研究和分析方法”。）具体改进包括：

- 将网络安全总成本降低了至少 15%，这意味着提高了整个安全生命周期流程（包括保护和预防以及检测和响应）的效率和生产力；
- 将数据泄露成本降低了至少 18%，这意味着提高了检测和响应流程的效率。具体收益包括减少或规避了相关的运营和声誉成本，包括潜在业务损失（客户和供应商）、投资和未来商机；
- 将其安全投资回报率 (ROSI) 提高了 40% 或更多，这表示减少和规避了网络风险以及相关的运营和声誉成本。

除了我们的研究以外，其他一些研究也发现 AI 可以实现类似的收益。Ponemon Institute 和 IBM 指出，事实证明 AI 和自动化是降低数据泄露总成本的最为重要的因素。[9] 同样，IBV 针对零信任安全性的研究发现，61% 的领先组织使用安全自动化和编排来降低安全资本和运营成本。[10]

这些研究结果针对“安全领导者为何应在整个安全生命周期中结合采用 AI 和自动化？”这一问题提供了令人信服的证据。接下来，我们将探讨安全领导者如何在两个关键领域改善绩效：“保护和预防”以及“检测和响应”。

某组织在未采用 AI 的情况下需要 230 个日历日来检测和响应网络事件并从中恢复，而如果采用 AI，则可以将这一时间缩短多达 99 天。



第 2 章

AI 助力改善整个安全生命周期

云安全中固有的责任共担模型、零信任方法中固有的 IT 集成再加上 AI 和自动化，构成了未来安全运营的基本能力。

安全 AI 和自动化可以生成富有意义的洞察，并结合情境化和历史数据，可改善与组织内部和外部合作伙伴之间的协同和协作。这样一来，经验丰富的技术人才便可腾出时间来及时调查威胁，从而防患于未然。通过改善保护和预防流程以及检测和响应流程的绩效，AI 和自动化可以对组织的整体网络弹性产生重大积极影响。

为了更好地了解这种影响，我们研究了 AI 采用者如何在整个安全运营生命周期中运用 AI 和自动化，包括保护和预防流程以及检测和响应流程。基于从研究中获取的洞察，我们评估了这些技术组合可如何改善运营效率和效能，并解释了绩效改进可如何创造下游业务收益，例如提高工作效率和改善员工体验。

通过改善运营绩效，AI 和自动化有助于增强整体网络弹性。

保护和预防：利用 AI 降低风险、控制成本以及建立信任

挑战

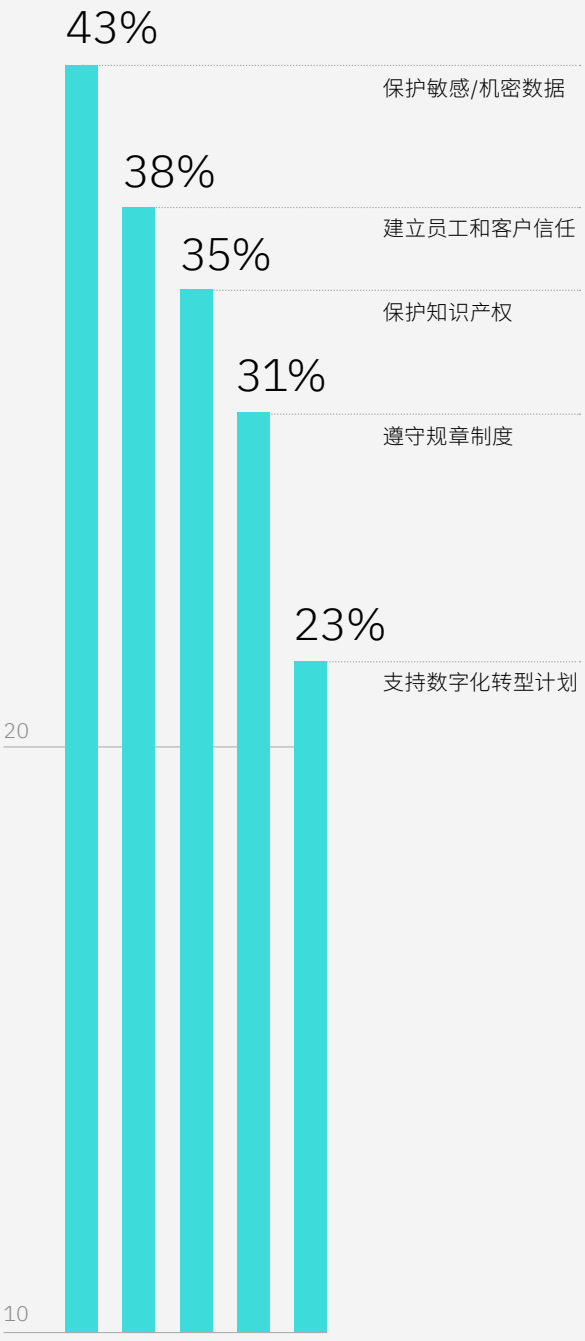
近年来，随着远程工作者、云端应用和云端服务器的数量持续增长，企业需要监控的端点和应用数量也在与日俱增。网络犯罪分子正在利用互联服务来创建新的威胁途径，攻击方式也从概率性网络钓鱼演变为协同式勒索软件活动 — 这种活动旨在胁迫企业支付赎金。根据 IBM X-Force® 的研究数据，勒索软件是 2021 年最主要的攻击类型，而网络钓鱼是最主要的入侵途径（占攻击总数的 41%）。[11]

日益复杂的网络安全威胁对企业及其客户产生了巨大的影响。为了建立并增强客户、合作伙伴和员工的信任，AI 采用者的优先目标是降低风险、保护敏感数据和保护知识产权（参见图 4）。

图 4

AI 安全防护

AI 采用者的目标是保护业务和客户数据并保持信任



问：在您的组织中，AI 的主要驱动力是什么？（目标侧重于保护和预防。）

AI 价值主张

结合 AI、自动化和零信任模型有望创造最重要的业务优势。在保护和预防方面，这些功能不仅可以消除运营孤岛，而且还将提高整个组织数字资产（数据、设备、用户、网络、工作负载、应用和整个生态系统中的合作伙伴交互）的可见性。

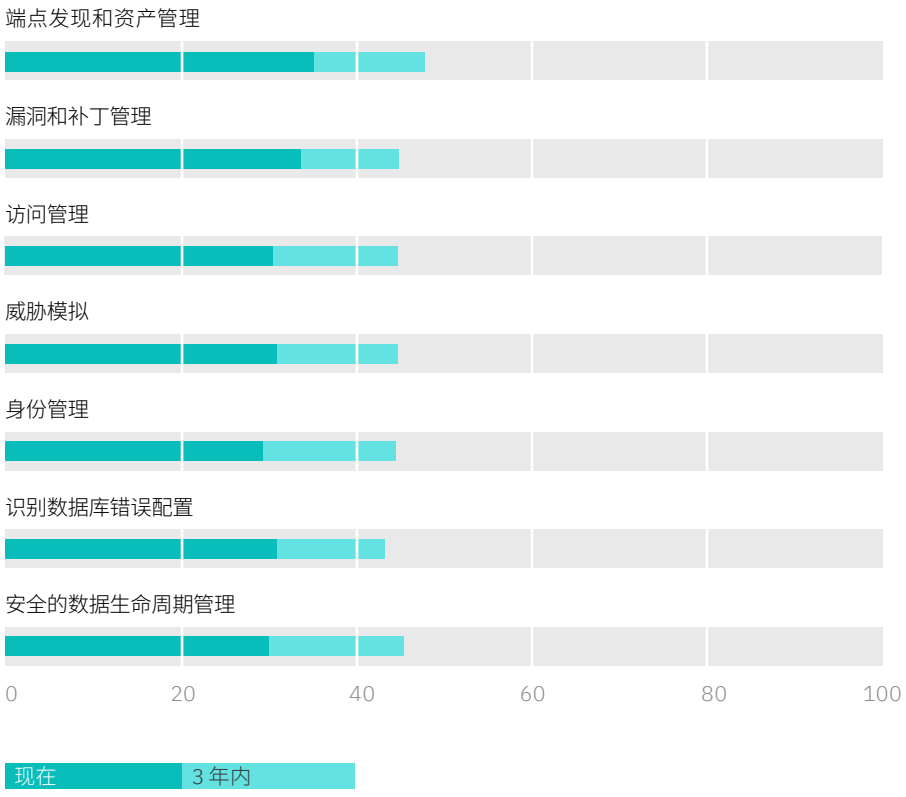
AI 和自动化可以定期执行敏感数据发现和分类，包括本地部署系统、端点、传输中和云端，从而改进数字资产视图。借助这些技术，企业可以利用源数据和元数据为任何特定交互重建完整上下文，还可以了解敏感数据的位置、哪些人可通过哪些方式访问敏感数据、哪些人在哪些时间访问了敏感数据以及执行了哪些操作。这有助于满足数据隐私和监管合规要求，并支持监控和控制对于高度敏感型数据存储库的访问。

为了更全面地了解数字环境，AI 采用者已将端点发现和资产管理列为最重要的 AI 应用场景。35% 的 AI 采用者目前正在将 AI 和自动化应用于此功能，并计划在未来 3 年内将其使用率提高至近 50%（见图 5）。紧随其后的应用场景是漏洞管理，占比达到 34%。平均而言，AI 采用者预计未来 3 年内在保护和预防领域 AI 的使用量将增加约 40%。（参见观点 “AI 如何助力保护和预防”。）

图 5

将 AI 应用于保护和预防

AI 采用者正在运用 AI 来洞悉不断增长的数字资产



问：目前实施了哪些 AI 自动化应用场景？3 年后呢？（侧重于保护和预防中的应用场景。）

观点

AI 如何助力保护和预防

通过以下五大应用场景，AI 采用者正在大力投资保护其业务的潜在价值，侧重于降低风险、防范攻击并借此建立信任。

应用 AI 来实现端点发现和资产管理。未经授权的设备在组织传统安全策略的雷达下运行，因而难以检测。AI 可以学习与特定资产类型、网络服务和端点相关的上下文、环境和行为，随后企业可以限制对授权设备的访问，并防止访问未经授权的非托管设备。

应用 AI 实现漏洞管理。AI 驱动的漏洞评估可以帮助识别配置不当的设备，以便管理员删除或重新配置这些设备。运营技术 (OT) 环境中的主动漏洞扫描可能会破坏系统的稳定性，但组织可以运用 AI 和自动化来执行被动监控。此外，AI 还可以提供关于漏洞攻击的信息，从而帮助客户确定漏洞修补优先级，以便采取基于风险的漏洞管理方法。

应用 AI 来实现访问管理。企业可以运用 AI 来审计用户和应用对数据和服务的访问。建立了对敏感资源的授权之后，AI 就可以协调整个控制平面的活动，包括监控行为、标记异常、生成上下文洞察、发送预警以及启动补救措施。

应用 AI 来实现威胁模拟。威胁模拟器可以连接至组织网络中的软件端点，以便模拟网络安全事件的生命周期。它不需要与生产服务器或端点交互即可测试实时安全防御，从而让企业能够在不影响其运营的情况下识别并填补防御体系中的漏洞。

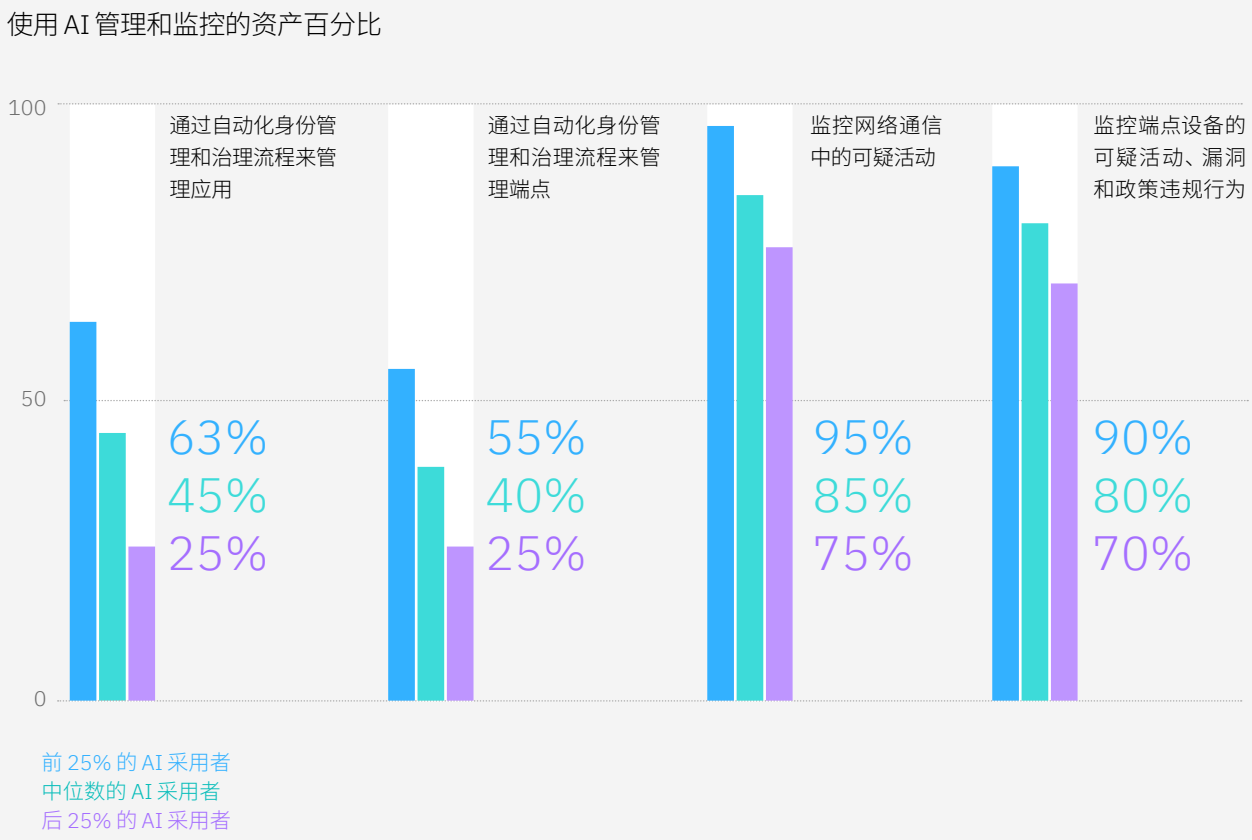
应用 AI 来实现身份管理。零信任安全运营对 IT 基础架构和安全身份验证功能提出了更高的要求，尤其是需要近乎实时地解析身份。尽管零信任可以大幅增强运营能力，但也对运营能力和协调提出了新的挑战（例如，支持远程工作人员使用来自多个位置的多个设备）。AI 可以结合历史行为、情境化数据和基于角色的策略来创建独特的用户配置文件，从而增强身份验证服务。

借助支持 AI 的自动化，组织可以为更多端点和应用提供保护，并增强网络通信监控能力（参见图 6）。绩优型 AI 采用者表示正在 63% 的应用和 55% 的端点中运用自动化身份管理和治理流程。这些数据表示通过 AI 获取的应用数量和端点数量分别增加了 67% 和 50%。如此一来，不断扩展的依赖多云服务的企业运营足迹，其可见性大大增强。

图 6

提高可见性

自动化可支持 AI 采用者
管理和监控更多资产



即便是这些领域报告的中位数百分比也反映了大量应用和端点已实现自动化管理，而且随着性能改进，未来还有进一步的增长空间。根据调研数据，AI 采用者在运用 AI 和自动化来监视网络通信和端点设备的可疑活动方面取得了更大的进展。绩优型 AI 采用者表示正在运用 AI 监控 95% 的网络通信和 90% 的端点设备。

保护和预防的真正价值源于在本质上难以衡量的因素：规避风险。通过从所有数字资产获取及时且更相关的性能洞察，安全团队可以更有效地规避威胁、降低风险以及保护和维护其组织的盈利水平和品牌声誉。

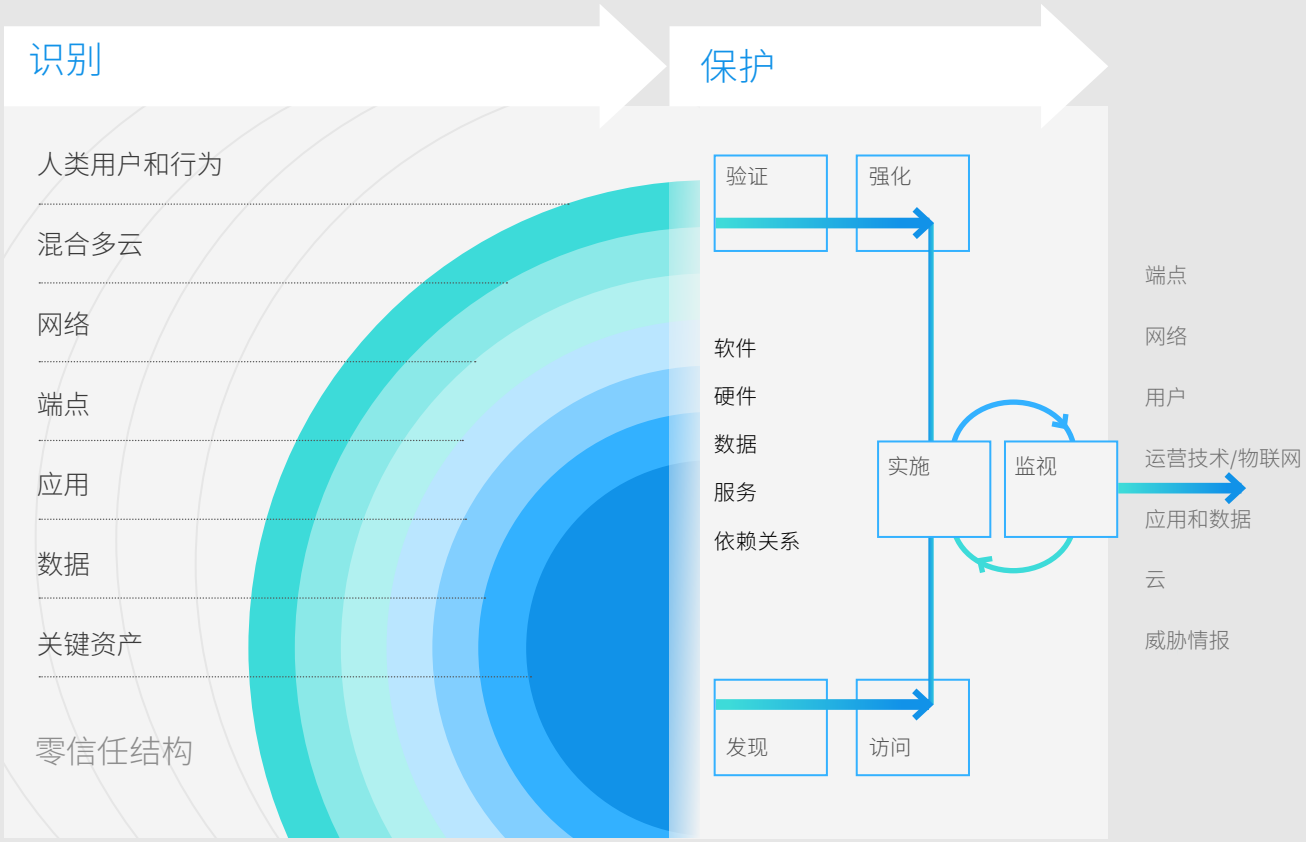
领先的 AI 采用者正在运用自动化来管理 63% 的应用和 55% 的端点。

观点

人工智能和自动化合力增强安全控制

保护和预防

AI 支持跨多云环境监控多个层

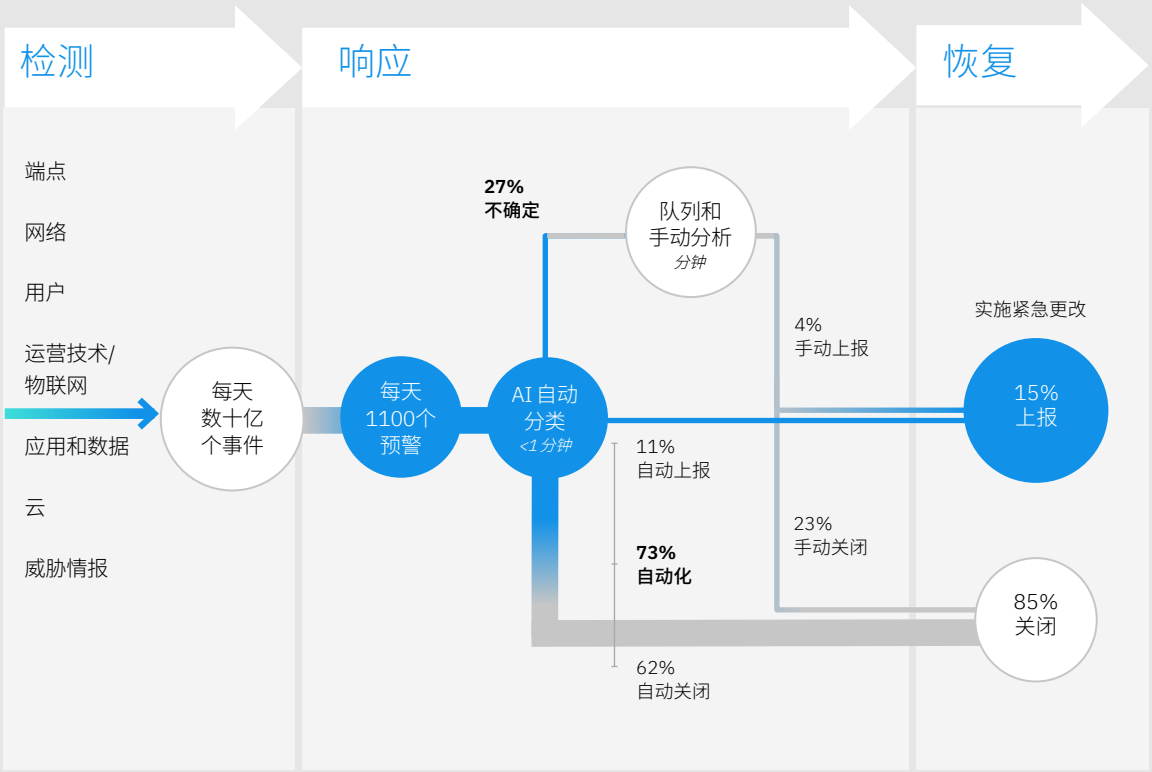


观点

结合人工智能和自动化改善安全运营绩效

检测和响应

运用人工智能和自动化缩减绩效指标



未来安全分析师的体验

未使用 AI

8 个工具/屏幕
19 个步骤
响应时间达到数小时或数天

结合 AI 和自动化

1 个屏幕
6 个步骤
响应时间只需数分钟

信息来源：IBM Security Services 基于 2021 年汇总绩效数据开展的分析和研究。
注意：所述性能阈值预计将持续改进。

检测和响应：运用 AI 提高工作效率并加快恢复速度

挑战

企业的良好运营不仅依托于防范和预防事件，还取决于能够以多快的速度检测和响应事件并从中恢复。根据零信任设计原则，安全专家应当假设其组织已经受到入侵且未来仍将再次受到入侵。

许多因素都促使组织将 AI 应用到其检测和响应活动中。如前所述，大多数组织都在快速扩大数字足迹，转型为日益开放的业务模式，其远程员工数量也在急剧增长，这些因素都导致各种新的安全事件层出不穷。许多安全组织都无法手动监控和管理安全事件，也无法快速有效地采取应对措施。

网络安全人才短缺进一步加剧了此问题。缺乏优秀的技术人才会对组织的安全状况产生重大影响 — 无论是更有效地运用资源来加快响应速度，还是运用专业能力来提高安全质量。

根据美国劳动力分析公司 EMSI 的数据，在每 100 个网络安全职位空缺中，只有 68 位合格候选人，而且其中许多人都已经处于在职状态。[12] 根据 IBV 最近开展的一项研究，组织每填补一个网络安全职位空缺（招聘到一位专业安全人才）就需要花费 150 天的时间。[13] 新入职的一线安全分析师需要借助额外的运营支持才能有效完成工作，但这也并不一定能够缓解人才短缺问题。他们通常缺乏行业经验，因此需要时间来培养威胁评估和安全排查方面的技能和信心。

AI 和自动化可以为这些安全分析师提供知识管理、案例管理和运营支持功能（例如，一线聊天机器人和自然语言知识库）。这最终将实现突破性成效：结合人类的判断力和 “AI + 自动化” 来增强智能能力。（参见观点 “AI + 自动化 — 人才革命”。）

观点

AI + 自动化 — 人才革命

网络文化意识和网络安全人才在实现安全和业务成效方面发挥着关键作用。成功的 AI 项目不会让人才落伍。AI 可以提高安全分析师的效率和效能，AI 还可以提高安全知识工作者的影响力。通过实现更灵活的互动模式，AI 缓解了一些资源和技能限制，可在安全成效中发挥决定性作用。[14]

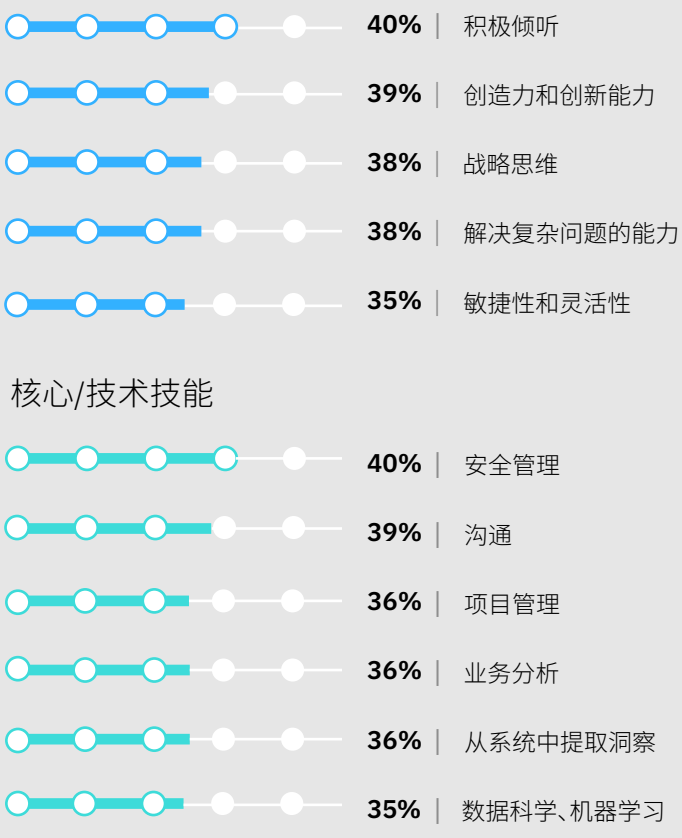
AI 采用者正面临对新人才的迫切需求。在过去的 12 个月中，AI 采用者们净增加了 15% 的新网络安全员工，并认为这一变化的 40% 归因于采取了 AI。受访高管表示，34% 的安全职位的技能需求发生了变化，其中 35% 的变化是由采用人工智能直接或间接推动的。

通过结合人为因素与技术因素，AI 采用者们可以通过对其网络安全团队进行再投资来直接解决人才短缺问题。组织可以将自动化的侧重点从成本优化转变为处理专业任务以及改善工作体验，以便在内部培养人才，助力员工提升技能。

AI 采用者优先关注员工的行为技能和技术技能。40% 的受访高管认为，在组织采用 AI 之后，员工最需要掌握的行为技能是积极倾听；而 39% 的受访者则认为创新能力和创造力是最重要的行为技能。在技术技能方面，40% 的受访高管认为安全管理技能最重要，而 39% 的受访高管则认为沟通技能最重要（见下图）。更加灵活地整合软技能与硬技能是推动释放全新 AI 价值最具前景的领域之一。

AI 对技能组合的需求

网络安全员工需要具备适当的硬技能和软技能，从而利用 AI 取得成功



问：为了适应 AI，您组织的网络安全人员需要/将需要发展/增强哪些技能？

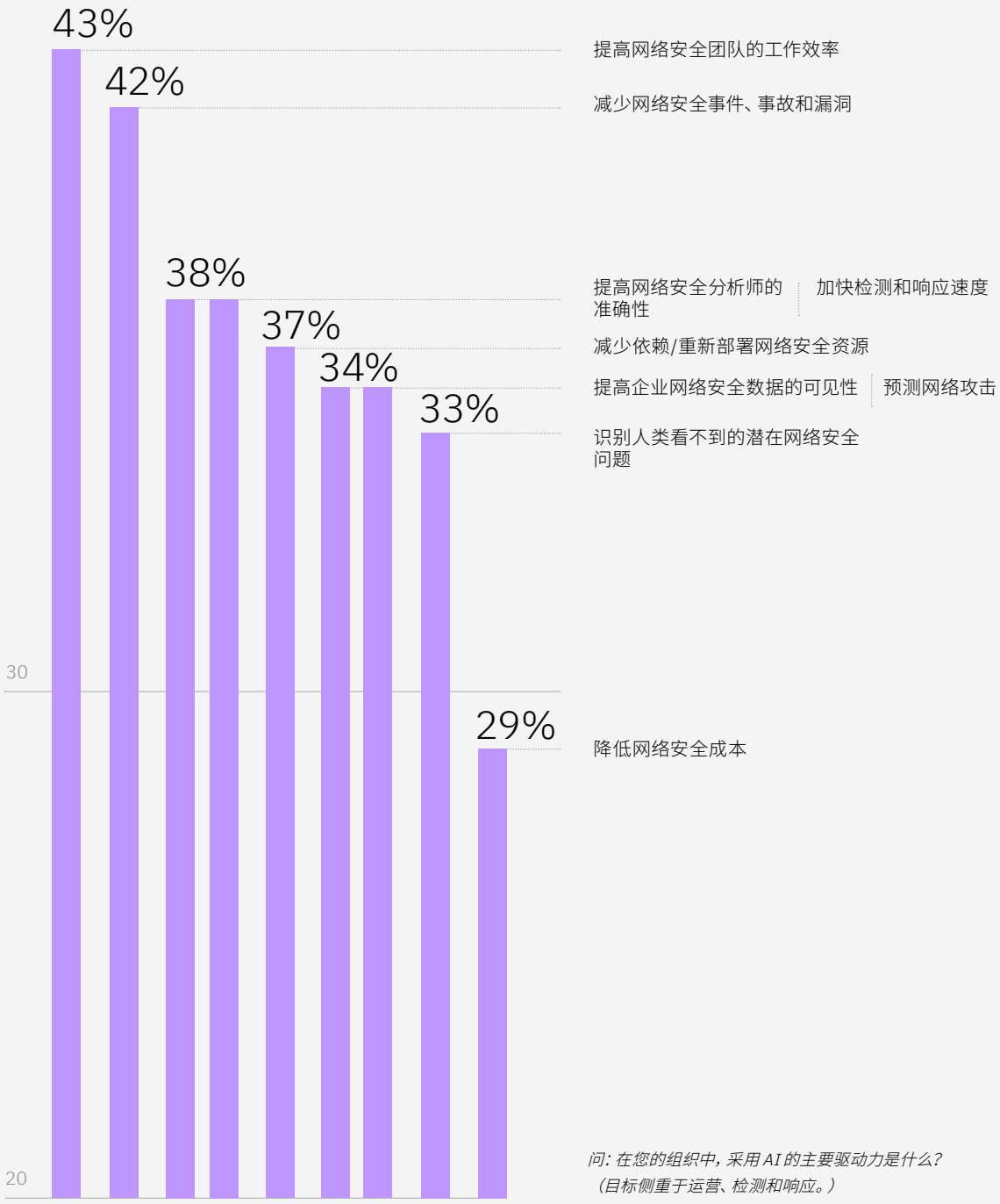
为了应对网络安全人才短缺挑战，AI 采用者正在部署 AI 和自动化来帮助超负荷运转的安全团队提升工作效率并改善工作体验。事实上，43% 的受访高管认为提高网络安全人才的工作效率是采用 AI 的首要驱动力。42% 的受访高管表示其采用 AI 的目标是减少安全事件、事故和违规，38% 的受访高管侧重于使用 AI 来提高网络安全分析师的准确性（见图 7）。

作为一个整体，AI 和自动化可以对解决安全事件的数量和速度产生巨大的积极影响，这是改善安全分析师工作环境的关键因素。通过更加深入地理解哪些威胁需要更多关注，安全分析师的工作重心可以从常规分类任务转变为价值更高的威胁调查活动。这最终将增强整个网络安全团队的处理能力和专业能力。

图 7

提高工作效率

AI 采用者希望提高安全分析师的检测和响应效率



问：在您的组织中，采用 AI 的主要驱动力是什么？（目标侧重于运营、检测和响应。）

AI 价值主张

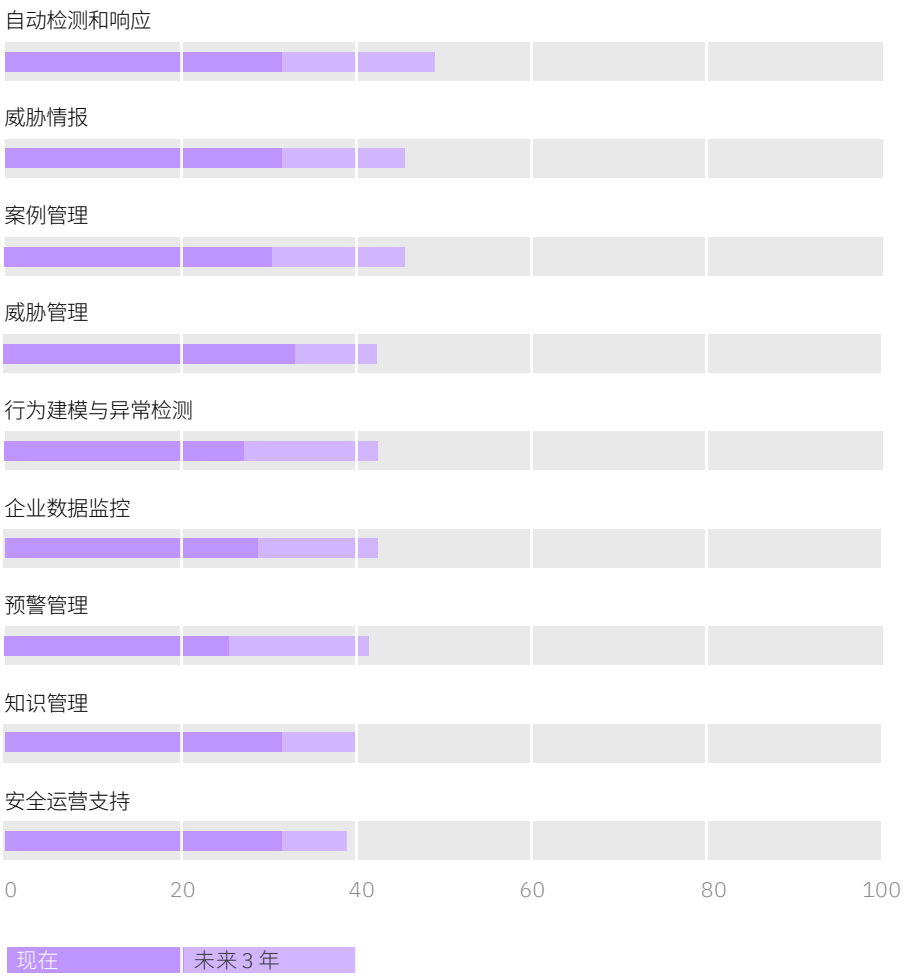
提高工作效率的秘诀是找到最具成效的领域，并在这些领域运用技术赋能员工团队。例如，在利用 AI 和自动化减少手动方法并提高效率方面，威胁检测是一个理想的应用领域。自动化、AI 驱动的调查流程可以选择性地优先保护高价值数据和资产、网段和云服务。此外，通过更加深入地洞悉网络通信、流量和端点设备，AI 和自动化可助力增强识别潜在威胁的能力，让网络安全人员能够始终如一地做出更加合理和明智的决策。

AI 采用者们认识了到运用 AI 和自动化进行威胁管理的潜力。34% 的受访高管表示这是其在检测和响应活动中应用 AI 的主要场景（参见图 8）。紧随其后的是自动检测和响应，49% 的受访高管表示这将成为其未来三年内最广泛实施的应用场景。而且，与保护和预防应用一样，AI 采用者预计在未来 3 年内，AI 在检测和响应领域中的应用平均将增长约 40%。（参见观点“运用 AI 加快检测和响应速度”）

图 8

将 AI 应用于检测和响应

AI 采用者正在运用 AI 来更快识别威胁以及主动响应网络攻击



问：目前实施了哪些 AI 自动化应用场景？未来 3 年内呢？（侧重于检测和响应中的应用场景。）

运用 AI 加快检测和响应速度

AI 采用者正在运用 AI 和自动化来大幅提高其网络安全员工的工作效率，并通过一些关键绩效指标来进行衡量。以下 5 个应用场景演示了具体应用。

自动检测和响应。安全 AI 和自动化可自动收集、集成和分析来自数百甚至数千个控制点的数据，并整合系统日志、网络流、端点数据、云 API 调用和用户行为。再结合威胁管理和预警优先级排序，组织可以通过端点检测和响应 (EDR) 以及跨层检测和响应 (XDR) 功能来为现有遥测解决方案提供强力补充。这使安全运营团队能够充分了解安全异常的情境、确定优先级顺序并投入足够安全人员来调查高影响威胁。

威胁情报。借助基于 AI 的安全智能，组织可以分析实时数据流以实时检测异常行为。结合跨域安全信息（通过集成内部遥测信号与外部情报源）可在切实可行的窗口中提供切实可行的情报，从而提高安全策略的有效性，尤其是与紧急威胁相关的安全策略的有效性。此外，还可以跨云环境应用相同的程序来扩展日志捕获功能 — 扫描可能指向更难以解释的攻击特征的不规则配置，例如零日攻击和高级持续性威胁 (APT)。

案例管理。借助安全案例管理功能，安全团队可以收集可疑活动的相关信息，并利用与案例相关的详细信息和日志来升级调查。应用 AI 可以提高数据的处理速度和处理量，还可以集成数据科学技术，从而自动对文档中的数据进行识别和分类。由于 AI 可以理解上下文，因此可以按主题对数据进行分组，而无需事先分类，从而帮助安全团队运用识别到的相关数据来进行推理并查找不明显的相似点。

威胁管理。AI 可以有效对预警进行分类，并区分假阳性和假阴性，让安全分析师能够首先关注最关键的预警，并大幅降低错过关键事件的几率。AI 还可以根据攻击特征、危害指标 (IOC) 和行为指标 (IOB) 对威胁特征进行分类和优先级排序，并触发预警。

行为建模和异常检测。自动化 AI 安全模型可以识别异常行为、动态评估漏洞并标记异常活动，包括所有潜在的危害指标。随后，机器学习可以根据情境变量、历史先例或威胁情报来源等各种因素来提出补救方案，并在特定控制点更新策略管理。

AI 采用者表示成功缩短了检测和响应事件的时间（参见图 9）。与实施 AI 之前的估算绩效相比，AI 采用者检查事件所用天数的中位值减少了 12%，而响应事件并从事件中恢复所用天数的中位值减少了 11%。领先绩优型 AI 采用者的数据反映了 AI 和自动化在改善绩效方面的巨大潜力。前 25% 的 AI 采用者表示，他们使用 AI 将事件调查时间缩短了近三分之一，并将响应和恢复时间缩短了近四分之一。他们还将停留时间缩短了 45%。

AI 采用者的数据表明，在整个安全运营生命周期中部署 AI 和自动化可以增强保护和预防功能，同时改善检测和响应能力。他们的成功揭示了组织如何在充满挑战的时期运用 AI 来大幅提高整体网络弹性。（参见案例研究 “AI 和自动化 — 改善工作环境和绩效”。）

绩优型 AI 采用者将调查网络安全事件的时间缩短了近 30%。

图 9

加速恢复

绩优型 AI 采用者可以更快
检测和响应安全事件

前 25% 的 AI 采用者
中位数的 AI 采用者
后 25% 的 AI 采用者

柱越短表示效能越高

案例研究

全球托管安全服务提供商

AI 和自动化 — 改善工作环境和绩效

一家为各行各业的数百位全球客户提供服务的托管安全服务提供商利用混合云和零信任功能实现了现代化安全运营，但仍然遇到了反复出现的容量问题。“受攻击面只会越来越大，”客户的一位首席安全分析师说道，“我们的问题有两个方面：有时会从大量来源收集到非常多的信息，而有时在一些关键时刻又缺少相关信息。”

技能和专业能力供不应求进一步加剧了问题的复杂性和难度。“我们正在争夺稀缺性人才，力争保持人才优势，”客户的一位首席高管说道。此客户的领导者首先运用设计思维和 IBM Garage™ 协作方法从业务成效的层面上明确了商机。“我们希望为安全分析师创造更加出色的工作体验。我们还希望了解更高的自动化水平将如何改善团队绩效，”客户的一位高管说道。

其一体化开发与运营团队阐明了四个主要目标：

– 为安全分析师减少噪音，让他们能够专注于处理高价值预警

– 编译情境化数据、元数据和服务日志以如实重建威胁环境，从而加快分类速度

– 通过更广泛的情境化和充实化数据/元数据加快调查速度

– 通过解释和推理提供补充性查明建议

大约一年后，此客户通过以下方式大幅提高了运营效率：

– 以高于 90% 的置信度自动分类 73%（之前只有 40%）的预警

– 使用特定于工作负载的零信任控制将总攻击面和相关风险降低约 50%

– 将攻击者停留时间和漏洞窗口减少 50%

– 将安全事件减少 75% 并将平均入侵时间 (mean-time-to-breach) 缩短一半

AI 可以为自动化提供助力，但该解决方案的在真正优势在于能够充分发挥人才的优势。AI 和自动化让安全分析师能够专注于处理影响更大的威胁，例如零日攻击、APT 检测、威胁搜寻和取证。安全分析师可以提供持续反馈，从而打造更加智能和人性化的解决方案。客户高管总结了解决方案对业务的影响：“通过引入自动化，再加上为我们团队提供更好的工作环境，对我们业务产生了巨大的积极影响。”

第 3 章

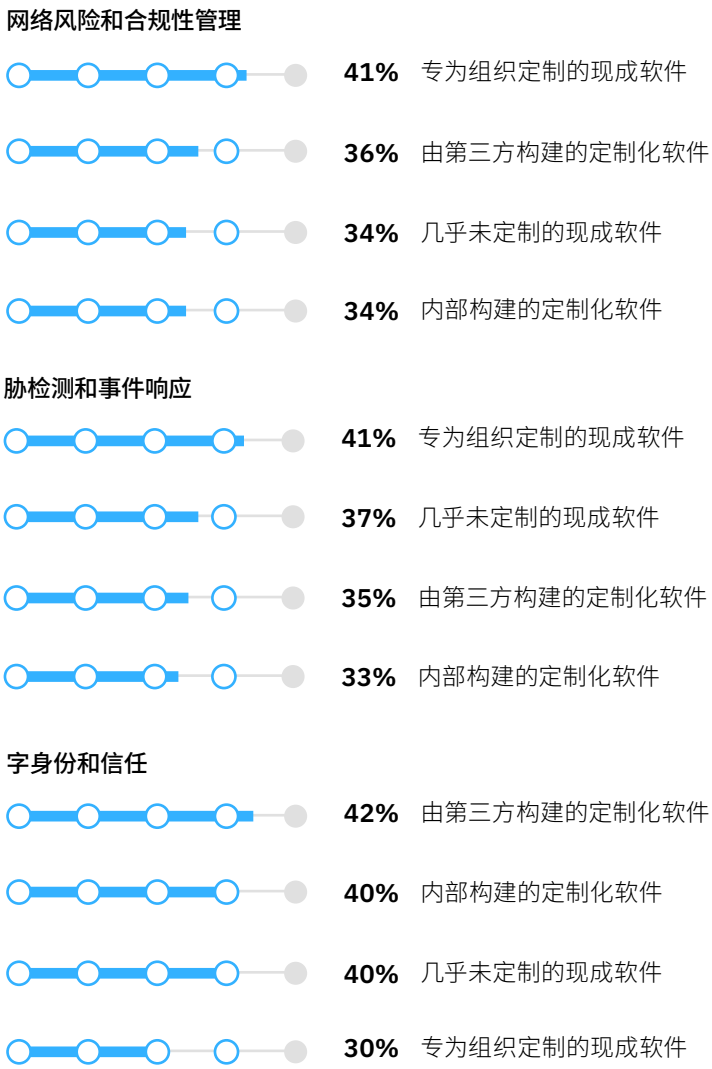
制定安全 AI 采用路线图

当您希望将 AI 洞察和自动化流程集成到组织的安全运营中时，请考虑成功的部署可能是什么样的。AI 采用者正在结合运用现成可用的解决方案和定制化工具。在网络风险和合规性以及威胁检测和事件响应方面，越来越多的 AI 采用者认为可配置的现成软件是最成功的部署类型（参见图 10）。而在数字身份和信任管理方面，AI 采用者则认为内部或第三方构建的定制化软件可实现更大的成功。

图 10

安全 AI 赋能

最成功的部署通常涉及某种形式的定制



问：您如何描述贵组织在网络风险和合规管理方面部署 AI 技术的方式？（选择前 3 项。）

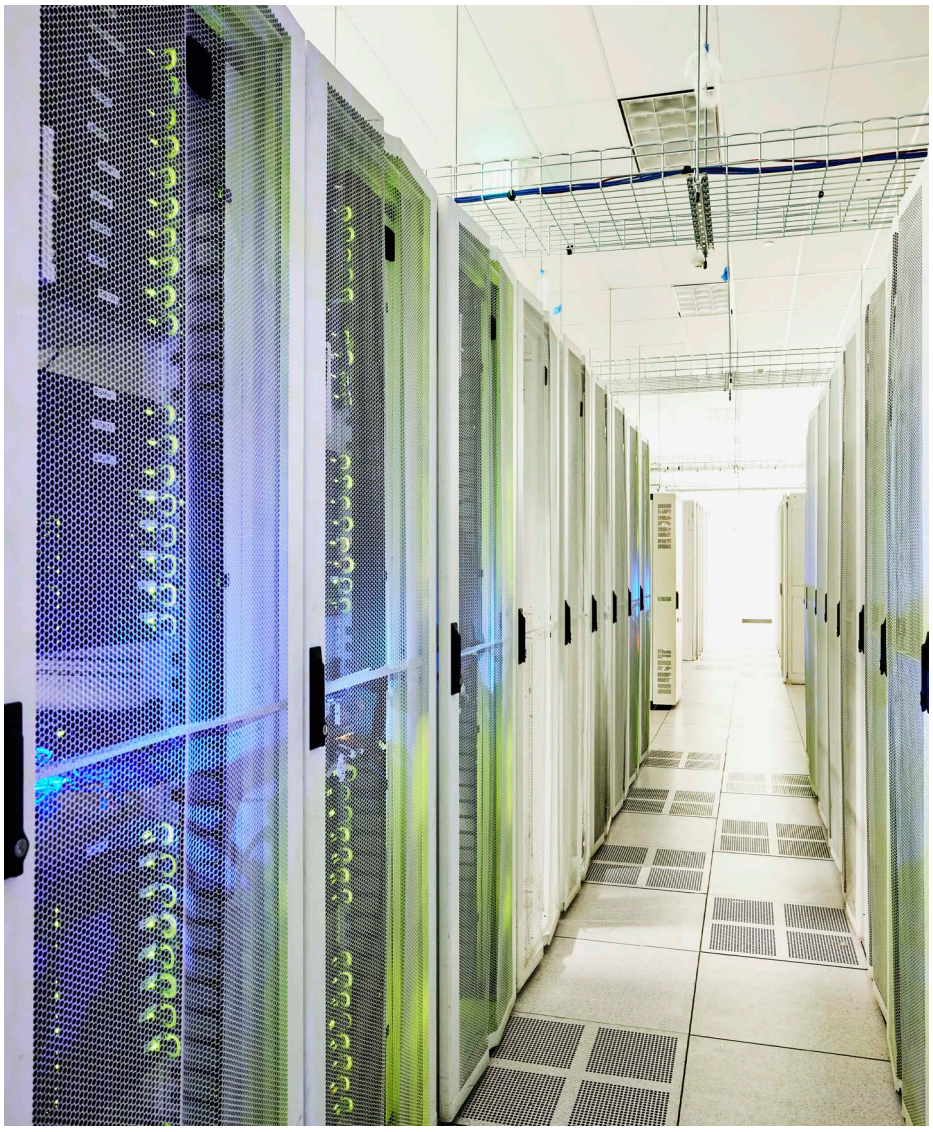
问：您如何描述贵组织在威胁检测和事件响应管理方面部署 AI 技术的方式？（选择前 3 项。）

问：您如何描述贵组织在管理数字身份和信任方面部署 AI 技术的方式？（选择前 3 项。）

高度配置和定制化开发的安全解决方案可以提供更强大的功能，实现更大的收益，但需要把与开发和支持相关的持续成本纳入到安全运营预算中。

尽管某些行业可能会受益于专业化 AI 安全应用（例如，银行和金融市场），但持续支持成本、人员配备需求和补丁计划是不可忽视的考量因素，尤其是要考虑维护和漏洞管理。许多组织都决定采用定制化解决方案，是因为在评估不断变化的风险态势和潜在安全漏洞后发现，这种方式具有令人信服的业务合理性。

定制化 AI 解决方案应当考虑持续支持成本。



行动指南

应用安全 AI 和自动化来创造业务价值

即使是最成功的安全组织也不能掉以轻心。运营是一个动态发展的过程，新的威胁途径也在不断涌现，组织必须要时刻做好充分准备并保持安全弹性。组织随时都面临被入侵的风险，不管是时间还是严重程度都无法预料。

此外，组织还需要认识到 AI 模型应当保持持续学习，这就需要由安全团队持续为 AI 模型提供新的安全效能洞察。保持 AI 模型持续学习有助于改善可实现的成效。

对于 AI 采用者而言，安全效能将影响运营效率和业务价值，同时为安全分析师创造提供更大赋能、更具自适应能力的工作环境。总的来说，这些因素将对组织的整体网络弹性产生重大积极影响。

无论您是首次试用 AI 功能还是扩展现有应用的 AI 功能，以下三项建议都可以作为您的行动指导。

01

利用多项关键安全指标执行绩效对标分析

识别安全改进的驱动因素

- 认识到将 AI 和自动化功能部署到安全运营中的战略紧迫性和战略合理性，并将这种优先级变化更新到网络风险和网络安全策略中。明确应用 AI 和自动化的目标是减少网络安全事件和漏洞，还是通过提高运营效率来降低成本？又或许是增强客户、员工或合作伙伴的信任？

根据对标分析识别需要改进的领域

- 查看关键风险和安全指标（保护和预防以及检测和响应），并与同类企业进行绩效对比分析。您可以根据差距来确定要重点改进计划的领域，应侧重于 AI 和自动化可以提供最大助益的领域。
- 一些组织提供了正式的对标分析服务，可帮助您进行对比。或者，您可以通过 Ponemon Institute、Gartner、Forrester、IDC、SANS Institute、云安全联盟 (CSA) 等在线资源查找安全指标。

02

优先考虑可创造最大价值并与您的首要安全目标相一致的安全改进计划

根据针对多项关键绩效指标的影响力和目标改进来设定优先级

- 评估改善各项关键绩效指标可以实现什么样的潜在收益。这将帮助您了解哪些领域可以在成本、效率、质量和时间等运营因素方面创造最大价值。而如果这些潜在领域与您的安全战略相一致，则在这些领域中采取措施应当可在帮助您实现战略目标方面发挥最重大的作用。

识别最具绩效改进潜力的 AI 应用场景

- 了解与保护和预防以及检测和响应最密切相关的绩效指标。例如，在保护和预防流程中，自动化身份或端点管理功能管控的应用和端点数量是一项关键指标。在检测和响应流程中，停留时间是一项重要指标。
- 请考虑这两个领域中最具绩效改进潜力的 AI 应用，以及您认为最重要的业务收益。根据这些优先级来制定您组织的安全 AI 和自动化路线图。明确您的优势并识别可在哪些方面利用合作伙伴来扩展您的专业能力。最后，选择最有可能成功的 AI 部署模式（无论是配置现有解决方案还是开发专业化解决方案），以及您希望在多大程度上依赖第三方来提供开发和支持流程。

03

为安全改进计划发展关键驱动力

定义安全 AI 策略和相应的运营计划

- 根据组织的整体网络风险和安全战略来实施、治理和管理 AI 应用，并确保全面落实到运营策略、控制和流程中。

明确并发展对于组织成功至关重要的行为技能和技术技能

- 请考虑自动化对组织网络安全团队的影响。他们会将自动化视为威胁还是机遇？就此与网络安全团队进行沟通的正确方式是什么？
- 在分析安全 AI 和自动化的成功因素时，请将人才发展和人才保留纳入考量，例如工作环境、对专业能力和专业知识的需求以及相关技能提升或再培训。请考虑在 AI 和自动化环境中需要什么样的技能组合？
- 确定 AI 和自动化可以在哪些方面为您的网络安全团队创造最大效益。识别差距并提供基于角色的培训，以培养和提升所需的行为技能和技术技能。考虑通过内部或外部劳动力合作伙伴服务来为团队提供体验式培训和网络安全模拟实践，一方面发展人才技能，另一方面增强实践经验。
- 最后，监控进展情况。随着新 AI 应用和功能的部署，根据对标分析来验证您的实际绩效，并确定各种投资的相对效率。

关于
作者

Sridhar Muppidi

首席技术官
IBM Security
linkedin.com/in/smuppidi
muppidi@us.ibm.com

Sridhar 是 IBM 院士 (IBM Fellow)，目前在 IBM Security 担任 CTO。他负责推动 IBM Security 产品和服务组合的技术战略、架构和研究，旨在帮助客户管理威胁防御以及保护数字资产。他是一位以结果为导向的技术思想领袖，在构建安全产品、为客户提供解决方案架构、推动开放标准以及领导技术团队领域拥有 25 年的经验。

Lisa Fisher

全球对标分析研究负责人
IT、安全性和云
IBM 商业价值研究院
中东和非洲地区负责人
linkedin.com/in/lisa-giane-fisher
lfisher@za.ibm.com

Lisa 负责针对各个行业和地区开展对标分析研究，从网络风险和网络安全的角度设想和阐述技术对业务的影响。Lisa 目前定居在南非。

Gerald Parham

全球安全性及 CIO 研究负责人
IBM 商业价值研究院
linkedin.com/in/gerryparham/
gparham@us.ibm.com

Gerald 在 IBM 商业价值研究院负责领导安全和 CIO 研究领域。他专注于研究网络战略、董事会咨询和生态系统级安全性，尤其是战略、风险、开放安全、信任和商业价值之间的关系。他在行政领导、创新和知识产权开发领域拥有超过 20 年的经验。

关于对标洞察

对标洞察反映的是主管对于重要业务和相关技术主题的洞察。对标洞察基于绩效数据分析以及其他一些对标评测结果。要了解更多信息，请联系 IBM 商业价值研究院：global.benchmarking@us.ibm.com

IBM 商业价值研究院

20 年来，IBM 商业价值研究院一直是 IBM 的思想领导力智囊团。我们提供有研究支持和技术支持的战略洞察，帮助领导者做出更明智的业务决策。

凭借我们在商业、技术和社会交叉领域的独特地位，IBV 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 ibm.co/ibv-linkedin 在 LinkedIn 上联系我们。

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

选对合作伙伴，驾驭多变的世界

在 IBM，我们积极与客户协作，运用业务洞察和先进的研究方法与技术，帮助他们在瞬息万变的商业环境中保持独特的竞争优势。

相关报告

零信任安全性入门

McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. “零信任安全性入门：建立网络弹性之指南.” IBM 商业价值研究院，https://www.ibm.com/downloads/cas/VB4LX4XQ

云安全的新时代

Thompson, Shue-Jane, Shamla Naidoo, Shawn Dsouza, and Gerald Parham. “云安全的新时代：利用信任网络，增强网络弹性.” IBM 商业价值研究院， 2021 年 4 月，https://www.ibm.com/downloads/cas/LZ7MXO4M

AI 伦理道德方略

“AI 伦理道德方略：助力企业建立值得信赖的人工智能文化.” IBM 商业价值研究院， 2021 年 4 月, https://www.ibm.com/downloads/cas/VQ9ZGKAE

研究和分析方法

IBM 商业价值研究院与美国生产力和质量中心 (APQC) 开展合作，对 1000 位全面负责信息技术 (IT) 与运营技术 (OT) 网络安全和信息安全的企业高管进行了调研。受访者来自 16 个行业，包括银行、金融市场、电子、软件、政府、保险、媒体、娱乐、零售和服务。这些高管分布在 5 个全球区域：非洲和中东地区、亚太地区、中美洲和南美洲地区、欧洲地区、美国和加拿大地区。未在安全部门流程中应用 AI 的企业也在调研范围之内。

受访高管应调研请求提供了 AI 在其网络风险和网络安全流程中的当前应用、计划应用以及其安全部门绩效的相关信息。由于许多因素会影响绩效，我们要求 AI 采用者（至少在一个安全流程中试点、实施、运营或优化 AI 的 637 家企业）就 AI 对常见网络风险和安全部门 KPI 的影响提供其自己的估算结果。这让我们能够计算每个 KPI 的绩效范围以及 AI 对每个 KPI 的影响范围。

本报告中的 KPI 定义如下：

停留时间是指成功入侵/攻击与发现/检测之间的时间。

响应网络安全事件并从中恢复的**平均时间（以日历日为单位）**从检测到事件并确定其范围之日开始。相关活动包括消除威胁并将受影响的系统恢复到事件前状况，测试、监控和验证受影响的系统，以及恢复运营。

调查网络安全事件的**平均时间（以小时为单位）**从安全预警升级为开展调查开始并一直持续到调查完成为止。

网络安全成本占 IT 成本的百分比包括与应用、云和数据安全、身份访问管理、基础设施保护、集成风险管理、网络安全设备、其他信息安全软件、安全服务和消费者安全软件相关的 IT 成本。这包括用于支持企业运营的流程的所有成本，不包括折旧/摊销（即基于现金流）和“转售 IT”。

安全投资回报率 (ROSI) 以百分比表示，其计算公式为：{[以美元计的估计总损失 x 网络安全总成本（网络安全解决方案或工作提供的缓解百分比）] – 网络安全总成本（网络安全解决方案或工作的总成本}/ 网络安全总成本（网络安全解决方案或工作的总成本）

数据泄露成本包括检测、升级、通知以及数据泄露发生后的响应活动所产生的直接和间接费用。数据泄露的平均成本为：（每年发生的数据泄露数量乘以所有成本因子）/（每年发生的数据泄露数量）。

本报告中使用的绩效范围定义如下：

绩优型 AI 采用者在每个指标上的表现均处于第 75 百分位或第 25 百分位，具体取决于特定指标的值是越高越好还是越低越好。如果某个特定指标的值越高越好，则绩优型组织（前 25% 的 AI 采用者）是处于第 75 百分位的组织。75% 受访者的指标值低于此水平，25% 受访者的指标值等于或高于此水平。如果某个特定指标的值越低越好，则绩优型组织是处于第 25 百分位的 AI 采用者。25% 受访者的指标值等于或低于此水平，75% 受访者的指标值高于此水平。中位数是回复分布的中点值；一半受访者的指标值低于此水平，一半受访者的指标值高于此水平。

致谢

IBV 衷心感谢 IBM Research 的安全研究人员团队，他们一直在积极探索新技术和应用创新在整个安全生命周期中的影响，成员包括 J.R. Rao、Marc Stoecklin 和 Ian Molloy。我们还要感谢 Srini Tummalapenta 和 Charles Henderson，他们毫无保留地分享了在阐述关键主题方面的专业知识。本报告撰写完成的与这些同事的慷慨贡献密不可分。

我们要感谢负责领导 IBM Security 全球安全专家团队的 Mary O’Brien 和 Chris McCurdy。IBM Security 的同事们根据与数百位全球客户的接触提供了宝贵和真实的建议。他们的工作为我们的大部分研究提供了重要基础。

最后，我们还要感谢为我们编撰本报告提供了大力支持的多位 IBV 同事，包括 Dave Zaharchuk、Kirsten Palmer、Heba Nashaat、Sherihan Sherif、Joanna Wilkins、Angela Finley 和 Kathy Cloyd。IBV 每周都会发布基于主要研究的新思想领导力报告。每份报告都由多元化的研究、分析和创意专业团队提供支持，他们合作精心创建了这些优质报告。

备注和参考资料

1 Turton, William, and Kartikay Mehrota. “Hackers Breached Colonial Pipeline Using Compromised Password.” Bloomberg. June 4, 2021. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password; Holmes, Aaron; “Ransomeware gangs targeted 3 different US water treatment plants this year in previously unreported attacks, according to federal agencies.” Insider. October 16, 2021. https://www.businessinsider.com/3-us-water-treatment-plants-attacked-by-ransomware-gangs-report-2021-10

2 Vigliarolo, Brandon. “Report:Pretty much every type of cyberattack increased in 2021.” TechRepublic. February 17, 2022. https://www.techrepublic.com/article/report-pretty-much-every-type-of-cyberattack-increased-in-2021/; 2022 IBM X-Force Threat Intelligence Index.” IBM Security. February 2022. ibm.com/security/data-breach/threat-intelligence/

3 “SolarWinds hack was ‘largest and most sophisticated attack’ ever: Microsoft president.” Reuters. February 14, 2021. https://www.reuters.com/article/us-cyber-solarwinds-microsoft/solarwinds-hack-was-largest-and-most-sophisticated-attack-ever-micro-soft-president-idUSKBN2AF03R; Robertson, Paul. “Best of 2021—Worldwide Hack: Microsoft Exchange Server Zero-Day Exploits.” Security Boulevard. December 27, 2021. https://securityboulevard.com/2021/12/worldwide-hack-microsoft-exchange-server-zero-day-exploits/; Torres-Arias, Santiago. “What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what’s at stake.” The Conversation. https://theconversation.com/what-is-log4j-a-cybersecurity-expert-explains-the-latest-internet-vulnerability-how-bad-it-is-and-whats-at-stake-173896

4 “The 2021 CIO Study. The CIO Revolution: Breaking barriers, creating value.” IBM Institute for Business Value. November 2021. ibm.co/c-suite-study-cio

5 Schneier, Bruce. “The Coming AI Hackers.” Harvard Kennedy School, Belfer Center for Science and International Affairs. April 2021. https://www.belfer-center.org/publication/coming-ai-hackers

6 “AI & Cybersecurity: Balancing Innovation, Execution & Risk.”Pillsbury Law and The Economist Intelligence Unit. September 9, 2021. https://www.pillsburylaw. com/en/news-and-insights/ai-and-cybersecurity-balancing-innovation-execution-and-risk.html

7 Morgan, Steve. “Cybercrime to Cost the World $10.5 Trillion Annually by 2025.” Cybercrime Magazine. November 13, 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

8 “Cost of a Data Breach Report 2021.” IBM Security and the Ponemon Institute. July 2021. ibm.co/security/data-breach. “Identity Theft Resource Center’s 2021 Annual Data Breach Report Sets New Record for Number of Compromises.” Identity Theft Resource Center. January 24, 2002. https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

9 “Cost of a Data Breach Report 2021.” IBM Security and the Ponemon Institute. July 2021. ibm.com/security/data-breach

10 McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. “Getting started with zero trust security: A guide for building cyber resilience.” IBM Institute for Business Value. July 2021. ibm.co/zero-trust-security

11 “2022 IBM X-Force Threat Intelligence Index.” IBM Security. February 2022. ibm.com/security/data-breach/threat-intelligence/

12 Hatton, Tim. “The Cybersecurity Talent Shortage:An Urgent Threat.” EMSI. March 8, 2022. https://www.economicmodeling.com/2022/03/08/the-cybersecurity-talent-shortage/

13 McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. “Getting started with zero trust security: A guide for building cyber resilience.” IBM Institute for Business Value. July 2021. ibm.co/zero-trust-security

14 Brandenburg, Rico and Paul Mee. “Cybersecurity for a Remote Workforce.” MIT Sloan Management Review. July 23, 2020. https://sloanreview.mit.edu/article/cybersecurity-for-a-remote-workforce/

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 | 2022 年 8 月

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

9NGZA7GK-CNZH-01