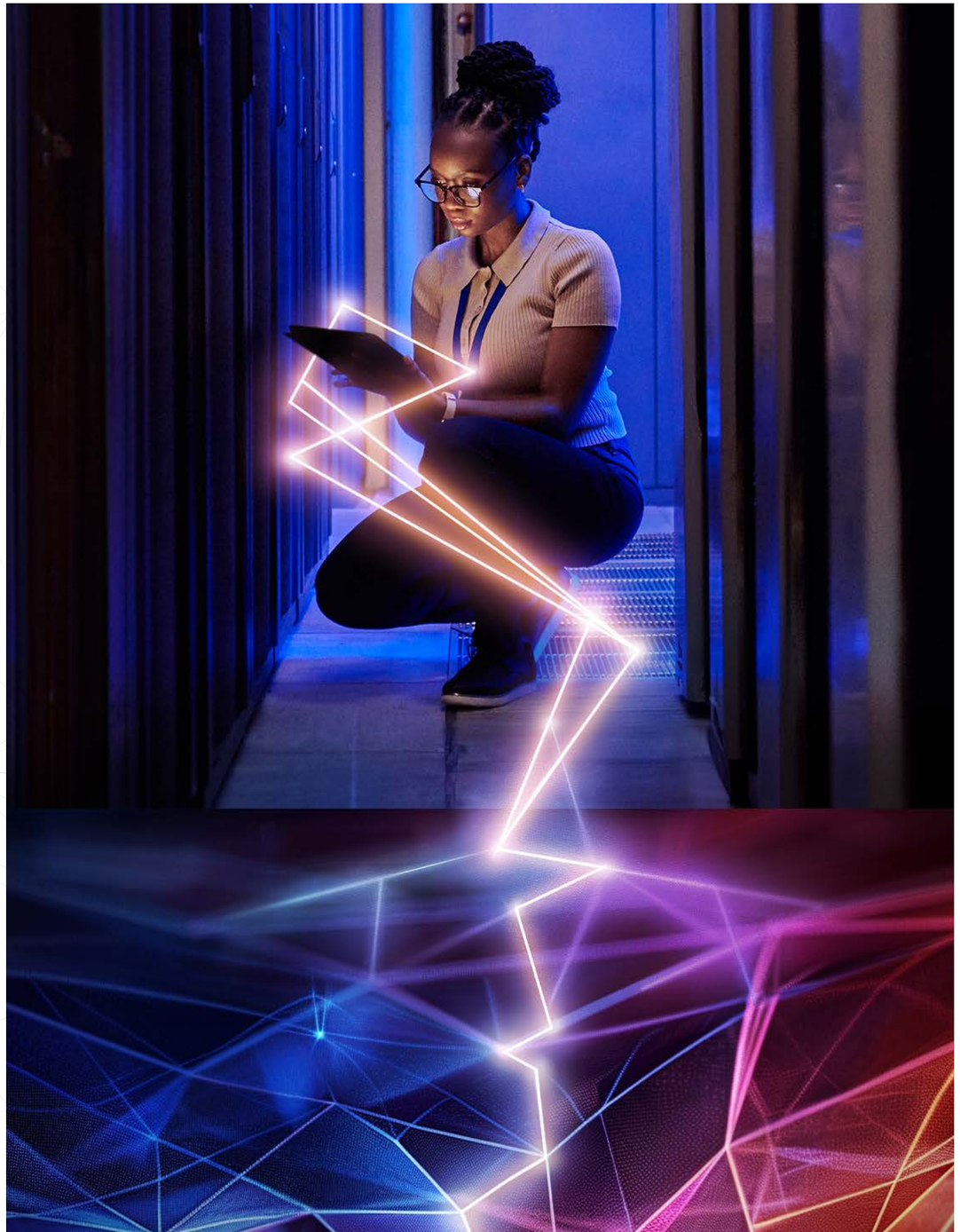
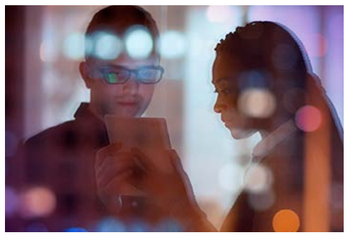
在 Gen AI 时代保护数字核心

网络安全是重塑的战略推动者

accenture

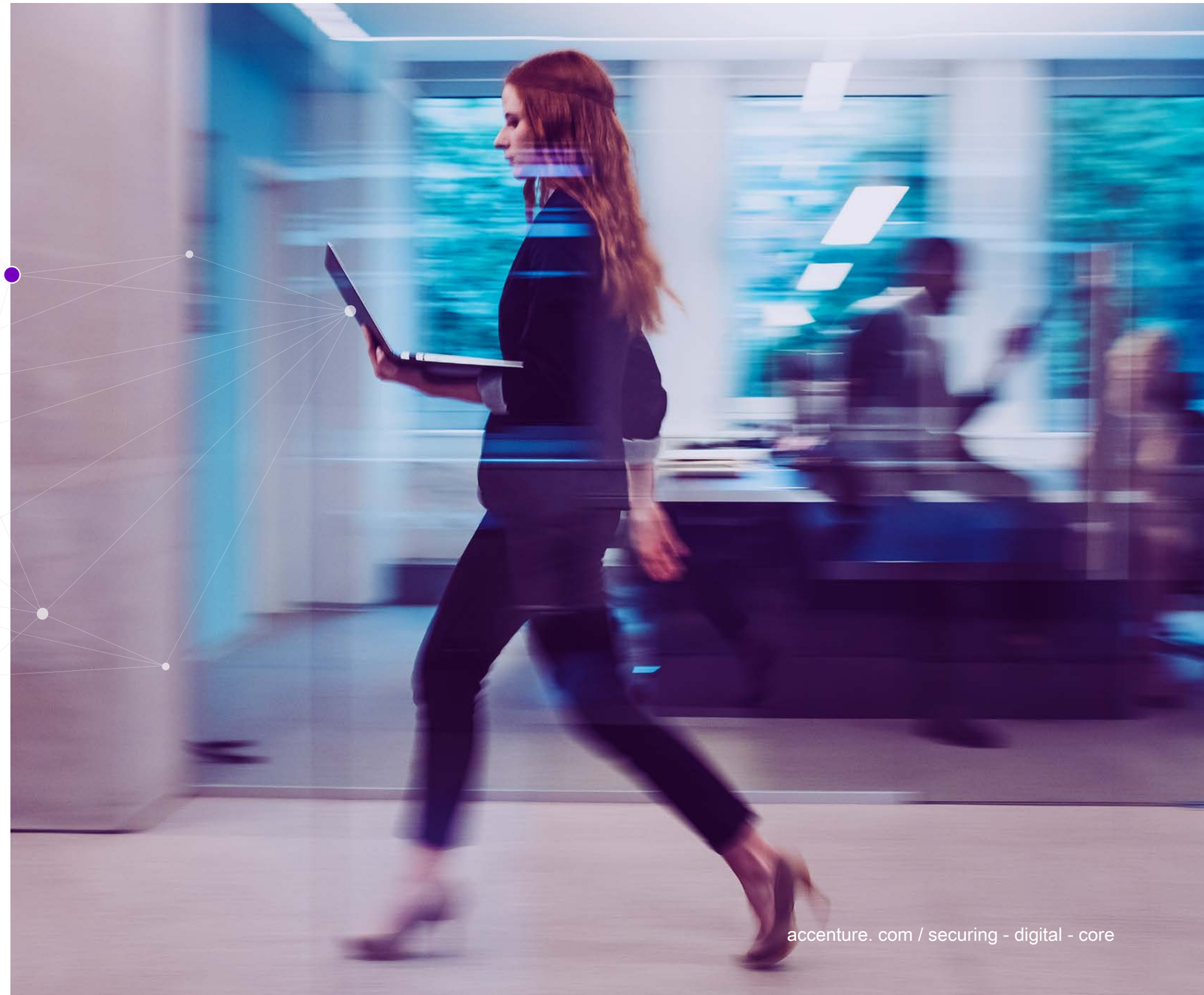


Contents



执行摘要

公司们竞相构建数字化核心，利用生成式AI重新发明业务的每一个环节。然而，在确保关键技术层免受未授权访问或攻击方面，许多公司正落后于人。



安全对于数字核心至关重要，因为其三大技术集——数字平台、数据和AI基础以及安全所在的数字基础——不断相互作用，推动重塑与创新。在我们最近发布的研究报告中，用数字核心重塑 我们发现，在数字化核心指数中处于顶级 quartile 的组织实现了 20% 更高的收入增长率和 30% 的盈利能力提升。

转变为行业领先状态需要利用合适的工具和实践以实现灵活性和创新，并结合安全能力和韧性。在这其中，安全不仅可以超越静态防御机制。如果企业将安全措施融入其不断演变的数字景观中，它可以成为促进业务增长和转型的推动因素。

说起来容易做起来难。我们发现 ， 平均而言 ， 安全能力滞后 23 点 [1]。基于我们针对尚未实现“行业领先”数字核心的企业开发的Digital Core Index。这些组织在关键领域（如开发安全与运营（DevSecOps）、实施零信任身份和网络模型、自动化安全配置、威胁建模以及保护 cyber-物理和边缘系统）落后于其领先的竞争对手。

随着生成式AI和其他颠覆性技术加速创新并重新定义行业，它们也扩大了威胁landscape，为恶意行为者提供了更多途径。在采用这些技术的竞争中，公司往往优先考虑速度而非安全性——忽视早期的安全集成，从而增加风险和

延长了修复努力的时间。这种反应性的方法还会累积技术债务，导致最终的成本远远超过如果从一开始就嵌入安全性所需的成本。

如今 ， 组织平均依靠 76 种安全工具来管理其安全状况 ， 这一数字正在增长 [2] 例如，每月从云服务提供商那里新增或修改的配置设置数量已达到数千项，安全团队不得不努力确保系统的安全和更新。这些复杂性往往会导致冗余、增加配置错误的风险并使集成工作变得更加复杂，从而降低安全效果的效率。结合人才短缺的问题，这意味着全球约有480万个网络安全职位空缺——这妨碍了安全解决方案的有效扩展。 [3] .

数字核心指数评估组织在数字核心七个支柱领域的企业技术栈，使用40个子组件构建我们的数字核心指数（标准化为100的尺度）。能力点代表特定技术的相对成熟度。差距表示为了达到更高层次的能力所需的技术现代化活动。

组织如何缩小这种安全成熟度差距 ？

安全性是竞争优势之一——它营造出一种以信任、韧性与适应性为核心的企业环境。这使得组织能够在自信地进行重塑的同时，抓住新的发展机遇和竞争优势。

构建稳健的安全体系是一场马拉松，而非短跑。组织可以通过激活三项战略杠杆，将其安全体系转变为能够满足业务所需的速度和规模运行，并同时降低成本和减少技术债务。

杠杆 01

流线

组织必须整合供应商并采用集成工具，同时淘汰legacy系统。利用生成式AI的能力可以显著减少正在使用的安全工具数量。这项技术可以简化流程、自动化常规任务，并通过提供高级洞察和威胁分析来增强决策制定。

杠杆 02

现代化

安全必须现代化其工具和策略，以跟上不断变化的数字环境。例如，通过采用内置代码仓库和管道安全扫描的基础设施即代码（IaC），可以实现安全配置的标准化，并将测试无缝集成到开发过程中。转向软件即服务（SaaS）和基于云的安全管理系统不仅可以减少管理和维护硬件、服务器和更新所需的时间和成本，还可以增强威胁检测、提高合规性并加快部署速度。

杠杆 03

规模和进化

自动化和网络安全-as-a-service（CSaaS）可以助力安全扩展。例如，使用生成式AI驱动的防御解决方案进行威胁测试，如自动红队演练和渗透测试。这些工具尤其及时，因为针对此类技术的监管措施即将出台。这些监管措施旨在解决安全风险、歧视和偏见、隐私问题以及对职业和劳动力市场可能产生的影响。领先的平台公司和超大规模企业已经开始基于这些技术推出安全功能。

为什么重新发明会让你面临风险

确保安全是实现重塑准备的关键使能器之一，因为它构建了信任和韧性基础，从而 enables confident innovation。

公司正在努力理解新技术如何改变其业务，并相应地将其深入嵌入数字核心以加速重塑过程。在埃森哲，我们将重塑准备度定义为一种持续状态，即支持当前业务、提高效率和有效性，同时响应组织的持续需求并迅速采用最新技术创新。因此，安全必须同样灵活，以应对任何新的威胁或新兴需求。

为了充分发挥生成式AI和企业技术转型的全部潜力，你需要一个具备重塑能力的数字核心。数字核心由七个不同的、始终运行的部分组成，帮助组织不断自我革新。这些部分包括数字化平台、数据与AI以及数字化基础架构，后者涵盖优先采用云基础设施、安全措施、可组合集成和持续控制平面（图1）。

具有可重铸数字核心的组织遵循三条原则：他们保持业内领先的能力水平，将投资转向战略创新，并主动管理技术债务。

安全是数字核心不可或缺的一部分——嵌入其基础架构的每一个层面，并贯穿每一层。没有安全，数字核心将变得脆弱，从而使重塑和提升竞争力变得更加困难且成本高昂。如今，业务的持续重塑通常由技术支持驱动，这种技术深入到业务之中，并跨越平台、合作伙伴和客户，横跨多种环境和架构。我们的研究显示，83%的组织正在加快其重塑努力。[4] 99.7% 的高管表示，他们致力于在所在行业建立新的业绩水平[5]。

54%

金融服务业高管表示，为了转型或重塑业务并提升客户体验而采取的努力引入了更多的技术风险。[6]。

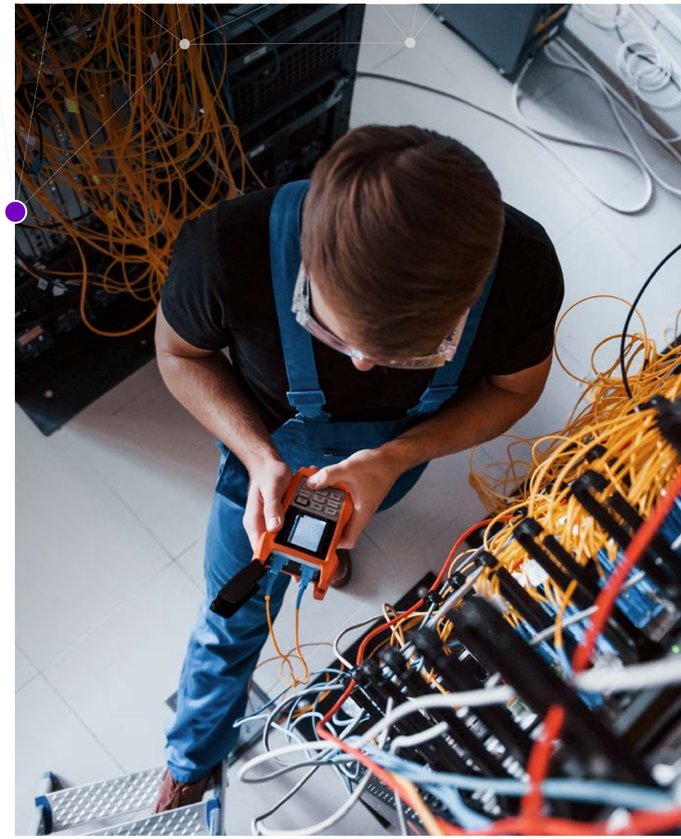
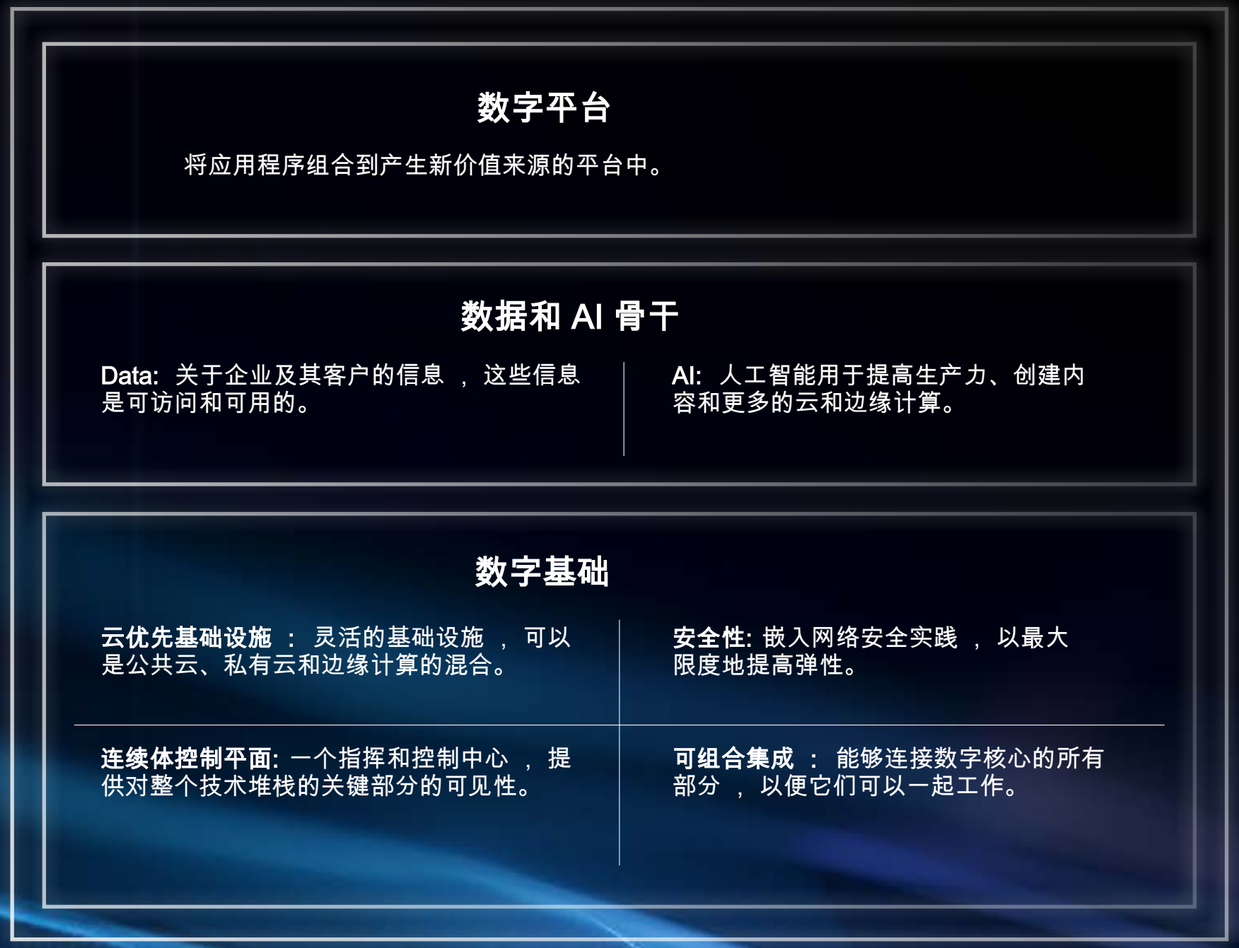


图 1 ： 数字核心的组件



什么是数字核心 ？

数字核心是一种思考和使用技术的新方式。

Accenture 将数字核心定义为能够创造并赋能组织独特重塑野心的关键技术能力。构建这一量身定制的数字核心需要整合先进的数字平台、无缝的数据和AI基础架构，并使用激进的新工程原则构建安全的基础。

这个量身定制的数字核心使组织能够超越竞争对手，以最高效的方式实现其目标——通过合适的云实践实现灵活性和创新；利用数据和AI实现差异化；通过应用程序和平台加速增长、下一代体验和优化运营——并将安全设计贯穿始终的每一个层面。

安全还在继续吗 ？

随着组织竞相采纳新兴技术以启用新的产品和服务，它们往往优先考虑速度而非安全性。

平均而言 ， 安全性有 23 个百分点的滞后
组织的能力尚未
实现 “行业领先 ” 的数字核心。

事实上，70%的高管表示他们仅在关键功能上实施安全控制，或在转型最终完成且漏洞被发现后才部署这些控制。[7] 这会产生连锁反应。当企业在采用新技术时没有从一开始就将 robust 安全措施和策略“设计”进去，公司的数字核心会变得容易受到威胁，技术债务也会随着碎片化安全解决方案的增多而增加。这使得补救工作越来越昂贵且耗时，并限制了企业的业务灵活性。

在数字核心方面，那些被定义为“行业领先”的组织（即我们在数字核心指数中排名前25%的组织）与最低四分位的组织相比，在安全能力上平均落后23个点（如图2所示）。大多数组织在诸如DevSecOps和零信任身份与网络、安全配置、威胁建模以及保护 cyber-物理系统等方面落后。

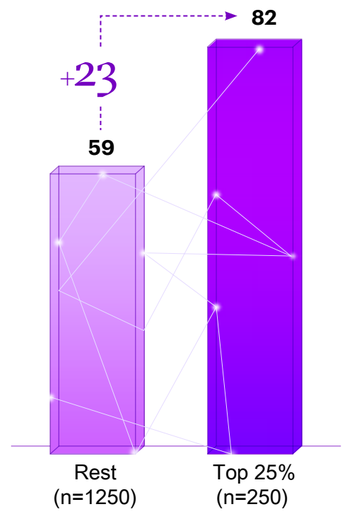
这一差距进一步被技术债务挑战加剧。美国的技术债务总额估计已超过1.5万亿美元。[8]. 安全问题是其中的一部分，根据我们的研究，34%的组织将其列为技术债务的主要贡献因素。它由此产生。

从临时解决方案转变为安全问题，这些临时方案最终需要重新处理，因为它们无效。此外，不整合或不提供其他安全工具上下文的点对安全态势和可见性造成影响，同时增加成本。

此外，安全复杂性和人才短缺增加了另一层难度。组织报告称他们平均依赖76种安全工具来管理其安全状况。[9]. 这使得转型努力变得更加复杂。此外，人才短缺问题——全球范围内有480万网络安全岗位空缺。[10] 这种复杂性严重阻碍了组织有效扩展的能力。

图 2 ： 安全成熟度缺口

数字核心指数 - 安全成熟度分数



网络攻击的成本

网络安全仍然是全球最大的业务风险 ，影响客户信任、业务增长和企业价值。

breaches 不仅会增加财务成本，还会产生重大的声誉影响——在攻击期间，79% 的网络安全专业人士将声誉问题列为他们的首要关切。[11]。

随着组织准备在安全服务上投入更多资金，优先投资与增长战略相契合的资金是一项关键挑战。虽然96%的CEO认为网络安全对于增长至关重要，但仍有74%的人担心潜在网络攻击可能造成的损害。[12] 此外，网络安全已成为企业ESG（环境、社会和治理）评估中的关键要素，影响评级、交易和并购活动，公开交易公司遭遇数据泄露后平均股价下跌7.5%。[13]。

迅速变化的威胁格局突显了这些担忧的紧迫性。

安全专业人士和管理人员都认识到不断上升的危险：

75% 的安全专业人员报告说，在过去一年中，网络攻击有所增加[14] 56% 的高管认为，生成式 AI 为攻击者提供了明显的优势[15]。

• 自 ChatGPT 推出以来，网络钓鱼攻击已激增 1, 265%[16] 2023 年，使用生成 AI 的 deepfake 尝试同比猛增了 3, 000 %[17]。

• 阿尔特纳希（Accenture）的网络安全intelligence（ACI）研究人员还注意到，从2023年第一季度到2024年第一季度，与深度假象相关的工具在暗网论坛上的交易量增加了223%。[18] .此外，从2022年到2023年，云环境入侵事件激增75%，威胁行为者利用云的独特功能发起攻击。[19]。

这些关切的严重性反映在最近几起备受瞩目的事件中：

• 一家Greater China地区的跨国公司因一起复杂的深度假信息诈骗案遭受了2500万美元的损失。诈骗者在会议电话中digitally recreate公司的首席财务官及其他员工，指示同事转账。[20]。

• 亚洲某航空公司的软件存在漏洞导致大规模数据泄露，暴露了6.5 terabytes的数据，包括飞行机组人员的个人信息。此次泄露源于一个配置错误的Amazon Web Services桶。安全调查人员发现了2300万个文件，包括敏感的飞行图表、导航数据和平文密码。[21]。

• 2023 年 5 月，一家全球汽车公司报告了一起影响约 26 万名客户的数据泄露事件，原因是配置错误的云环境。来自日本、亚洲和大洋洲的客户数据被暴露。该汽车公司迅速阻断外部访问，并在全国范围内的所有云环境中启动调查。[22]。

这些事件突显出随着威胁landscape不断演变，安全挑战日益加剧。但在重塑过程中，组织的安全政策和行为也显著贡献于安全挑战的增加。

79%

网络安全专业人员将声誉列为攻击期间他们最关心的问题[11]。

缩小安全漏洞

为了在数字核心中弥补安全成熟度的差距并实现重塑准备，公司应该激活三个战略杠杆。

杠杆 01

简化安全性以降低成本并优化投资

合理化安全措施消除了冗余，降低了成本，简化了流程并优化了投资。高效的集成解决方案实现了更好的资源分配和更强的安全态势。

应采取的行动 ：

整合供应商和工具

Consolidate 安全产品以简化工具集并减少复杂性。这将帮助您实现更好的安全效果，如更快的威胁检测和改进的事件响应时间。

实现这一目标需要对现有的安全解决方案进行彻底评估，以将它们整合到一个统一且流程优化的系统中，从而消除冗余并提升整体安全性。通过利用生成式AI的能力，可以在安全运营中解锁新的效率和有效性水平。例如，生成式AI可以将各种安全工具的功能（如入侵检测、威胁情报和事件响应）整合到一个单一、协调的系统中。

在独立工具上采用集成平台

投资集成平台而非依赖孤立的独立工具，以简化管理并增强组织对新兴威胁的防御能力。集成平台不仅简化了运营流程，还能够实现实时情报共享，这对于预防零日威胁至关重要。通过整合多样化的数据点、仪表板和用户体验，这些平台为安全团队提供了对组织风险状况的整体视图。这种统一的方法使团队能够更快更高效地识别和缓解威胁。此外，数据和工具的集中化有助于减少疏漏的风险，并提高在不同系统之间关联事件的能力，从而形成更为稳健和 resilent的安全策略。

淘汰旧工具并投资于同类最佳解决方案

升级到现代工具以简化管理并优化资源配置。首先，从不再与现代业务流程相匹配的遗留工具转向，以加速组织的安全转型。这一战略转变不仅将减少复杂性，还将消除冗余，从而显著提升整体安全态势。将资源集中于提供强大防护以应对当今威胁的先进技术上。

案例研究

公共交通组织的零信任旅程

一家公共交通组织需要增强其网络安全，通过在其混合云环境中引入零信任原则。通过评估网络安全计划、识别差距并定义零信任愿景，Accenture共同创造了一个实用的计划，并开发了一个战略项目目录，优先考虑关键项目，如用于身份和证书管理的网络安全网关。最终结果是减少了业务中断的风险，并将资产可见性从10%提高到90%以上；跨部门连接了团队，重新定义了角色和治理，实现了成本降低，包括优化投资策略、增加自动化和合并软件许可证。

杠杆 02

现代化并将安全性与业务集成

重塑数字化核心以实现再发明需要重新思考和审视安全问题，并在此基础上投资创新并解决技术债务。组织不能以牺牲安全为代价来追求快速成长。确保强大的安全措施不仅包括更新针对新创新的安全措施，还涵盖通过专门的安全计划或现代化手段来解决遗留系统的问题。

一个全面的安全方法是必不可少的。许多安全流程超出了典型的安全功能范围，并且需要与业务同步进行现代化改造以实现韧性。灵活的安全计划将使组织能够迅速应对攻击、确保无缝运营并降低费用。

应采取的行动 ：

将安全嵌入整个云原生应用保护 (CNAPP) 生态系统

利用专有的模板、预定义脚本、剧本和技术创新集成，确保在既有项目和新项目环境中实现稳健的安全性。快速将安全运营迁移到云端，使组织能够访问先进的工具和预制资产，现代化其安全基础设施。例如，通过实施基础设施即代码（IaC）、安全扫描以及自动化持续集成和持续交付/部署（CI/CD）管道，安全配置可以在开发早期阶段标准化并集成。

生命周期管理。生成式AI可以通过提供嵌入安全参数的Terraform基础设施即代码（IaC）模板进一步增强云安全，简化安全合规基础设施的创建过程，同时减少配置错误。此外，确保您的生成式AI云服务提供商（CSP）环境的安全性对于安全地部署如OpenAI在Azure、Google GCP Gemini和AWS Bedrock等独特的AI服务至关重要。这些战略举措确保安全措施能够灵活应对、可扩展，并且能够满足动态威胁环境的需求。

保护数据和 AI

为了应对不断演变的AI环境中的威胁，您需要所有关键部门的支持，包括法律、监管、人力资源和运营部门。这可以通过组建跨功能团队来监督AI的采用、审计和安全措施，并建立明确的政策和控制措施来实现。AI安全应纳入治理、风险和合规（GRC）框架中。组织应根据其特定业务需求定义AI治理原则，并在法律和合规职能之间分配共同责任。与政府和行业同行的合作可以帮助制定前瞻性的网络安全政策。

拥有统一的安全基础架构、共同的数据模型以及集成运营确保了人工智能的无缝集成。

随着AI模型的普及，定制化的AI防火墙可以作为强大的第一道防线，确保交互、防止数据泄露并阻止恶意或未经授权的使用。但仅靠AI防火墙是不够的。全面的防御策略必须包括安全架构、数据保护、访问控制和持续监控，以防止在编排层、RAG数据库和API等方面出现漏洞。确保整个AI栈的安全，包括数据层、基础模型、AI应用以及身份访问和控制，至关重要。

此外，通过红队演练或对抗性测试等方法融入丰富的风险情境，可以增强安全性。这种方法通过严格测试AI模型应对真实世界的攻击场景，发现潜在弱点并构建更为稳健的防御体系。这确保了风险管理的有效性。

评估随快速变化的安全环境不断演进。为了进一步增强AI安全，自动化在简化防御机制方面发挥关键作用，使组织能够迅速应对大规模的AI相关威胁。我们在数字核心指数中的安全成熟度评分显示，领先的企业在安全自动化方面领先于其他企业15个指数点（如图3所示）。

安全的网络物理系统

cyber-物理系统（CPS）对于创造价值至关重要，任何中断都可能导致生产停滞或任务失败。随着连接性的增加，组织对勒索软件和恶意软件攻击的脆弱性也在增加。识别并保护所有CPS，并定期进行漏洞评估。我们在调查中发现，仅有39%的组织具备实时检测信息技术和运营技术事件的能力。[23]。根据我们的数字核心指数，行业领导者在 CPS 安全性方面表现出色，比同行高出 18 个指数点[24]。

实施零信任原则

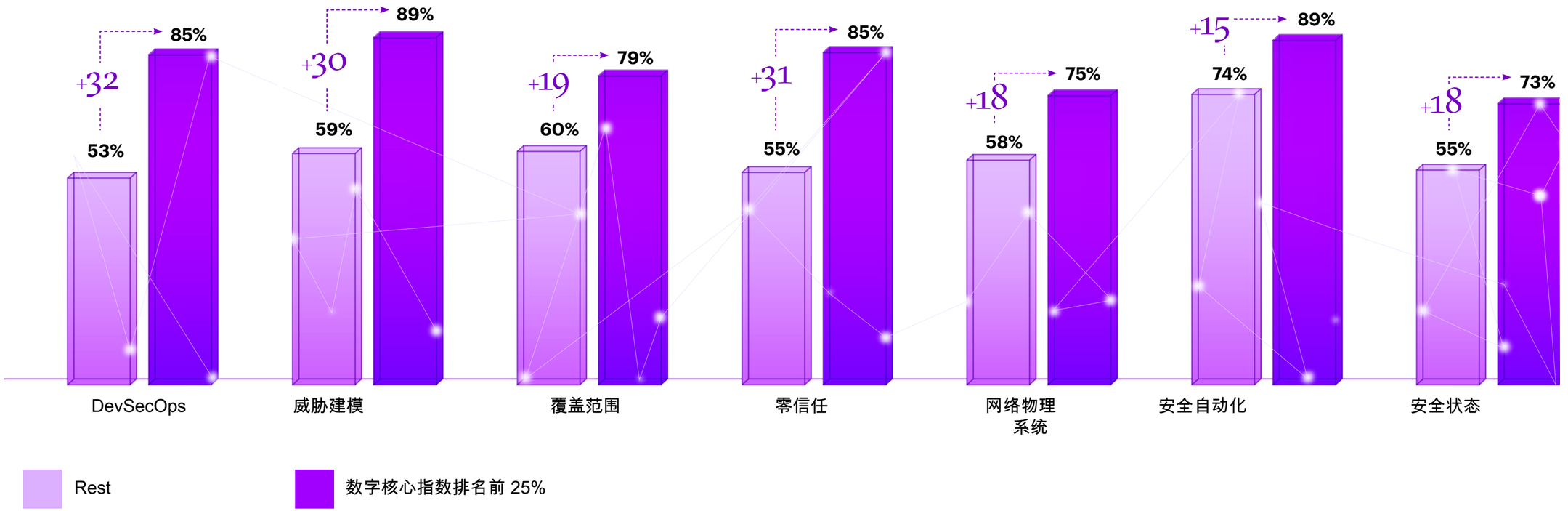
零信任从根本上重新定义了传统安全模型，通过增强组织与现代化应用的连接方式。这种方法对待每一个访问尝试都视为潜在的未授权访问，无论用户的身份或网络位置如何。根据数字核心指数，采用零信任实践领先的企业比同行高出31分。

对于零信任网络，从安全访问服务边缘（SASE）开始。SASE 改进了客户端连接到现代化应用的方式，相较于传统VPN，后者对网络上的所有内容都有访问权限。SASE 将网络和安全功能整合到统一的云服务中，随着组织将安全措施迁移到云端。这种整合减少了复杂性、提升了灵活性，并且保障了多云软件定义广域网（SD-WAN）架构的安全性。

建立网络弹性以加强数字信任

超越传统方法，利用数据和AI进行主动的威胁准备、预测和防御。这一策略的关键组成部分是实施先进的身份和访问管理（IAM）实践，这是一种由政策和技术组成的框架，确保只有授权用户才能访问技术资源。例如，无密码认证就是一个实例。无密码解决方案通过消除与密码盗窃和滥用相关的风险来增强安全性，确保只有经过验证的用户才能访问敏感系统和数据。当与主动威胁检测、自动化事件响应和高级安全措施结合使用时，这些IAM创新显著增强了网络韧性，并强化了客户信任和忠诚度。数字核心指数中的安全成熟度得分显示，领导者在威胁建模和安全状态方面分别比其他公司高出30和18个指数点。

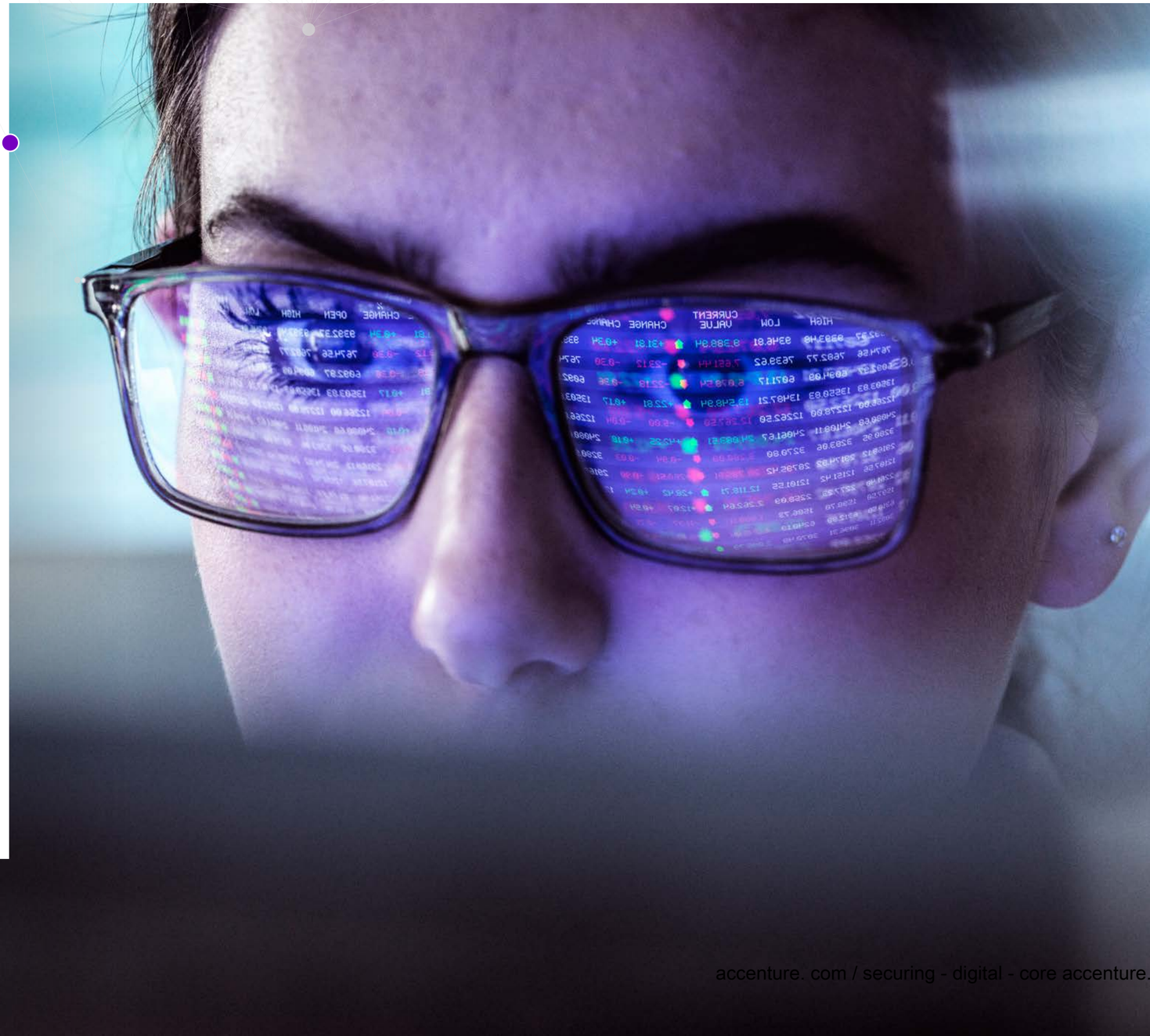
图 3 ： 证券成熟度评分


+32
85%
53%
+30
89%
59%
+19
79%
60%
+31
85%
55%
+18
75%
58%
+15
89%
74%
+18
73%
55%
DevSecOps
威胁建模
覆盖范围
零信任
网络物理系统
安全自动化
安全状态
Rest
数字核心指数排名前 25%

案例研究

面向全球产品制造商的全面云、身份识别和托管安全服务转型

作为其数字化转型的一部分，一家全球产品制造商委托埃森哲安全服务将其业务应用和数据迁移到云端，并提高其IT安全状况。埃森哲的方法包括加速设计即安全的云转型、提高可见性并减少网络安全风险。在八周内，埃森哲修复了客户的AWS云环境，并通过自动化身份控制和治理保护了企业数据湖中的敏感数据。此外，通过增强检测能力、事件响应能力和与MITRE ATT&CK框架对齐，客户的安全运营显著提升。关键成果包括修复了超过36万个漏洞，将误报警减少超过85%，并将可见度从极低提升到约90%。新应用团队的上线时间从两周缩短至48小时，促进了安全的全球协作。最后，客户团队得到了提升，能够独立管理关键的安全控制措施。



杠杆 03

通过自动化和网络安全即服务进行扩展

人才和技能短缺是现代安全化进程中的一大障碍。为了应对这一挑战，企业应利用人工智能和云计算安全服务（CSaaS）来进化并扩大其安全计划。

71%

信息安全分析师执行的任务可以使用生成 AI 进行自动化或增强 [25]。

应采取的行动 ：

通过自动化进行扩展

随着由人工智能驱动的威胁变得更加复杂，传统安全解决方案已变得不够充分。采用基于人工智能的防御技术，并利用自动化工具进行威胁测试，如红队演练和渗透测试。特别是在AI监管不断加强的情况下，这些措施显得尤为关键。领先平台组织和超大规模企业已经开始推出基于AI的安全功能。例如，埃森哲的托管检测与响应（MxDR）服务，借助谷歌云的人工智能技术，能够无缝集成到各种安全环境和云平台中。

使用生成 AI 增强和自动化安全性

通过将生成性AI集成到运营中来转型手动安全任务。我们的分析显示，信息安全部门执行的71%的任务可以通过自动化（28%）或增强（43%）来进行。这种方法不仅提高了效率，还提升了安全态势。我们在数字核心指数中的领先企业得分达到了89个指数点，平均比其他企业高15个点。

采用网络安全即服务

CSaaS 对数字转型至关重要，提供了可扩展、由专家管理的安全解决方案，能够适应不断变化的威胁环境。将安全管理工作外包，专注于创新，同时减少维护多种安全工具和人员相关的复杂性和成本。这种模式不仅增强了整体安全，还确保了合规性和成本效率，成为数字时代成功的关键驱动力。

案例研究

零售组织利用 CSaaS 改善业务成果

当一家零售连锁企业转型为独立的上市公司时，其需要彻底革新其信息技术运营。Accenture 帮助支持零售商的信息安全团队，通过实施和管理公司的安全运营，包括威胁情报功能和安全运营中心（SOC）。如今，Accenture 提供涵盖数据保护、身份管理、网络安保、漏洞管理及安全意识培训等全面的服务。该零售商现在能够从中受益于增强的网络安全韧性以及更加安全的业务成果。

开始使用

在当今数字时代，有效的安全防护不仅仅是保障，更是战略性的使能器，能够区分市场地位。它营造了一个充满信任、韧性和适应性的环境，使组织能够安全地进化其数字核心，抓住新的机遇并强化其竞争优势。

通过询问这些至关重要的问题开始保护您的数字核心识别漏洞和推动行动的问题。

每个公司都应该问自己的问题 ：

流线

• 使用了多少安全工具来管理我们的安全状况 ？

• 我们是否仍然依赖传统安全工具来防范网络威胁 ？

现代化

• 我们组织的网络安全是否已迁移到云端，并设计了加速安全工具部署和配置的资产？

• 我们的网络安全计划是否足够成熟和敏捷 ，以有效地应对现代威胁 ？

规模和进化

• 我们是否利用AI通过自动化来扩大安全规模？ • 我们是否利用CSaaS专长来进化安全运营？

参考文献

1. 以数字化为核心重塑自我 | 毕马威
2. 安全领导者同行报告 | Panaseer
3. 2024年网络安全人才研究 | ISC2 研究
4. 在生成式AI时代重塑自我 | 毕马威
5. 2024年以数字化为核心重塑自我调查 | 毕马威
6. 信任守护者调查2024 | 毕马威
7. 具有韧性的首席执行官：网络安全韧性 | 毕马威
8. 隐形的1.52万亿美元问题：陈旧软件的挑战 | 《华尔街日报》
9. 安全领导者同行报告 | Panaseer
10. 2024年网络安全人才研究 | ISC2 研究
11. 2023年网络安全状态报告 | ISACA
12. 具有韧性的首席执行官：网络安全韧性 | 毕马威
13. 网络安全泄露对企业的影响 | 《哈佛商业评论》
14. SecOPs 2023之声 | 深信服
15. 世界经济论坛网络安全展望2024 | WEF 和安永
16. 钓鱼邮件状态2023 | 斜线网宁
17. 身份欺诈报告2024 | Onfido
18. 穿过幻象——揭开深度假新闻的真实威胁 | 普华永道
19. 全球威胁报告2024 | 科德斯派克
20. 第一个使用AI进行诈骗的案例：深度假新闻诈骗者非法获得2.5亿美元 | Ars Technica
21. 厄戈斯航空公司数据泄露事件：6.5TB数据暴露在未受保护的AWS存储桶中 | 技术监测
22. 云配置错误导致丰田汽车大规模数据泄露 | 首席安全官
23. 以数字核心重塑调研2024 | 普华永道
24. 以数字核心重塑调研2024 | 普华永道
25. 研究建模与分析 | 普华永道

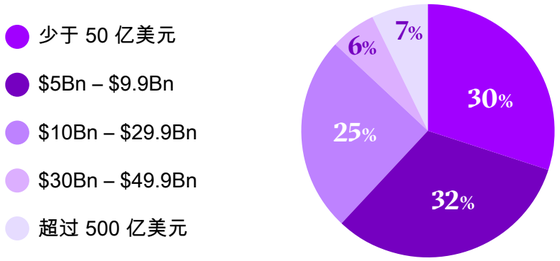
关于研究

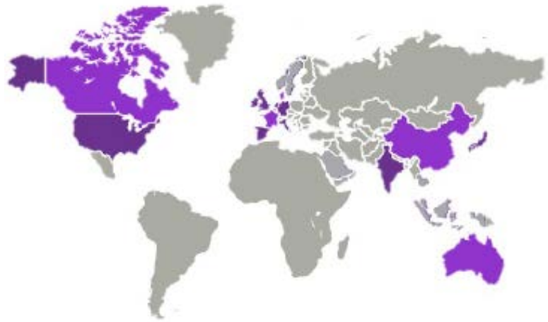
量化高管调查

用于支持这一观点的数据基于我们《以数字为核心进行重塑》研究中的安全相关数据。

1,500 全球高管
52% 完成技术转型
19 仅限行业
C 级

公司规模





行业覆盖范围

金融服务银行 (83) 资本市场 (45) 保险 (86)

Resources

公用事业 (83) 能源 (包括石油和天然气) (83) 化学品 (84) 自然资源 (81)

产品

零售（115）消费品与服务（113）航空、旅行与运输（80）航空航天与国防（41）工业设备（80）生命科学与制药（79）汽车（81）

媒体与技术

媒体与通信 (80) 高科技 (82) 软件与平台 (86)

公共服务 (40) 健康与公共服务医疗保健 (78)

10 个国家

澳大利亚 (50) 印度(80)
加拿大 (70) 意大利 (50)
中国(80) 日本(100)
德国 (130) 英国 (130) 法国 (90) 美国 (720)

安全指数

我们构建了一个综合指标（指数）来衡量公司数字核心能力的强度，基于39个评估问题（其中7个集中在安全方面）。我们应用了两步聚合过程，对应于数字核心组件的定义，并将总体得分标准化到0-100的尺度，其中100表示所有组件的最大强度，而0表示其不存在。接下来，我们根据整体数字核心指数得分分布创建了三个组织群体。领先群体对应于数字核心指数的前四分位数，我们称之为领导者。然后我们将领导者的各个组件的安全成熟度得分与其余群体进行了比较。该指数代表了他们数字核心的整体强度，即每个组件能力的平均值。能力点表示特定技术的相对复杂程度。差距表示为达到下一个能力水平所需的现代技术现代化活动。差距越大，实现目标能力水平所需的时间和投资就越多，从而解锁相应的价值。

Authors

Paolo Dal Cin

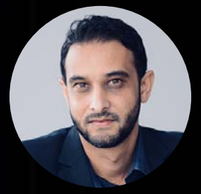
全球领先 - 埃森哲安全

雷克斯 · 塞克斯顿

埃森哲安全首席技术官

安德鲁 · 温克尔曼

网络保护团队首席技术官 - 埃森哲安全



Yusof Seedat

全球研究主管 - 埃森哲安全

Acknowledgements

研究负责人 ：
Manav Saxena

研究团队 ：
Gargi Chakrabarty, Arlene Lehman, Shachi Jain

营销团队 ：
Mark Klinge, Kamilla Giedrojc, Eileen Moynihan, Ewa Szkudlarek

作者们特别感谢John Delmare、Muthu Raja Sankar、Ganesh Devarajan和Sadhana Joliet为本次研究提供的见解和贡献。

关于埃森哲

埃森哲是一家全球领先的专业服务公司，帮助世界上领先的商业机构、政府和其他组织构建其数字核心、优化运营、加速收入增长并提升公民服务，从而在速度和规模上创造实际价值。我们是一家以人才和创新为驱动的公司，在全球超过120个国家和地区为客户提供服务，人数达73.8万人。今天，技术正在推动变革的核心，而我们是世界领导者之一，致力于推动这一变革，并拥有强大的生态系统关系。我们将自身在技术领域的优势与无与伦比的行业经验、功能专长以及全球交付能力相结合。由于我们在战略与咨询、技术、运营、行业X和埃森哲歌曲方面广泛的服务、解决方案和资产，我们能够提供独特的成果。我们的文化强调共同成功，并致力于创造全方位的价值，这使我们能够帮助客户取得成功并建立值得信赖的长期关系。我们衡量成功的标准是为客户、彼此、股东、合作伙伴和社区创造全方位的价值。

访问我们 www. accenture. com

关于埃森哲研究

德勤研究就组织面临的主要商业问题创造思想领导力。结合数据科学驱动的分析等创新研究方法，以及对行业和技术的深刻理解，我们分布在20个国家的300名研究人员每年发布数百份报告、文章和观点。与世界领先组织共同开发的引人深思的研究帮助我们的客户拥抱变革，创造价值，并利用技术和人类智慧的力量。如需更多信息，请访问德勤研究网站www.accenture.com/research。