2026 版本

SafePloy 安策

THALES
CYBERSECURITY

数据威胁报告

代理时代的数据安全：人工智能是新的内部威胁

cpl.thalesgroup.com

#2026数据威胁报告

目录

由

S&P Global
Market Intelligence

资料来源：2026年数据威胁报告定制调查
由泰雷兹公司委托的标普全球市场情报451研究项目

引言

数据安全已成为企业人工智能战略的核心议题，因为企业能否成功实施AI项目，关键在于能否持续、可控地访问其专有数据源。2026年泰雷兹数据威胁报告深入剖析了企业在保障数据这一核心资产安全的同时推动创新时，必须应对的复杂权衡。

人工智能与智能代理系统的激增正加剧数据管理和安全压力，数据显示专门用于人工智能安全预算的受访者比例同比激增50%。企业在确保安全获取构建AI价值的原始数据时，正面临数据质量和安全的双重挑战。随着智能应用获取的数据量持续扩大，企业必须完善数据安全与管理机制，避免让人工智能演变成新的内部威胁。

企业正面临加速运营的压力，但安全运维的复杂性却让这些努力举步维艰——安全工具集的泛滥、混合云与多云IT架构的日益复杂化，都让安全防护雪上加霜。人工智能技术正迫使企业整合聊天界面、模型上下文协议服务器等新元素，而安全团队却在这些新兴技术的安全防护上举步维艰。威胁态势也在持续演变，攻击者运用人工智能技术，量子计算风险日益凸显。更棘手的是，安全团队脚下的AI生态系统正不断发生剧变。

尽管今年的《数据威胁报告》呈现积极态势，但要确保企业最敏感数据的安全仍需加倍努力。该报告汇总了来自20个国家的3100余位受访者的调研数据。多数企业采用全多云运营模式，其数据和应用程序分散部署在不同云服务商平台，不过并非所有企业都真正践行了这一模式。

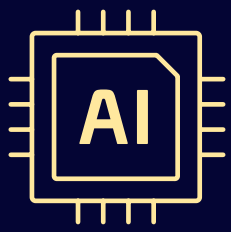
将今年的调查结果与往年数据对比，我们发现几个值得关注的领域。云环境中大量敏感数据仍未加密，云应用和云管理基础设施仍是攻击者的主要目标。云安全运维的复杂性尤其具有挑战性，特别是在人员配置受限的情况下。正如其名称所示，云安全需要同时具备云运维和安全应用的专业能力，而这两方面都存在人才短缺问题。此外，随着人工智能应用对数据量和算力需求的持续增长，安全从业者需要在更大规模上应对访问控制、身份验证和权限授权等挑战。

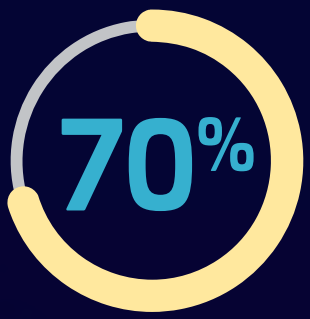
关键发现

AI时代安全优先级正在改变

人工智能安全支出持续攀升——

30% 目前，许多组织已为人工智能安全设立了专项预算（从20%上升），但仍有超过一半（**53%**）的组织仍在使用现有安全预算来资助人工智能安全。





在AI安全领域，AI生态系统内部的变化速度是首要考量因素，70%的受访者将变化速度列为最突出的AI风险。

61%

他们报告称，其人工智能应用正遭受攻击者攻击，其中敏感数据成为首要攻击目标。

人工智能驱动的攻击成为突出威胁——**59%**已经出现

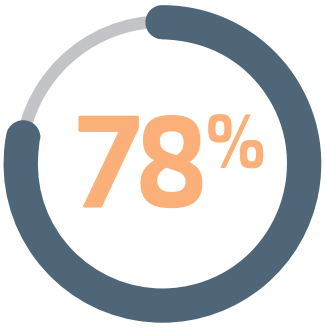
深度伪造攻击

48%

因人工智能生成的虚假信息而遭受声誉损害。

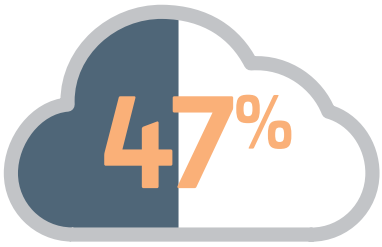
报告指出，人工智能生成的虚假信息和深度伪造内容显示出第二高的攻击增长。

数据保护在人工智能时代至关重要



高管层报告没有发生任何违规行为，而他们的IT和安全团队的违规率则为**57%**。

52% 鉴于身份与访问管理是最紧迫的安全领域，攻击者正利用凭证进行攻击。



云端敏感数据中仅有约半数经过加密。

完全掌握其数据存储位置。

50%

将密钥管理列为应用安全的首要关注点。

复杂性限制了对数据安全态势的清晰洞察

安全复杂性带来更大风险——

工具计数较高

77% 配备五种或更多数据保护工具

7 工具是数据保护与监控的平均值

46% 拥有五个或更多关键管理系统

只有 **39%** 对数据安全工具的理解充满信心

28% 将人为错误列为违规的主要原因，但**63%**将国家攻击者列为三大最严重问题之一。

审计失败与更高的违规风险相关——

只有 **6%** 通过审计的机构中，有**30%**报告没有过去违反规定的情况，而未通过审计的机构中，没有报告过去违反规定的情况。

云是重要的攻击目标

云资产是三大主要攻击目标——

被引证人

35% **34%** **32%**

云存储、云应用和云管理基础设施是三大主要攻击目标。

凭证盗窃是针对云基础设施的主要攻击手段——

67% 凭证盗窃和机密信息滥用现象日益严重。

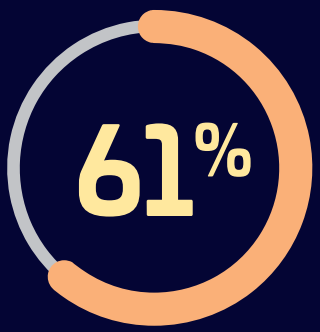
地缘政治风险上升重塑数据主权

54% 正将应用程序和数据架构的重构与重写作为实现主权目标的主要工作重点。

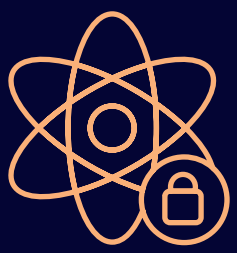
36% 认为加密和密钥管理等加密保护措施足以实现数据主权。

未来风险，今日显现

量子安全问题转向现实层面：先收割后解密（HNDL）



被引为首要关注点。



各组织正采取行动以减轻量子风险

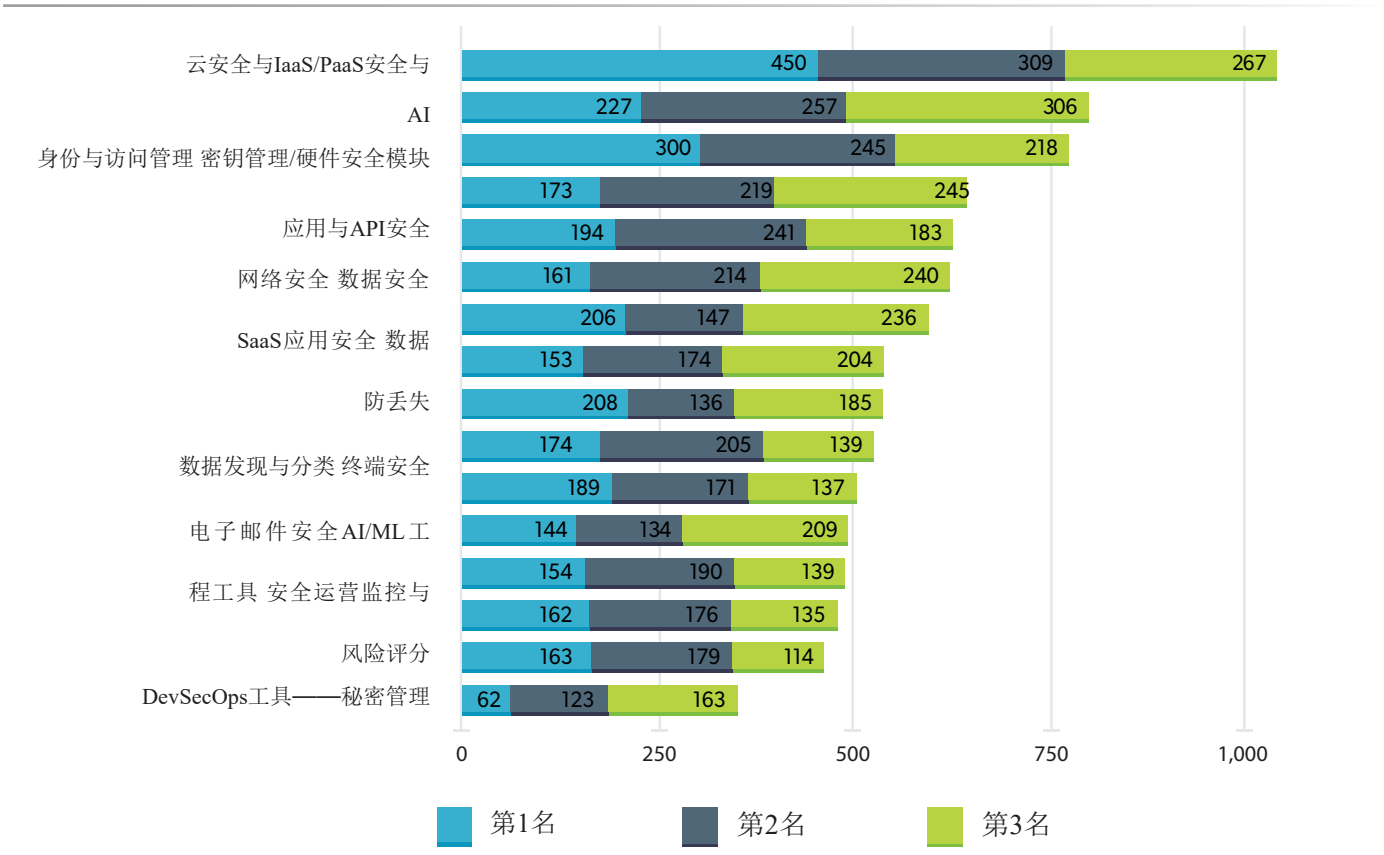
59%

正在对后量子密码学（PQC）算法进行原型设计与评估。

人工智能与智能运营带来的安全压力持续加剧

安全团队正面临企业采用人工智能带来的快速变革，而智能代理的引入更让本已复杂的安全生态雪上加霜。根据451研究公司《企业之声》近期发布的智能代理AI研究报告，超过三分之一的企业（34%）表示已部署嵌入式智能代理，更有73%的企业计划在12个月内投入使用。智能应用带来的数据使用量和处理速度呈爆发式增长，企业已在数据管理和安全防护方面面临严峻挑战。在《数据威胁研究》中，仅有三分之一受访者能全面掌握企业数据存储位置，而能对所有数据进行分类管理的企业比例也仅略高于39%——而数据分类管理正是实现有效数据保护的关键步骤。

安全支出优先事项



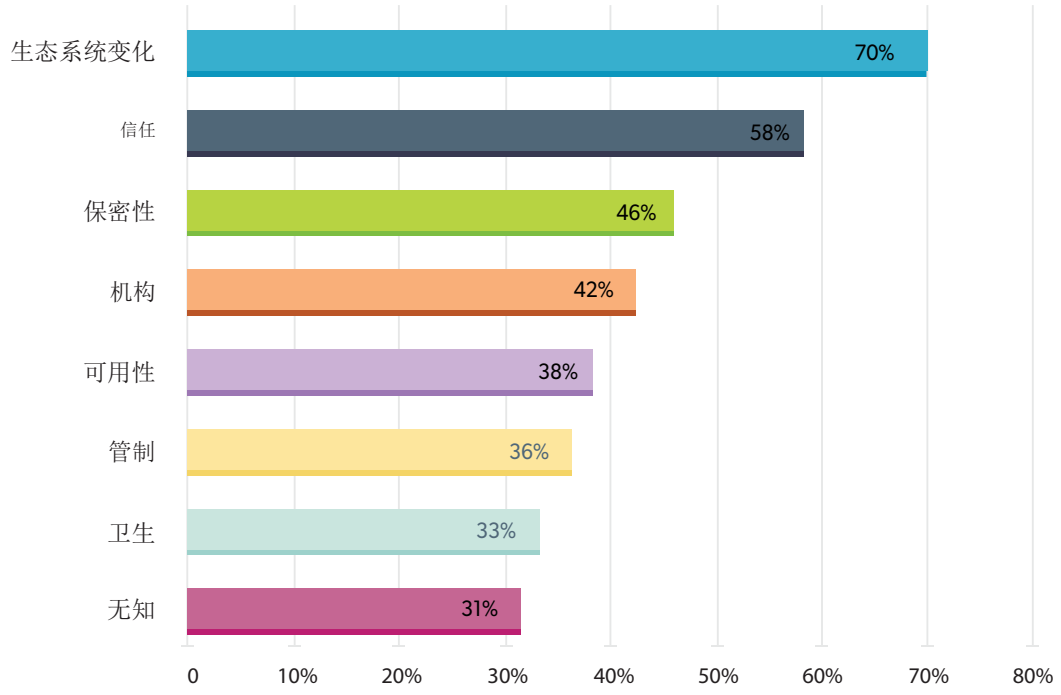
注：本文档中所有图表均源自标普全球市场情报451研究公司2021-2026年度数据威胁定制调查。

人工智能安全防护面临严峻挑战，尤其是在技术日新月异的背景下。值得注意的是，人工智能生态系统的快速变化已成为最突出的安全隐患：70%的受访者将其列为三大风险源之一。保护移动目标本就困难重重，而人工智能智能体只会让这类目标的数量和速度持续攀升。在基于人工智能和大语言模型的攻击中，针对敏感数据泄露的攻击增长最为显著。在17个重点领域中，人工智能安全支出的优先级仅次于云安全，位列第二。四分之一的受访者将人工智能安全列为三大支出重点。

锁定移动目标难度极高，而人工智能智能体只会进一步增加此类目标的数量与移动速度。

人工智能正被攻击者所利用，这要求防御策略必须与时俱进。在人工智能攻击类型中，由AI生成的虚假信息（包括深度伪造）已成为增长第二快的攻击类型。支撑AI应用和数据的基础设施仍是攻击者的主要目标：基于云的资产仍是今年数据攻击的首要目标。鉴于AI使用海量数据且其代理程序的可发现性日益增强，加密已成为必要措施。如果组织内部人员无法找到、分类和保护重要数据，攻击者很可能会找到获取这些数据的途径，后果难以预料。从许多方面来看，人工智能已成为新型内部威胁。

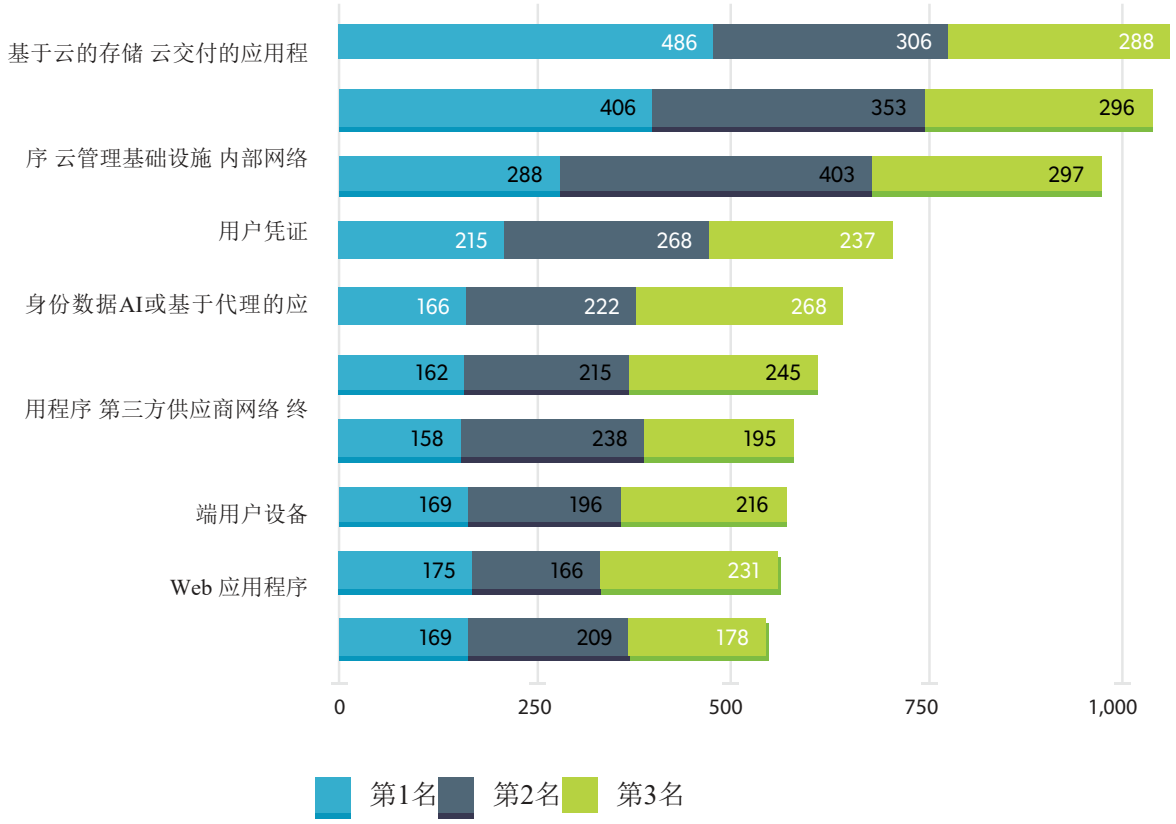
最令人担忧的人工智能安全风险



数据威胁态势

研究结果有助于描绘数据威胁的全貌。各机构正密切关注攻击方式的变化，并积极应对新型攻击手段。最新调查显示，云资产再次成为三大主要攻击目标，其中云存储（35%）、SaaS应用（34%）和云管理基础设施（32%）位列网络攻击首要目标。排名靠后的身份安全问题也引发关注：用户凭证从一年前的第八位跃升至第五位，被21%的受访者列为三大攻击目标之一。与此同时，身份数据从第十位攀升至第六位，20%的受访者将其纳入三大攻击目标之列。

首要攻击目标



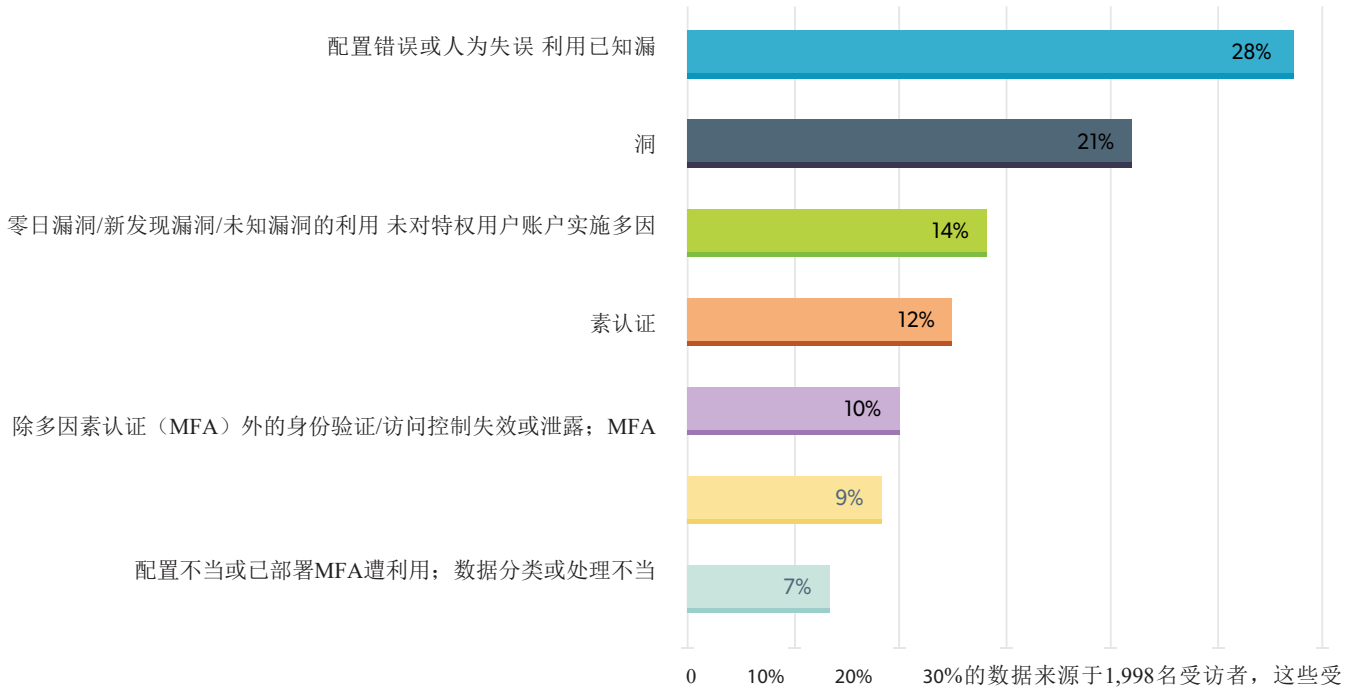
.基于云的资产再次成为三大攻击目标，其中云存储占比最高，达35%...

今年的结果反映出审计失败和报告违规事件的发生率相对稳定。

略超半数的受访者表示从未发生过数据泄露事件：54%的机构报告未发生云服务泄露，57%的机构报告未发生本地系统泄露。类似比例（58%）的机构表示在过去12个月内通过了所有合规审计。延续往年趋势，审计未通过的机构更可能报告数据泄露事件。在审计未通过的机构中，仅有6%表示从未发生过泄露事件，而通过所有审计的机构中这一比例上升至30%。

部分企业对数据泄露历史的认知可能存在不足，数据显示不同岗位上报的泄露事件存在显著差异。与管理层或实务人员相比，高管层对数据泄露事件的识别率明显偏低。超过四分之三（78%）的CEO、总裁和董事总经理表示其所在机构未发生过本地数据泄露事件，而涵盖所有层级实务人员的全样本调查显示，这一比例降至58%。云数据泄露事件的差异虽小但仍值得关注：62%的高管表示无云泄露记录，而整体调查群体中该比例为54%。这些差异可能对安全预算的优先级分配产生实质性影响。

数据泄露的最常见原因



访者的所在机构都曾遭遇数据泄露事件。

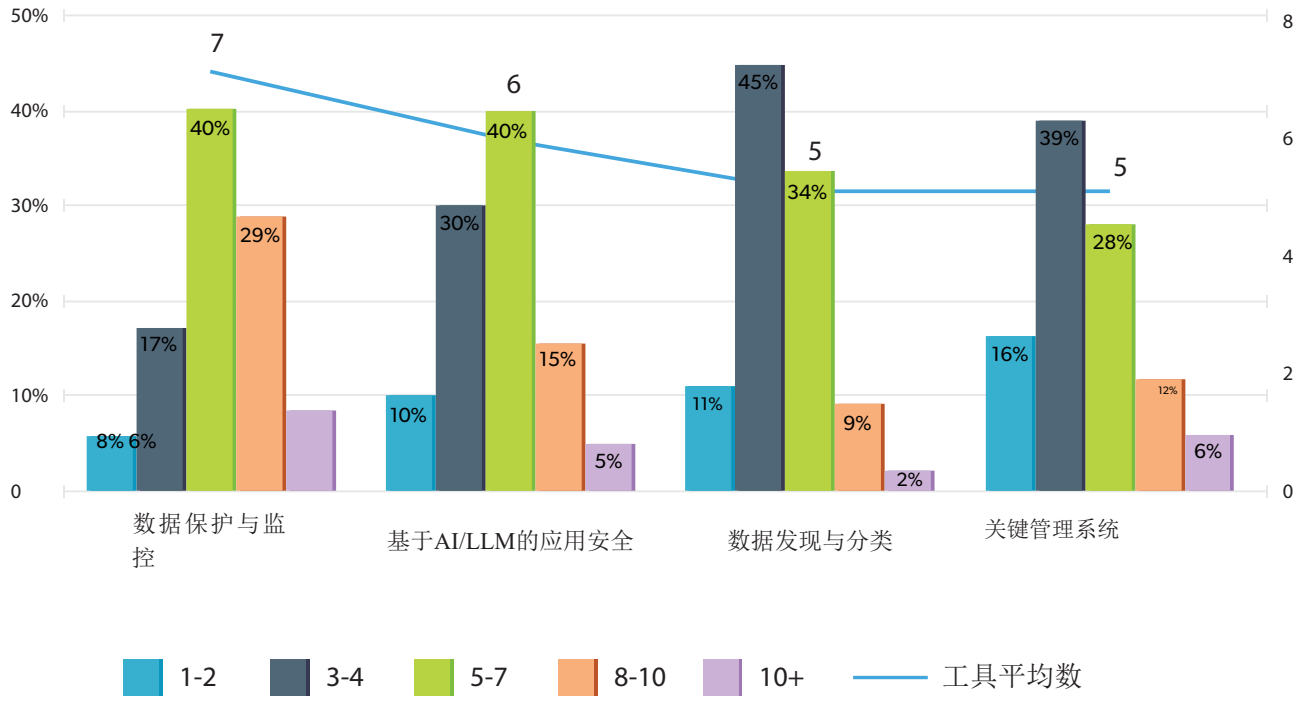
人为失误仍是数据泄露的头号元凶（占比28%），远超已知漏洞和未知漏洞的利用这两个第二大常见诱因。这表明运营问题堪称风险源头，也凸显出必须直面安全挑战中的人为因素。由于人为失误竟未被列为首要安全隐患，这就要求我们转变安全防护的优先级考量——必须重新审视安全缓解策略的侧重点。

复杂性影响安全有效性

复杂性对安全运营造成的负面影响，始终是本报告的核心议题。今年的调查深入剖析了导致复杂性加剧的关键因素——安全工具泛滥。这种现象通过增加安全团队需要监控和维护的系统数量，进一步加剧了复杂性。它要求协调整合来自不同渠道的监控结果和警报，还可能造成安全覆盖的盲区。鉴于人为失误是报告中披露的首要安全漏洞原因，运营层面的复杂性很可能正是导致安全漏洞的主要诱因。

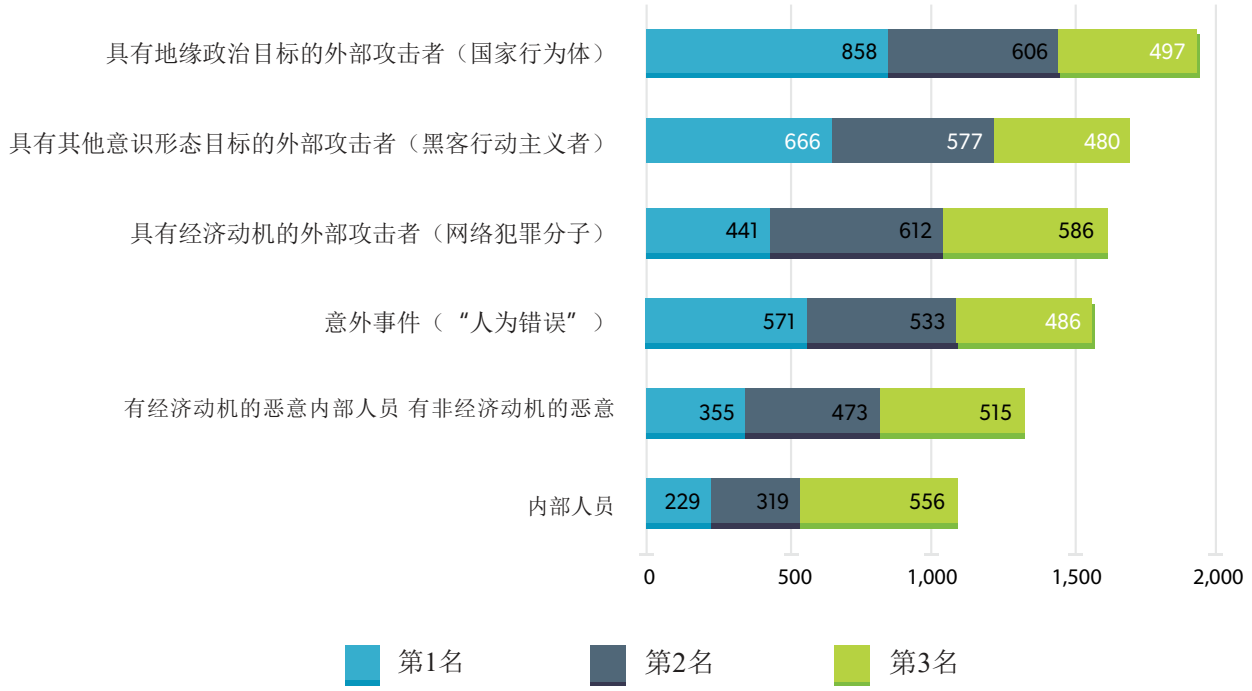
企业可能通过自然增长和人为干预两种方式增加安全工具数量。自然增长方面，不同团队或项目可能重复采购相同的安全工具；人为干预方面，企业并购可能导致多个安全工具组合被整合到统一的安全团队中。无论成因如何，研究结果显示安全工具的分散使用现象普遍存在。其中数据保护与监控领域最为突出，企业平均使用七种工具，73%的企业使用五种及以上工具。随着人工智能应用的普及，数据安全关注度持续提升，这一现象尤其值得关注。人工智能安全工具的分散使用程度位居次席，平均每家企业使用六种工具，其中60%的企业报告使用五种及以上工具。

数据发现与分类数量
以及正在使用的密钥管理系统



然而，安全工具整合仍面临阻力。任何取消安全管控的决定都需经过审慎评估。但令人意外的是，当被问及抗拒整合工具的原因时，83%的受访者表示其他可用工具存在兼容性或功能不足的问题。这更令人担忧的是，仅有39%的受访者对现有工具的理解和掌握程度表示高度自信。这种矛盾思维——既坚信替代工具功能缺失，又普遍缺乏对这些工具的认知——暗示安全决策者可能不愿改变自己不理解的事物。

最令人担忧的威胁行为者



无论出于何种阻力原因，工具整合都是简化和扩展安全操作的必要手段。

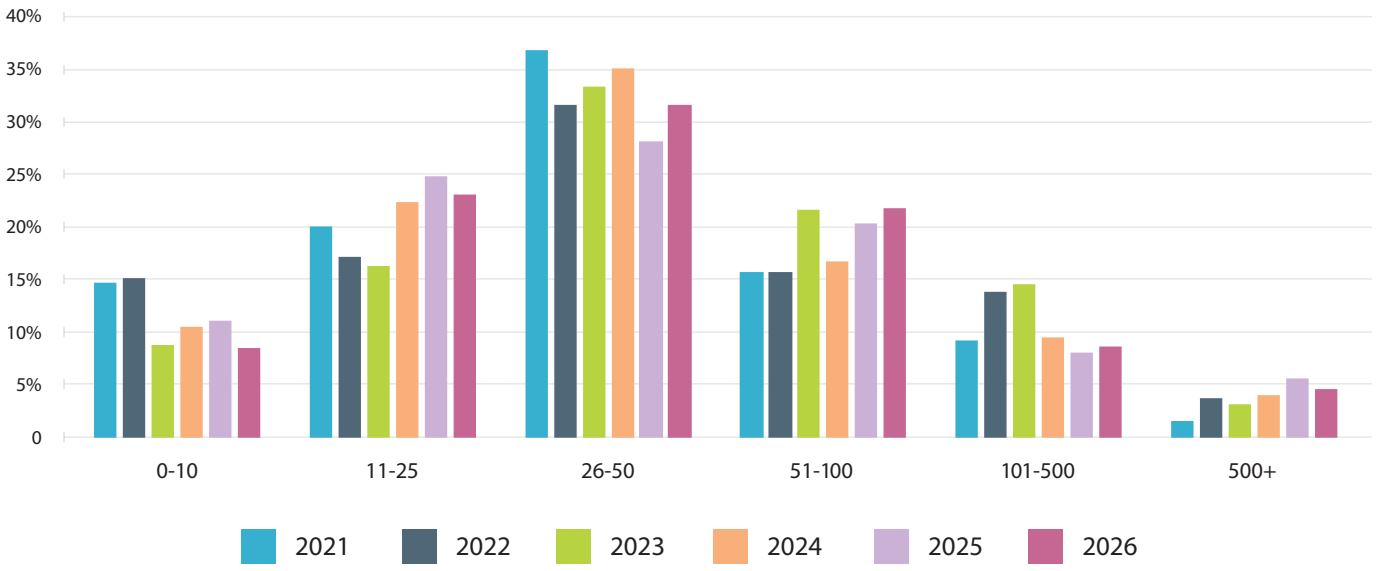
如今的组织架构正日益呈现混合化与复杂化趋势——不仅采用更多云服务提供商，还致力于加强应用程序的安全防护。这种复杂性的加剧，也折射出安全理念中的另一重错位：正如调查结果所示，尽管国家攻击者仍是63%受访者列为三大安全威胁的首要对象，但人为失误仍是数据泄露的头号元凶。如何降低复杂性降低了安全团队出现人为错误的可能性。要实现成功，工具整合不仅要简化操作流程，还需支持扩展以覆盖现代企业基础设施。

云数据正遭受攻击

企业正日益依赖云基础设施支撑核心业务，而攻击者持续将攻击目标锁定于这些关键应用与数据。如前所述，受访者已连续三年将云资产列为三大主要攻击目标。

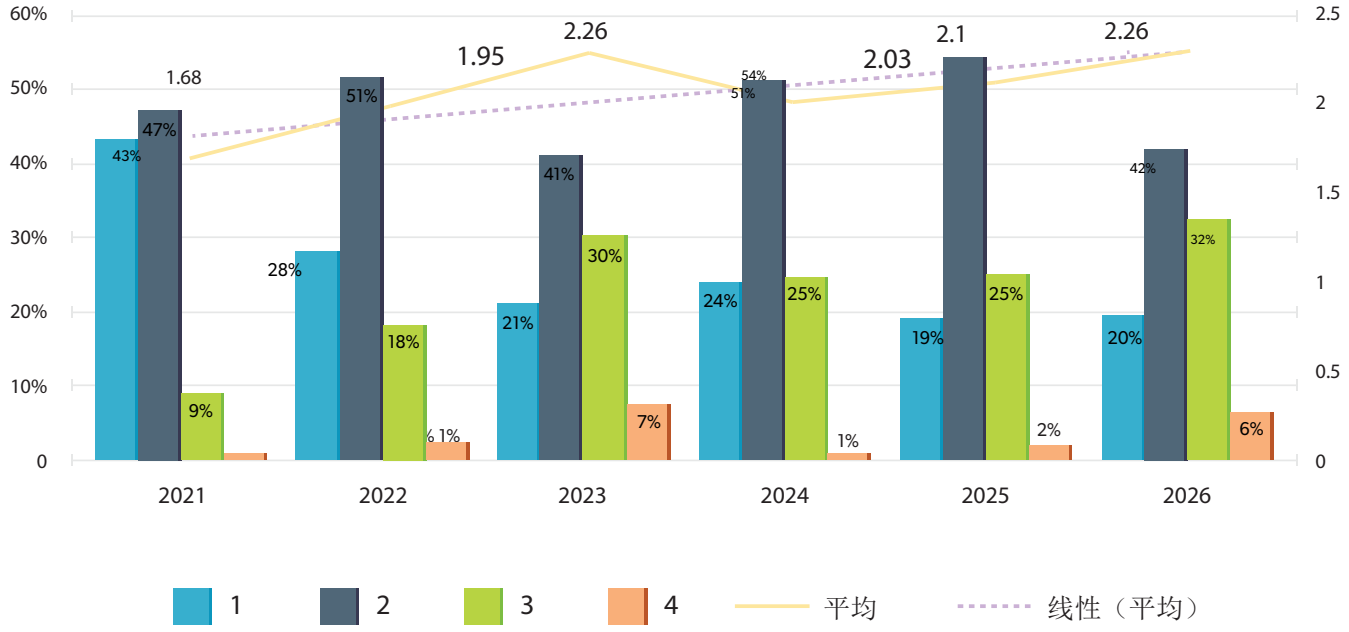
多云基础设施的普及趋势给安全团队带来了更大压力，因为他们不仅要精通复杂云计算架构的防护，还需将安全措施延伸至多个云服务商的环境。最新调查显示，企业平均使用的云服务商数量已回升至2.26家，SaaS应用数量也增至89个。云安全再次成为安全支出的首要类别，这表明企业正全力加强这一关键资源的安全防护。

SAAS 应用程序 使用 数量

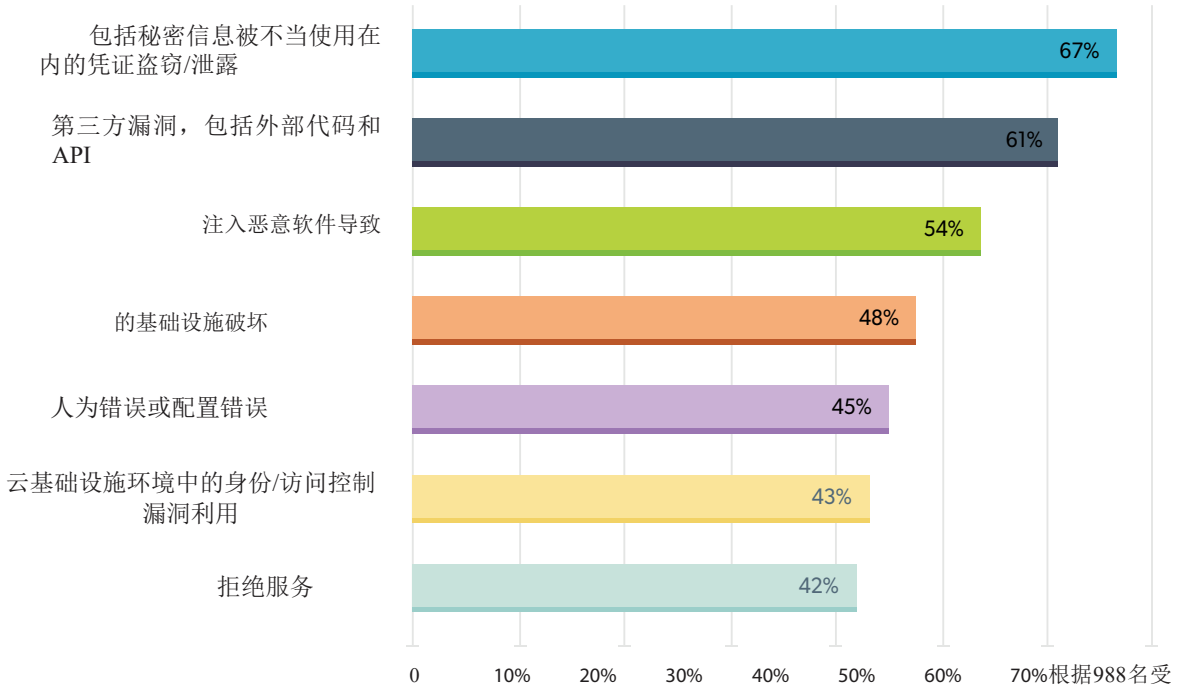


雪上加霜的是，云安全人才严重短缺。调查显示，云安全技能已成为仅次于身份与访问管理技能的第二大安全痛点。身份安全与云安全面临的双重压力，正体现在针对云管理基础设施的各类攻击中。其中，凭证盗窃/泄露攻击已成为最常见且呈上升趋势的攻击类型，这凸显了采用先进身份保护措施的必要性。

IAAS 云服务提供商数量



云管理基础设施的凭证攻击

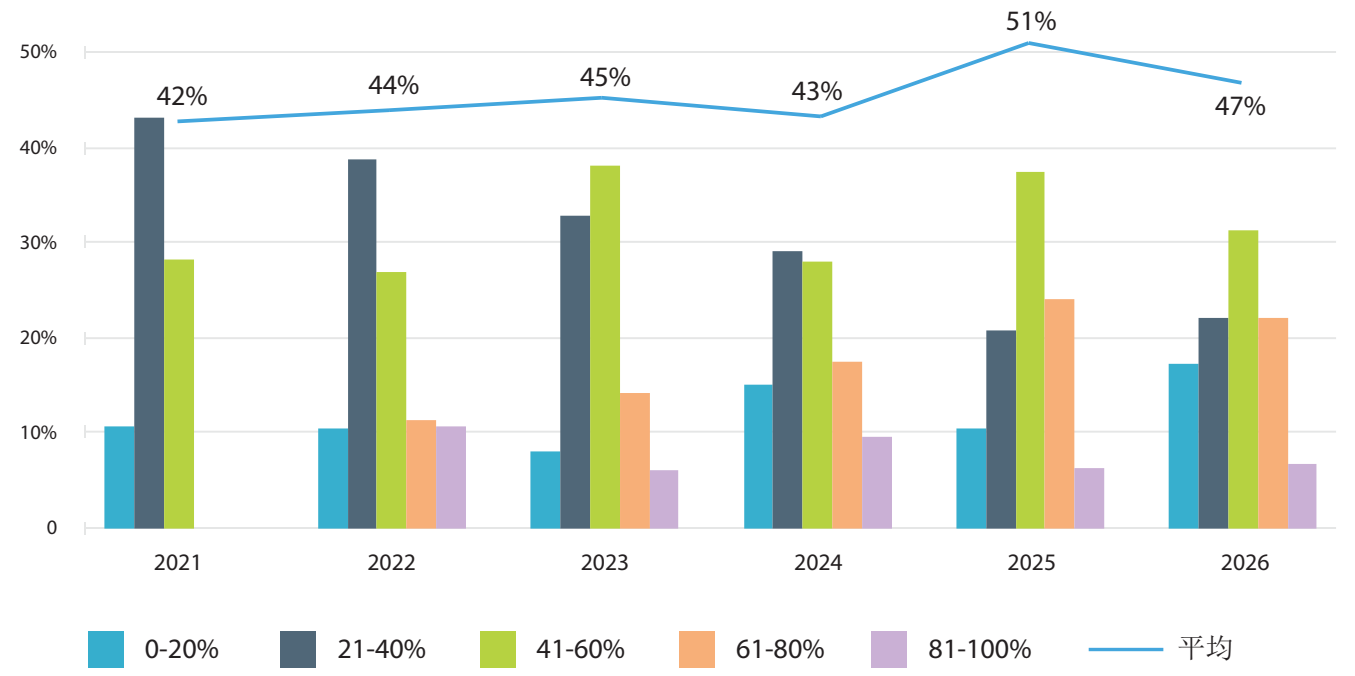


访者报告的云管理基础设施攻击增加情况。

值得注意的是，在日益增多的云攻击类型中，恶意软件注入已从一年前的第四位跃升至第三位。这一变化反映出攻击者正越来越多地利用软件供应链攻击以及恶意模块和插件。应对这些攻击需要高超的技术和强化的数据保护能力。数据可见性和访问保护已变得至关重要，因为凭证泄露可能绕过用户访问控制。

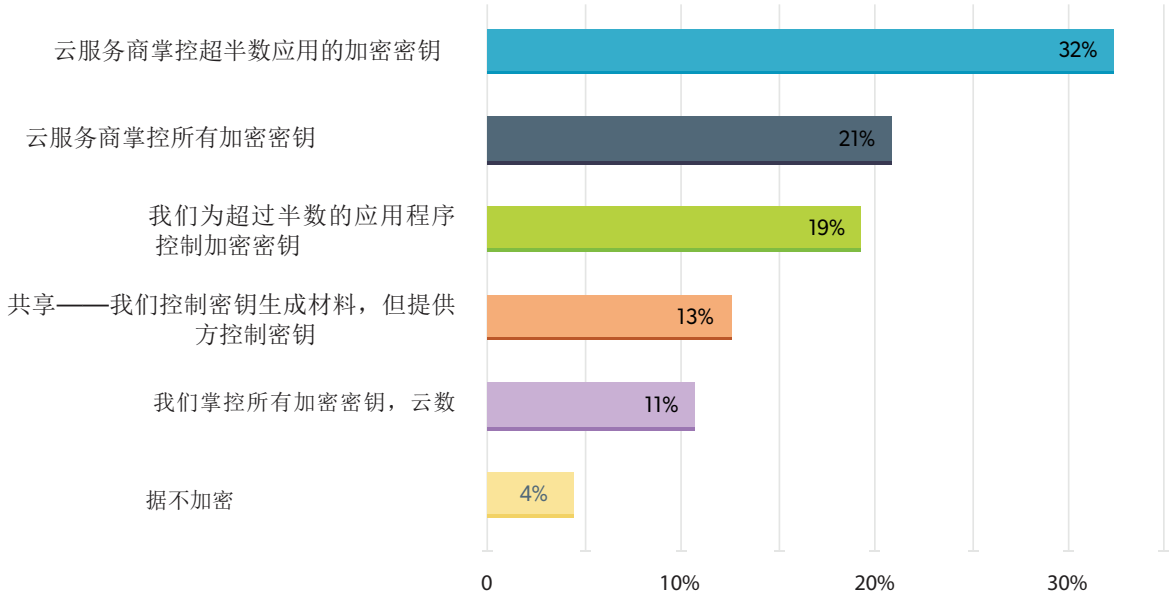
综合背景来看，调查揭示云环境中敏感数据规模庞大且持续增长，其中大部分防护措施不到位，存在泄露风险。数据显示企业在保护最核心资产——数据方面进展缓慢，令人担忧。被归类为敏感的云数据平均占比仍稳定在51%以上，而通过加密保护的敏感数据平均比例则小幅下降至47%。随着人工智能应用获取更多数据权限，智能体在数据处理中获得更大自主权，数据防护措施亟需升级。为有效抵御日益强大的AI辅助攻击，企业必须能够全面定位并分类所有数据资源。

敏感云数据加密比例



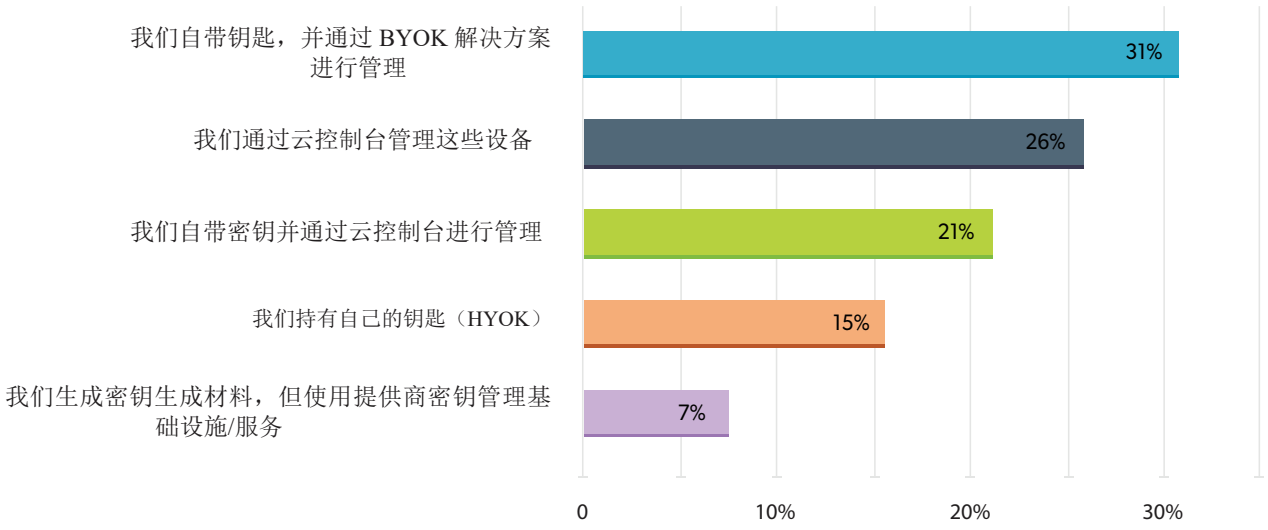
今年的调查结果显示，企业数据安全能力的成熟度仍缺乏显著提升。53%的受访企业坦言，其云服务商掌控着超过半数应用的数据加密密钥。这种局面不仅错失了有效保护敏感数据的良机，更导致数据安全运维陷入不必要的复杂化。由于无法实现对外部集中管控加密管理，企业在多环境密钥管理方面面临额外挑战。

加密密钥的控制点



调查显示，采用自带密钥进行数据加密的组织比例较上年略有上升。近三分之一（31%）的机构正在实施‘自带密钥’（BYOK）方案，并通过自有系统管理密钥。这一举措在降低数据安全操作复杂度方面迈出了积极一步。不过仍有改进空间，仍有四分之一的机构依赖云控制台进行密钥管理。

密钥管理方法



量子风险现实

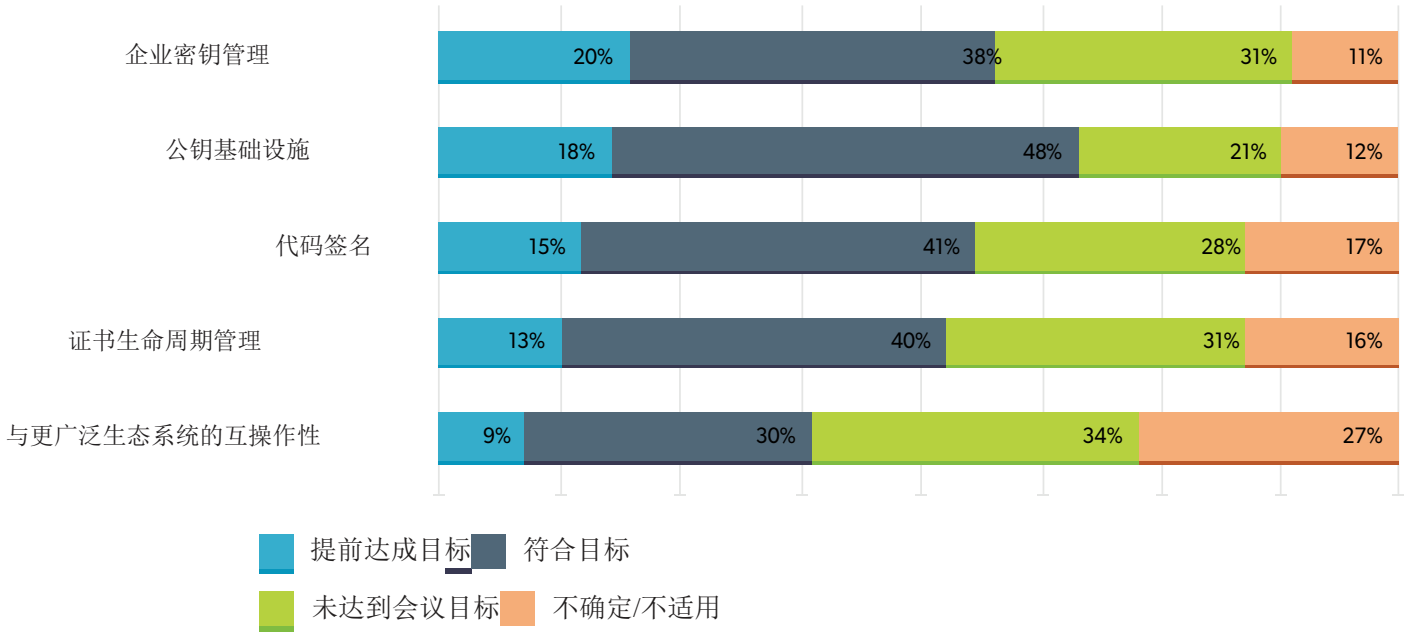
今年的调查还深入剖析了量子计算这一新兴风险领域。这项技术前景广阔，但也暗藏安全隐患——量子计算机可能破解当前主流的加密算法。因此，安全团队必须充分认识并应对量子风险带来的影响。

今年的调查结果显示，人们对量子计算的担忧已趋于成熟，这表明公众对相关风险的认知不断加深，应对措施也在持续加强。61%的受访者将“现有数据未来被解密”（即“现在收割，以后解密”， HNDL）列为最突出的风险。而“未来加密系统被攻破”虽位列第二，却在去年的调查中高居榜首。虽然 HNDL 攻击可能带来更直接的短期风险，但加密系统一旦被攻破，将动摇支撑数据安全的加密信任基础。这可能导致基于伪造数据的攻击（即“现在收割，以后伪造”， HNFL），而伪造数据对包括人工智能在内的众多数据应用场景都构成严重威胁。

被61%受访者列为首要风险的是现有数据的未来解密，即‘先收割后解密’（HNDL）策略。

本次调查评估了各组织在缓解量子风险方面的进展，具体体现在未来18-24个月计划实施的安全措施中。结果显示，正在原型测试和评估后量子密码（PQC）算法的组织比例略有上升（59%）。调查还考察了各组织在信任基础设施关键环节实施 PQC 的自我评估进展。超过50%的受访者认为其在企业密钥管理、公钥基础设施和代码签名方面的实施进度符合或超前计划。超过半数受访者在证书生命周期管理（CLM）方面也处于符合或超前进度，但该领域更令人担忧。由于安全证书颁发机构与浏览器软件供应商组成的“证书颁发机构浏览器论坛”近期通过的新规——将传输层安全证书的最长有效期缩短至2029年前的47天——各组织已面临改进 CLM 流程的压力。这一变化将要求 CLM 领域实现更高自动化水平，同时通过升级管理流程可同步整合 PQC 改进，为未来做好准备。

后量子时代安全目标的实现进展



基于对2140个组织进行的调查、探索或量子计算实验。

调查显示，近三分之一（32%）的受访者已着手开展量子计算项目，或已确定相关研究方向，或开始进行实验探索。在人工智能领域，受访者最关注量子计算的潜在影响，其中机器学习领域最受期待，57%的受访者认为该技术将显著提升分类能力。此外，高级模拟（54%）和并行数据处理（49%）也被频繁提及。

近三分之一的参与者（32%）已确定量子项目或开始尝试量子计算。

再生世界中的主权

在技术与地缘政治格局不断变化、数据整合与共享日益深入的背景下，企业正主动掌控主权治理进程。近半数（45%）企业表示，软件、数据或运营的可移植性是其主权治理计划的核心驱动力。

这一结果与一年前的数据一致，反映了主权倡议的核心动机。三分之一的受访者（34%）明确表示希望对软件和数据拥有完全控制权，以确保未来的可移植性。

在企业应用中，添加AI模型和代理层需要对数据管理保持新的警惕，并带来新的主权风险。通用AI应用面临外部和内部的双重挑战。应用程序运行的地点和方式的解耦，模糊了某些工作负载的主权边界。例如，Claude Code是一种代理式编码工具，允许用户使用自然语言自动化流程。它通常会从所有可用数据源中进行完整的检索增强。代码库、云和本地企业资源都可能被访问。在这种框架中，代理技术将以前使用独立工具和数据源执行的流程融合在一起，数据驻留线和操作独立性可能会被削弱。

尽管36%的受访者表示其组织正在使用50个或更多的SaaS应用程序，但仅凭数量并不能定义风险，因为多个SaaS应用程序可能被集成在一起。例如，客户拓展应用程序可能与客户关系管理及其他营销技术应用程序相连。鉴于这些集成，组织必须更加警惕地定义并确保数据的长期驻留，而非静态评估每个应用程序或用例。采用代理工具（如Notebook LM、Cursor或Claude Code）需要动态的数字主权。相互关联的应用程序所带来的危险——以及由此产生的对强大主权和安全措施的需求——通过“ShinyHunters”攻击小组在2025年成功入侵互联SaaS应用程序的速度和成功得到了凸显。

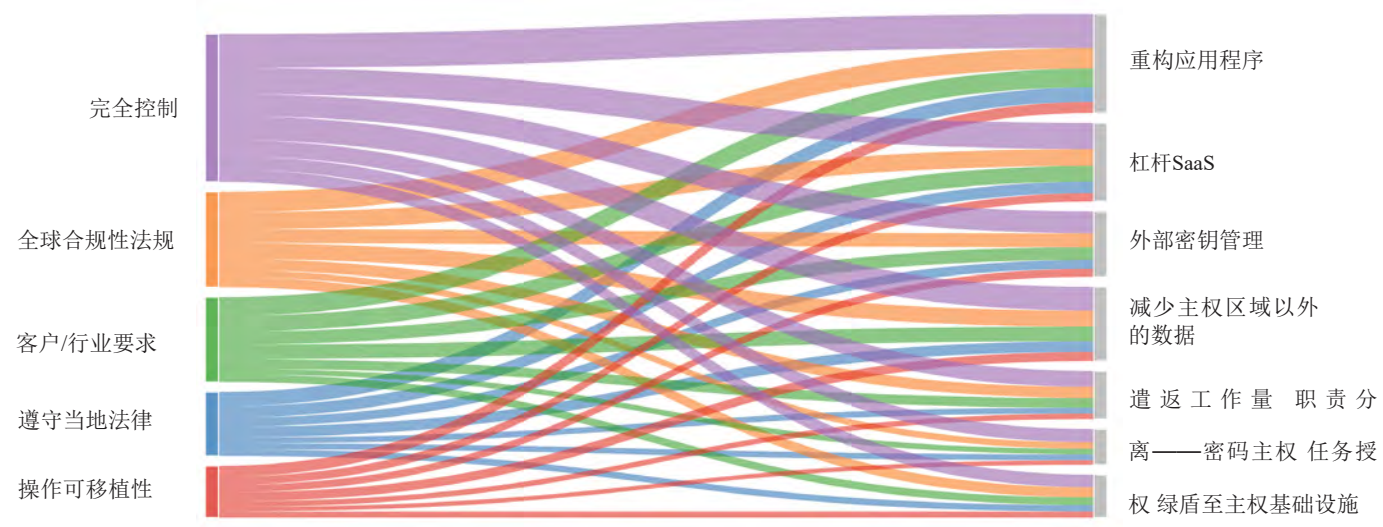
总体而言，数字主权的实践与地方及区域隐私法规同步发展。妥善处理个人公开身份信息（PII）或非公开信息（NPI），可确保居民数据始终处于合法管辖范围内。企业若收集、存储或处理此类数据，需通过多种选择确保数据受控于适当管辖。践行这些选择，即是对数据行使主权。

数据主权是主权体系的第一层级。在此框架下，数据要么必须存储在特定领土内，要么必须采用高强度加密技术，确保只有该区域内的授权方或流程能够访问数据。近半数受访者（49%）认为，当涉及主权目标时，云基础设施的物理位置对部分或全部工作负载至关重要；另有36%的受访者表示，无论数据存储在何处，采用强加密技术和外部密钥管理都能提供充分保护。

对于更严苛的工作场景，还需要具备运营主权。除了云工作负载的地理位置要求外，这意味着所有参与运营的人员都必须是相关司法管辖区的公民。最近出现的数据大使馆概念表明，这些前哨站可以设在原属国管辖范围之外，但仍需遵守该国规定的管控要求。加密技术对运营主权同样具有影响：19%的受访者表示将通过更明确的加密措施——即“密码主权”——以及加强定义与实施加密的职责分离来推进主权倡议。

软件主权标志着在操作主权基础上更进一步，因为数据可以脱离现有应用程序并轻松移植到新系统中。对数据和软件的全面掌控是主权倡议最常被提及的驱动力，企业正通过实质性变革来实现这一目标。五分之二的受访者（40%）正通过减少主权区域外可获取的数据量来实现主权，54%的企业正在重构应用程序以更好地分割或隔离数据。

流量分析:从主权驱动到解决方案



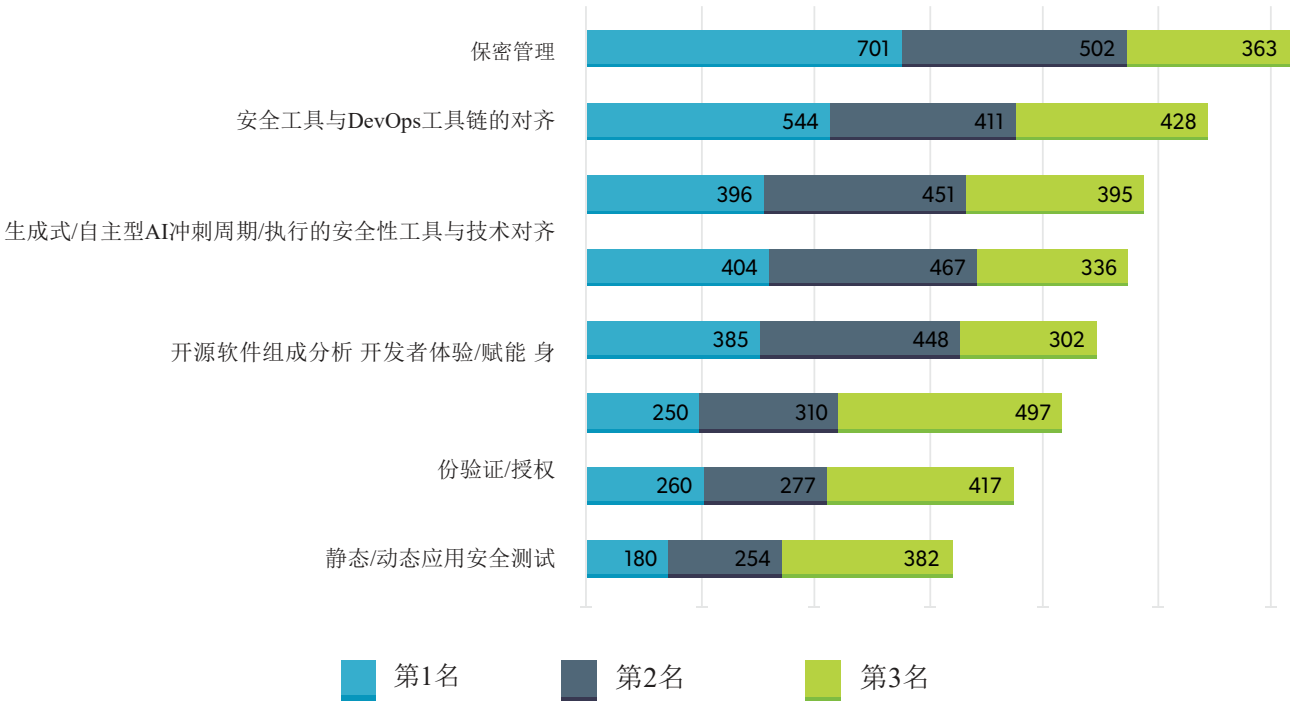
虽然主权建设最初多以支持隐私法规为初衷，但如今它正助力企业转向更具优势的经济领域。人工智能与软件即服务（SaaS）生态的迅猛发展，催生了全球数据中心的繁荣浪潮，这给可持续发展、能源效率和系统韧性带来了额外压力。通过数字主权和全面数据掌控，企业能有效规避孤立或难以迁移的数据孤岛所带来的经济风险和技术债务。

应用开发中的数据安全

应用程序开发是安全运维的前沿阵地。构建安全的代码和应用架构是基础性工作，而这一领域正面临人工智能和智能应用带来的双重压力。随着AI编码工具和应用开发工具向更广泛用户开放，安全团队必须确保这些工具及其生成的应用程序都建立在安全架构和服务之上。值得注意的是，在DevOps流程中，管理数据访问权限的机密安全防护，始终是被高频提及的首要安全挑战。

在此背景下，数据安全工具与框架必须提供开发人员构建安全应用的支撑框架——这一要求在智能应用领域尤为重要。调查数据显示，受访者对DevSecOps和密钥管理工具的投入水平在所有技术类别中垫底，这凸显了该领域的特殊关注点。当安全团队投入资源应对智能应用带来的风险时，必须将开发基础设施和数据保护列为优先事项。

DEVOPS 最大安全挑战



结论

数据安全的有效保障向来不易，而人工智能与智能应用带来的压力更使其面临严峻挑战。数据需要满足更广泛的应用需求，以更大规模和更高速度流通，同时必须保持严密的安全管控。要实现并维持这一愿景，持续稳定的运营数据安全至关重要。数据安全态势管理（DSPM）、数据监控与治理、数据保护必须相互强化，既可应对日益增长的演变风险，又能实现可观的潜在收益。

人工智能生态系统正飞速发展，安全团队不仅要部署灵活的防护措施，还需提升对数据的掌控能力，以应对即将到来的变革。随着企业采用更高水平的自动化技术，推动人工智能与智能代理驱动的集成进程，必须简化安全架构，才能满足市场竞争对系统规模和响应速度的严苛要求。

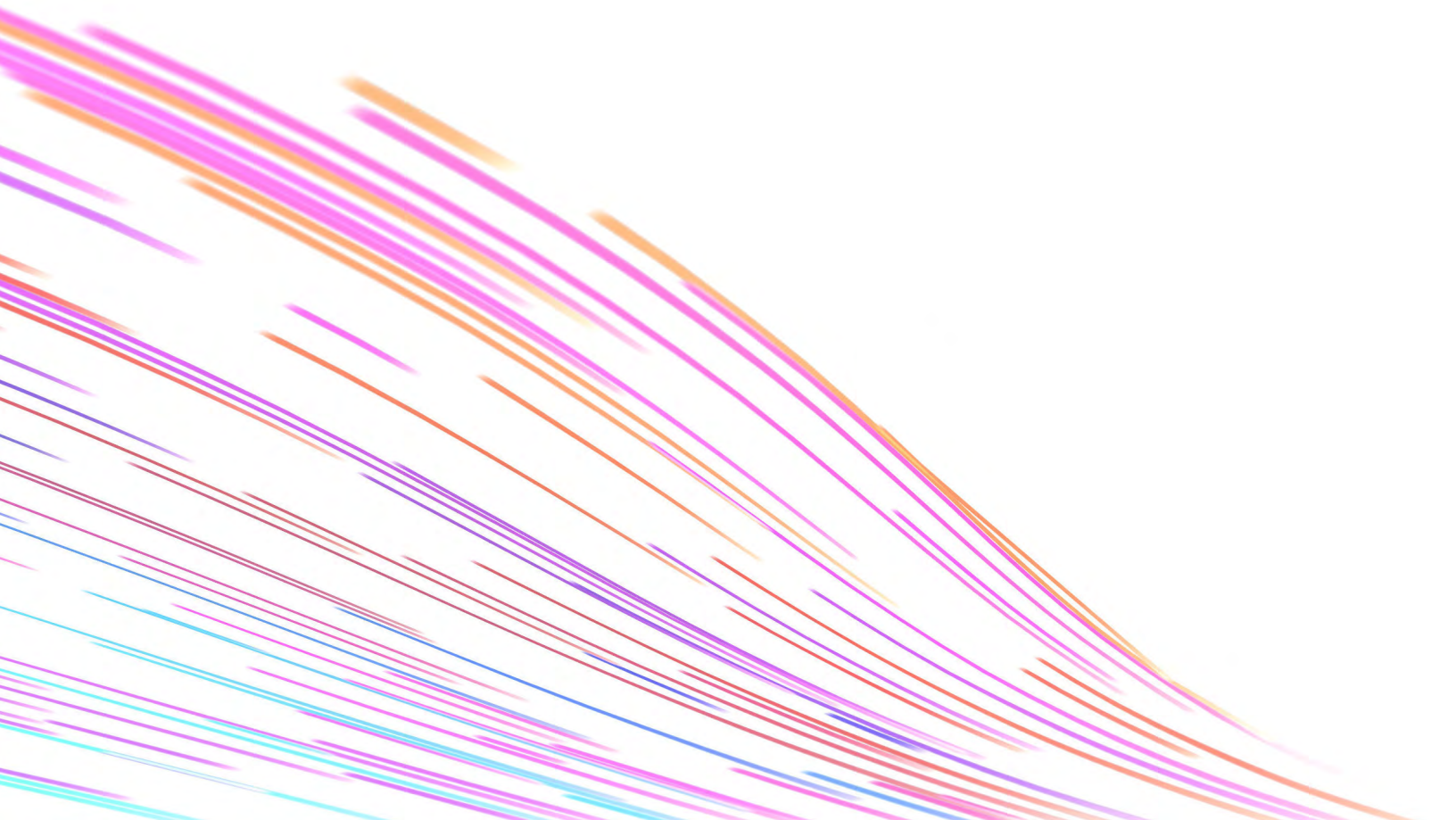
研究结果提出了若干实际的后续步骤：

- 数据识别与管控的持续性至关重要：数据资产正快速形成复杂网络。当前企业平均部署89个SaaS应用，这些通用应用的集成导致大量数据进出通道，成为攻击者可利用的漏洞。要在多应用、多云环境及不同司法管辖区实现数据的持续识别与管控，必须采用平台化解决方案。反之，分散的管控措施不仅会增加系统复杂度，还会扩大潜在风险。
- 主动出击是行业准则：安全领域领导者必须与内部利益相关方及行业同行建立联盟，以理解并应对新的竞争压力。人工智能展现出巨大潜力，既能开拓市场，又能创造新产品与服务，从而带来新机遇。然而，当被问及人工智能兴起对市场增长的竞争压力时，仅有19%的受访者表示其处于行业领先地位。
- 主权至关重要：具备未来适应性的可移植性将决定哪些平台能持续使用，尤其在监管严格的行业和司法管辖区。拥有数据主权、运营自主权和软件自主权的企业，能更灵活地迁移至最佳执行环境并持续运营。随着人工智能工作负载和项目日益受限于计算能力、数据中心和能源约束，自主选择并实施管控的自由度比以往任何时候都更为关键。
- 信任建立在安全之上。人工智能助长的虚假信息和错误信息带来的新危险是普遍存在的，97%的受访者报告

  人工智能生成的虚假信息可能造成各类组织损害，包括商业邮件深度伪造、商标或品牌滥用、关键人员受害、声誉损害及招聘欺诈。若安全工具能持续满足用户和利益相关方的实际需求，将有助于更高效地实现预防、检测与响应。

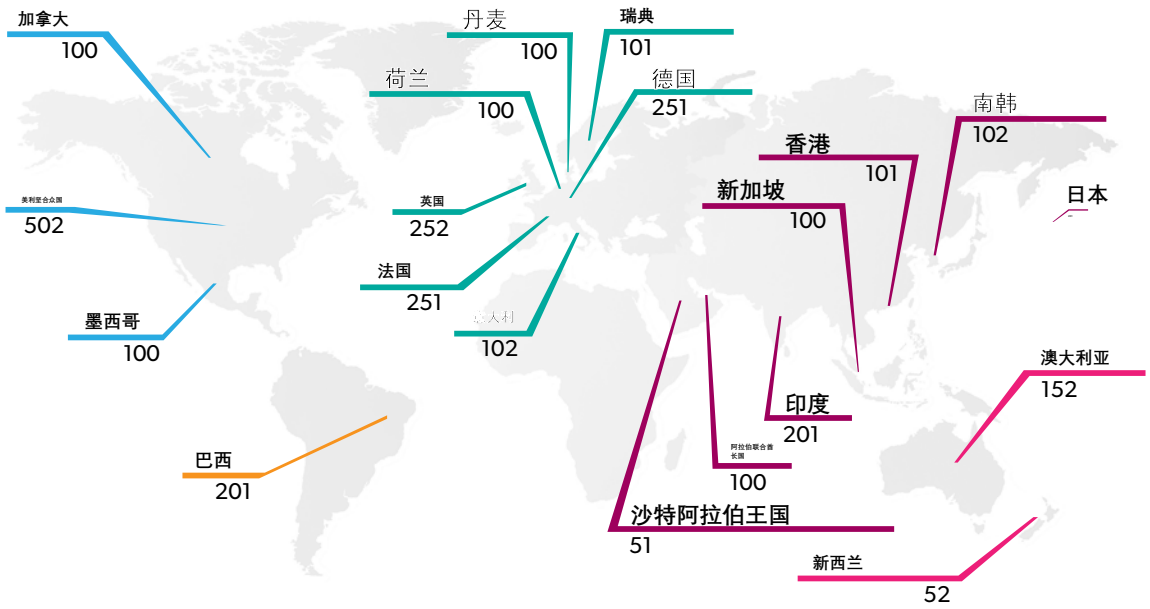
- 当前正是采取行动的关键时刻。尽管生态系统发展迅猛，企业仍需基于现有数据采取行动。数据质量低下或初始数据治理不善，是制约人工智能应用最普遍的问题。而对数据资产的不完整认知——包括其构成、存储位置及最佳保护方式——则引发了第二大问题：暴露数据的安全风险。
- 简明灵活且可扩展的安全工具能有效降低运维复杂度。研究中体现的这种复杂程度，在智能体主导的世界中已难以为继。安全功能必须具备足够的适应性，能够为最适合应用需求的各类基础设施提供防护。企业既要保留原生安全控制，又要实现跨本地环境和多云平台的防护延伸。数据加密作为关键要素，必须覆盖多样化基础设施，并有效应对新兴的量子计算风险。

基于智能体方法的人工智能应用正不断模糊用户与系统的界限。智能体和AI基础设施日益实现多系统自动化、数据源整合与抽象化。当前AI虽仍主要服务于用户，但其权限下放程度之深，可能使智能体演变为新的内部威胁。为应对这一风险，企业需制定、传达并严格执行统一且易于理解的政策，确保个人、团队乃至整个组织都能快速适应并实现安全发展。



方法学

本研究基于一项针对3,120名受访者的全球性网络调查，通过针对各国特定人群的定向问卷收集数据，目标群体为安全与IT管理领域的专业人士。除调查主题相关知识水平标准外，筛选标准还排除了来自年收入低于1亿美元及1亿至2.5亿美元选定国家的受访机构人员。本研究采用观察性研究方法，不作因果关系推断。



税收	数量 受访者
1亿至2.499亿美元	213
2.5亿至4.999亿美元	701
5亿至7.499亿美元	799
7.5亿至9.999亿美元	774
10亿至14.9亿美元	265
15亿至19.9亿美元	137
20亿美元或以上	231
共计	3,120

工业 部门	行业数量 受访者部门	数量 受访者
医疗保健 263 旅游/酒店业		181
零售	255电子商务	171
汽车制造251		166
金融服务业 237 教育		141
技术	222 生物技术	124
能源与公用事业213国防		115
政府207航天		80
运输	189 电信	79
医药品	187 其他的	28
共计		3,120

THALES

CYBERSECURITY

SafePloy 安策

如需联系信息，请访问
https://www.safeploy.com/news/1789.html

立刻联系

关注公众号