Deloitte.

2023全球网络安全前瞻调研报告

将网络安全置于业务核心位置
构筑长期价值

网络安全即正解

当下，网络安全行业的发展保持着强劲态势。企业领导人通过全新、敏锐的视角洞察网络安全给企业带来的商业价值。网络安全是构筑企业及其强大增长战略的重要组成部分。

德勤《2023全球网络安全前瞻调研报告》结果显示，网络安全不再只是企业一项义务或一系列以技术为主的网络健康实践，它已发展成为关乎业务成果实现的重要职能。本全球调研（德勤迄今规模最大的网络安全调研）通过对来自不同行业的企业领导人展开访谈，深入揭示了网络安全现状，亦聚焦于探明其未来趋势。我们发现网络安全对业务发挥着日益巨大的促进作用。各大企业纷纷将网络安全纳入议程，并视之为重大业务计划和投资的关键。

网络安全的未来振奋人心。诚邀您与我们共同探讨本报告的主要观点。除调研结果相关数据外，本报告还包括直接来自受访高管的意见和见解，以及德勤对网络安全、云和其他业务发展支持技术的相关洞察。

祝好！

德勤全球网络安全服务领导人

Emily Mossburg

目录

聚焦网络安全

将网络安全置于业务核心位置以构筑长期价值

随着全球企业纷纷将对网络安全的关注重点从网络安全技术及威胁本身转向在业务中深度整合网络安全思维和网络安全行动而实现的潜在积极成果，网络安全的未来变得更加引人瞩目。

全球日益互联，带来新增长机会的同时也催生出新风险。数字技术、数据的指数级增长以及业务需求的日益发展正不断扩大网络威胁攻击面并带来新的挑战，网络安全问题由此升级为战略性业务问题。网络安全、风险管理以及跨部门协作对于消除网络威胁、保护商业价值和维护客户信任至关重要。

近年来，许多企业领导人都在关注向数字化业务流程的持续转型及其技术环境和网络威胁形势的快速演变。事实上，混合IT架构和数字化转型已成为企业面临的两项最大挑战，由此产生的复杂性将成为企业新常态。[1]

本次调研结果所呈现的新形势，聚焦了当前全球数百位不同行业领导人对网络威胁、企业活动及未来的看法。调研对象包括企业首席高管以及拥有IT、安全和风险背景的资深高管。

网络安全正超越其传统IT本源，发展为独特的业务职能领域，并成为业务成果交付框架的重要组成部分。

合作伙伴关系转型

“我们逐渐开始将网络安全问题视为重要的企业业务风险。将网络安全视为推动转型的核心力量（而非次要因素或事后考量事项）的企业，其合作伙伴关系亦发生重大转变。无论是DevSecOps还是在产品开发中，我们都在网络安全方面投入了很多工作，我们开始与（内部）合作伙伴展开协作，确保业务的安全开展。”

——壳牌集团首席信息官/首席信息安全官Allan Cockriel

展望2023年及未来，网络安全的发展将远远超出其技术本源。对于许多企业而言，网络安全如今与业务运营、成果及机遇之间的关联愈发紧密。网络安全已不再只是技术问题，而是关乎组织发展战略的根本性议题。对于企业网络安全决策者而言，网络安全已成为业务架构的组成部分，是实现企业愿景的核心要素。

正如网络威胁从IT问题转变为业务问题一样，网络安全战略亦从IT战略转变为业务战略，并最终支持战略业务目标和增长。企业董事会层面日益重视网络安全，并将其作为业务优先事项之一。在本次调研中，70%的受访者表示网络安全是董事会常规议题，会按月或按季度开展讨论。

这也清晰地表明，网络安全对于制定高级别、战略性业务决策至关重要。

企业愈发意识到网络安全在支持实现商业成功方面所发挥的作用。

绝大多数受访者认为网络安全与业务成果息息相关：86%的受访者表示，网络安全计划至少对一项业务优先事项具有显著积极影响。大多数企业纷纷表示将在这一价值主张的基础上持续建设：58%的受访者称所在企业正计划在来年加大网络安全投资。

70%

的受访者表示网络安全是董事会常规议题，会按月或按季度开展讨论。

董事会洞察

“董事会显然很关心网络安全问题，并将为此合理调配资源，董事会现已具备知识与能力甄别其网络安全负责人究竟是名副其实，或是滥竽充数。随着他们认识到这一差别，高管层和董事会的容忍度将会有所改变。”

——某消费者保护组织首席信息安全官

尽管网络安全对业务具有促进作用，但不同企业的网络安全建设水平或有不同。部分企业已走在网络安全发展的最前沿，并为其他企业开辟出一条正确路径。

在本次调研中，德勤从网络安全规划、战略行动实施以及董事会参与情况三个维度，评选出了高绩效、高网络安全成熟度企业。这类企业正全面实施网络卫生相关重要计划，包括：运营与战略计划、持续改善企业信息安全的行动计划以及监控并跟踪合作伙伴和供应商安全状况的网络风险计划。

将网络安全和商业价值有机结合的高成熟度企业更有可能将网络安全的积极影响辐射到以下领域：

- 品牌声誉
- 客户和数字信任
- 运营稳定性（包括供应链和合作伙伴生态系统）
- 营收

高成熟度企业也更可能表示，网络安全可带来关键业务战略价值，增强其尝试新事物的信心，并提升业务敏捷性和效率。这类企业也更可能认识到第三方网络安全服务所蕴藏的高价值。

助推业务发展

“若不考虑信息安全和隐私影响，并将其嵌入适当的流程中，就无法实现项目、计划和业务目标。因其与业务组件及领域密切相关，我们在业务构思阶段便将此项工作纳入考量。我们的策略是全力提供业务支持，也认识到没有业务就不存在网络安全和隐私问题。我们希望能够安全合规地为推动业务发展、促进增长做出有意义的贡献。”

——万豪国际集团高级副总裁兼首席信息安全官Arno Van Der Walt

54%

全年收入50亿美元及以上的企业称每年的网络安全支出超过2.5亿美元。

71%

收入在5亿美元至50亿美元的企业称每年的网络安全支出不足2.5亿美元。

调研方法

方法论

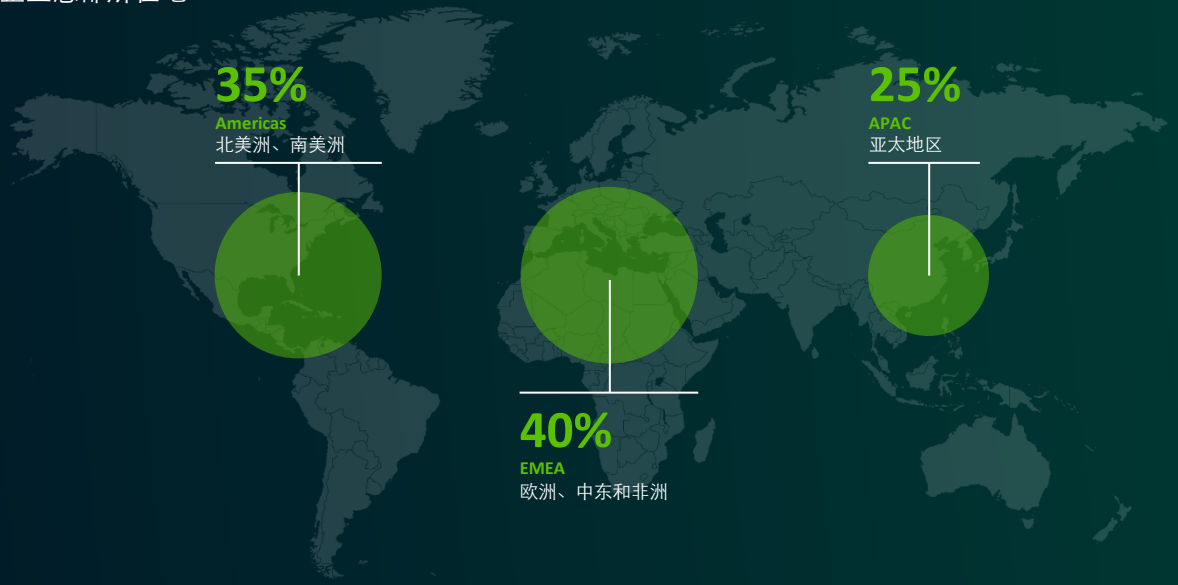
德勤基于当前商业和技术环境的复杂性展开《2023全球网络安全前瞻调研》，重点关注那些已认识到网络安全的重要性但难以实现其价值的企业领导人的需求。我们对来自20多个国家的一千余位董事级或更高级别（首席高管或更高级别）的网络安全服务领导人展开调研，他们均来自员工人数不低于1,000名且年收入不低于5亿美元企业。

为准确把握网络安全对当今企业日益增长的影响，我们将样本量从2021年的近600位受访者增至1,110位受访者，增加了近一倍。德勤还与来不同地区及行业的多位网络安全服务资深高管展开深度访谈，以收集更详细的见解，并帮助验证我们的调研结果。我们的调研方法涵盖了与网络安全未来相关的战略、战术、文化以及技术实施等各个方面。

本次调研旨在：

- 探讨自德勤2021年调研以来的网络安全发展变化
- 运用前瞻性视角，聚焦网络安全未来
- 了解网络安全为企业带来的商业价值和影响，以及领先企业为实现网络安全更高价值而采取的特定行动

受访企业总部所在地



网络安全即未来

除回顾网络安全在过去两年的发展概况外，我们还以网络安全成熟度为新切入点，探究网络安全建设水平领先企业采用更成熟的网络安全战略所产生的业务影响。

我们将高网络安全成熟度企业与中低成熟度企业区分开来，由此评选出网络安全建设水平领先企业，并充分了解网络安全对于业务成果和价值实现的影响程度。

如今，*网络安全*即*业务*，网络安全是关乎企业发展的根本性要务，其重要性不言而喻。对任何企业而言，网络安全的未来发展将取决于高管层和董事会的承诺，以及企业透过其所预见的商业价值。总之，我们的调研结果显示，随着首席信息安全官等高管与董事会携手合作，共同领导业务并推动创新，网络安全呈现蓬勃发展新态势。

换句话说，企业应将网络安全纳入业务战略的方方面面。每个职能部门都应重视网络安全管理，这不只是为降低IT风险，更是为持续挖掘其潜在商业价值，从而实现业务目标。

显著影响

“我们缓解风险的经验，清楚地表明我们了如何卓有成效地保持了运营工作的持续平稳高效运行——尤其是与我们的业务合作伙伴相比，他们往往面临运营或集成挑战。”

——某消费者保护组织首席信息安全官

网络安全发展历程

自德勤2021年调研报告发布以来，全球各行业在多个领域面临持续起伏，同时相应地调整其优先事项、业务计划和能力。

2021年调研和本次调研均问及受访者所在企业的数字化转型优先事项，以帮助企业确定哪些是重要技术，并考量是否应将其纳入未来网络安全战略。

较之于2021年企业的两大优先事项，云取代数据分析从第二位升至首位。运营技术/工业控制系统和人工智能/认知计算仍位列前五，优先级略有上升。5G首次跻身今年五大要务之列，反映出该标准对于企业目标的重要性与日俱增。

云的重要性有增无减，由此引发了复杂的网络安全考量因素，这些因素是异地托管数据和应用程序所固有的，且往往存在于各种环境。尽管云和网络云的成熟度差异很大，但我们近期开展的有关云的前瞻调研结果表明，许多企业正在克服此等问题，并在与风险相关的云用例中取得良好成果。事实上，有83%的企业称其云投资在降低业务和监管风险方面取得了良好成果。[2]这是一个积极信号，表明云安全能力、责任共担模式和数据隐私计划正日益成熟并逐步落地。

数字化转型优先事项

过往与当下

2021

数据分析　云　ERP系统新建/升级计划　运营技术/工业控制系统　人工智能/认知计算

2023

云　数据分析　运营技术/工业控制系统　人工智能/认知计算　5G

网络安全的作用

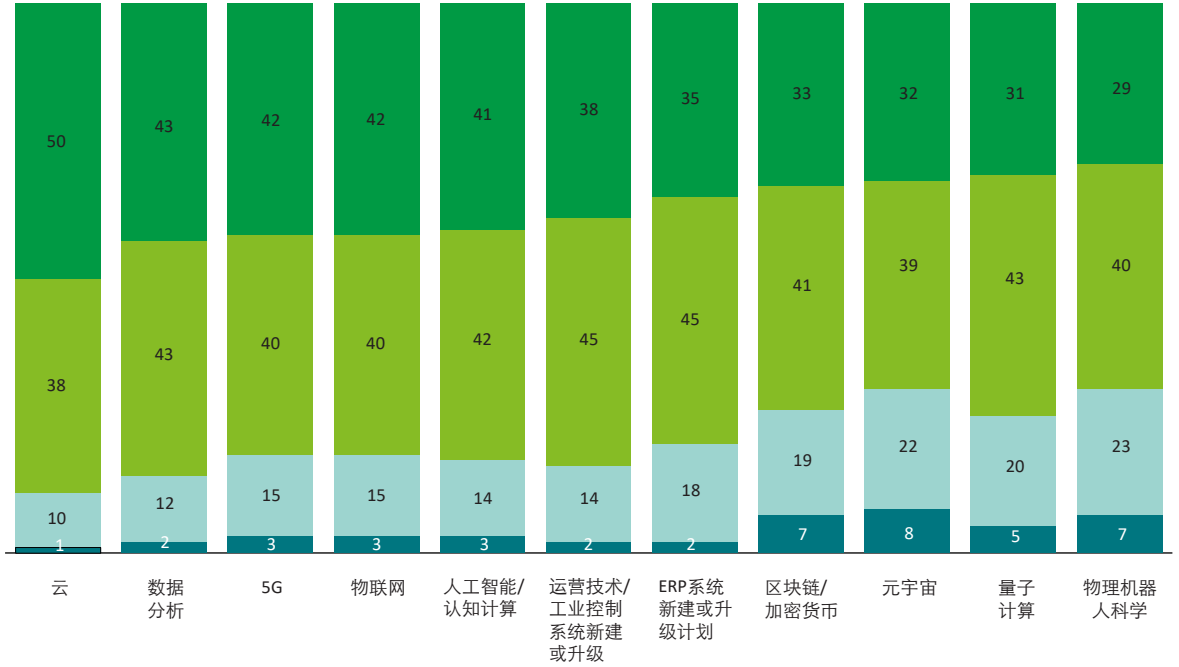
在本次调研中，我们问及受访者网络安全在企业主要数字化转型计划中所发挥的作用。结果很明显：高管纷纷认为网络安全在所有数字化转型优先事项中发挥着至关重要的作用，尤其是在云、数据分析和5G方面（图1）。

数字化转型优先事项和新兴技术不断演变，而网络安全事件对企业的影响也在不断加剧。即便企业着眼于网络安全就绪带来的积极效益和长期业务价值，也仍须注重构建抵御网络威胁的核心能力，以减轻不良业务后果和风险。

图1：网络安全成为企业关注焦点

网络安全将在企业的数字化转型计划中发挥主导作用

（由于四舍五入关系，百分比加总可能不等于100%。）



首要议题

“各大企业均将网络安全列为首要议题，并将其纳入了战略设计、预算设计以及解决方案设计。”

——某金融服务机构首席信息安全官

网络安全事件及其影响洞察

网络安全或数据泄露事件发生频率持续增长，91%的企业称至少遭遇过一次事件，而在2021年调研中这一比例为88%。企业内部的众多网络使用者、数据源、工具和技术均可能引发网络安全问题。

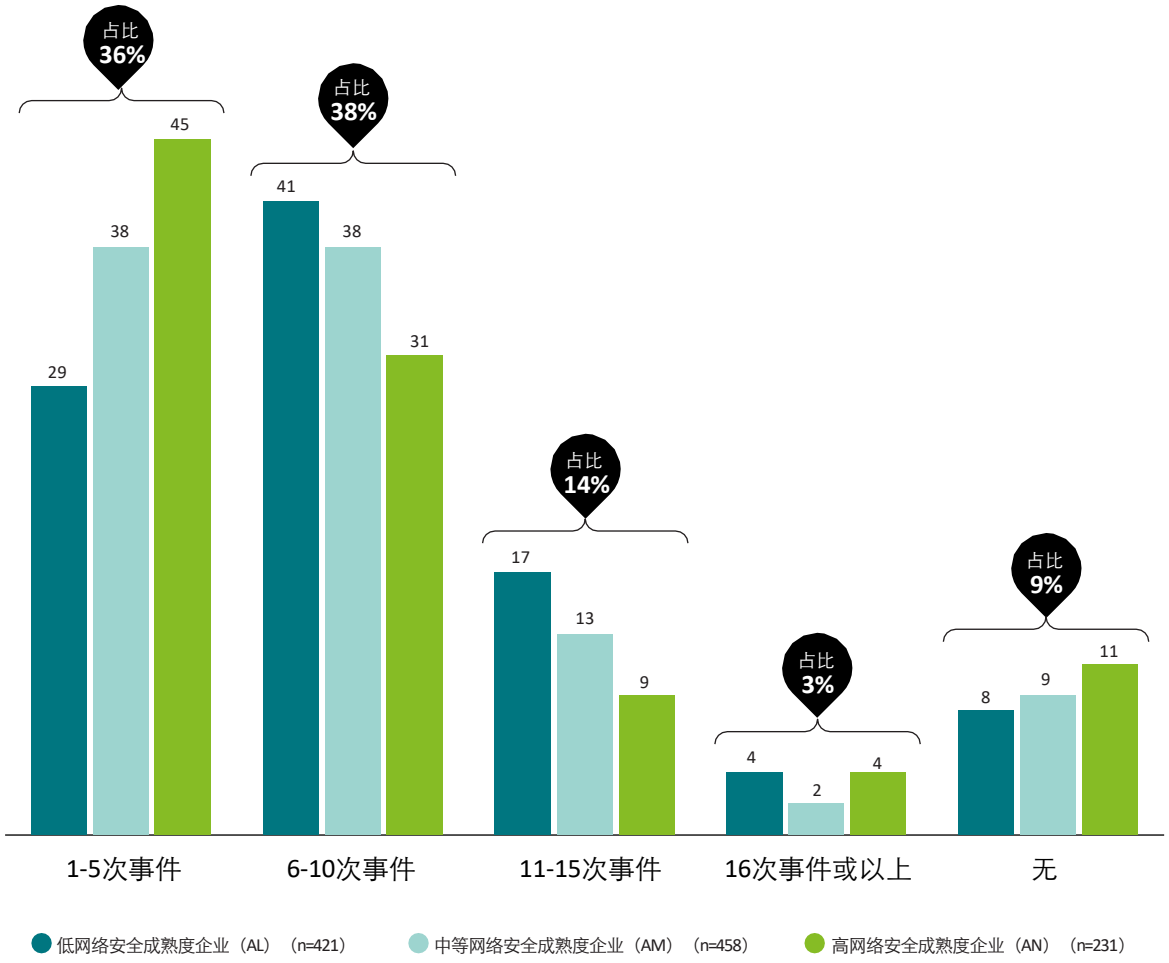
高网络安全成熟度企业似乎更担心来自网络犯罪分子和恐怖分子的攻击，以及网络钓鱼、恶意软件和勒索软件攻击。中低成熟度企业更担心拒绝服务型攻击。值得注意的是，低成熟度企业称遭遇了更多重大网络安全事件（图2）。

91%

的企业称至少遭遇过一次网络安全或数据泄露事件。

图2：重大网络安全事件发生数量

（百分比）



与此同时，业务运营中断仍然是网络安全事件造成的最大影响，尽管收入减少和客户信任流失的排名跃升至第二和第三位（56%的受访者表示在一定程度或很大程度上承担了相关后果）。此处存在一个潜在假设：网络安全成熟度较高的企业对网络安全事件造成的业务影响的实际情况有着更深刻的理解，可能会以不同方式看待影响。成熟度较低的企业可能会评估理论性影响。无论如何，高成熟度企业的确从网络安全计划中获得了更大效益，包括提高品牌声誉、客户信任、运营效益和财务效益。中低成熟度企业则更多地在提高品牌声誉和客户信任方面获益。

鉴于上述重大影响，企业须在其生态系统（涵盖网络安全战略、解决方案和控制举措）中制定基于风险的网络安全战略，这对于企业的未来网络安全至关重要。零信任安全架构可以通过加强安全态势、简化安全管理并改善最终用户体验来实现现代化企业环境。实施零信任安全架构需要制定一个业务成果导向型战略，并辅以大量投入和规划，如解决基础网络问题，实现人工流程自动化以及展开安全部门、技术环境乃至企业整体转型规划。[3]

图3：网络安全事件的最大影响

网络安全和数据泄露事件对企业造成的负面影响

（基于2021年排名前两项的答案和2023年排名前两项的答案）

网络安全和数据泄露事件造成的负面影响	2021年（排名）	2023年（排名）	2023年（百分比）
运营中断（包括供应链和合作伙伴生态系统）	1	1	58%
收入减少	9	2	56%
客户信任流失/负面的品牌效应	4	3	56%
声誉损失	5	4	55%
战略计划撤资	不适用	5	55%
对技术完整性失去信心	不适用	6	55%
对人才招聘/留用的负面影响	8	7	54%
知识产权盗窃	2	8	54%
股价下跌	3	9	52%
监管罚款	7	10	52%
领导层变更	5	不适用	不适用

零即是无限

零信任安全架构的实施不仅是一项技术实施，更是一场由文化、沟通和意识决定成败的业务和文化变革。

零信任安全架构的全面实施离不开企业在治理（架构和运营）、支持技术（如分析技术和自动化）以及核心领域（如身份、数据和设备）方面的协作配合。

56%

的受访者表示所在企业在一定程度或很大程度上受到相关影响。

网络安全成熟度的意义

如今，网络安全的重要性日益凸显，我们从与全球数千家企业的合作中借鉴经验，根据受访企业的网络安全成熟度对其进行分组。

确定网络安全成熟度

为确定网络安全成熟度并评选出引领网络安全未来的高绩效企业，我们基于三套领先实践对企业进行评级：

强大的网络安全规划
即拥有抵御和应对网络威胁的战略、运营和战术计划

关键的网络安全活动实施
例如开展定性和定量风险评估、行业基准分析以及事件响应情景规划

有效的董事会参与
例如企业董事会定期处理网络安全相关问题

深入探究不同成熟度企业分组：
我们通过对领先实践设定分值，最终将受访企业分为以下三组：

不同行业、不同规模企业的网络安全成熟度

我们从多项特征着手对三组受访企业展开深入探究，以确定其网络安全成熟度趋势及特征。

在按低、中等、高成熟度划分的三个组别中，均匀分布着来自不同行业、拥有不同规模和收入的企业——这表明企业的网络安全成熟度水平与其所处行业或规模并无显著关联。

38%
的**低网络安全成熟度**企业不遵循任何领先实践

41%
的**中等网络安全成熟度**企业，遵循一套领先实践

21%
的**高网络安全成熟度**企业，遵循两至三套领先实践

网络安全建设关乎企业价值实现

我们提出的三套领先实践——网络安全规划、活动实施以及董事会参与——其遵循程度取决于利益相关方对网络安全责任和企业全面参与的重要性之认知。

尽管首席信息安全官是企业网络安全的守卫者，但这些领先实践只有通过企业全面参与才能实现。

各企业可参考以下建议：

- 成立一个由IT和高级业务领导人组成的治理机构，负责监督网络安全计划
- 展开企业和/或董事会层面的事件响应情景规划和模拟
- 定期向董事会报告网络安全更新以获得资金支持
- 每年对全体员工开展网络安全意识培训

高成熟度企业已然认识到在其内部合理分配网络安全责任的有效性。此等做法与德勤的一般性指导（即为各业务部门配备网络安全专业人员，或至少为各业务部门配备负责与网络安全团队对接的人员）不谋而合。高成熟度企业将治理不足视作网络安全管理面临的首要挑战的比例下降了31%（低成熟度企业为35%，中等成熟度企业为34%，高成熟度企业为22%）。

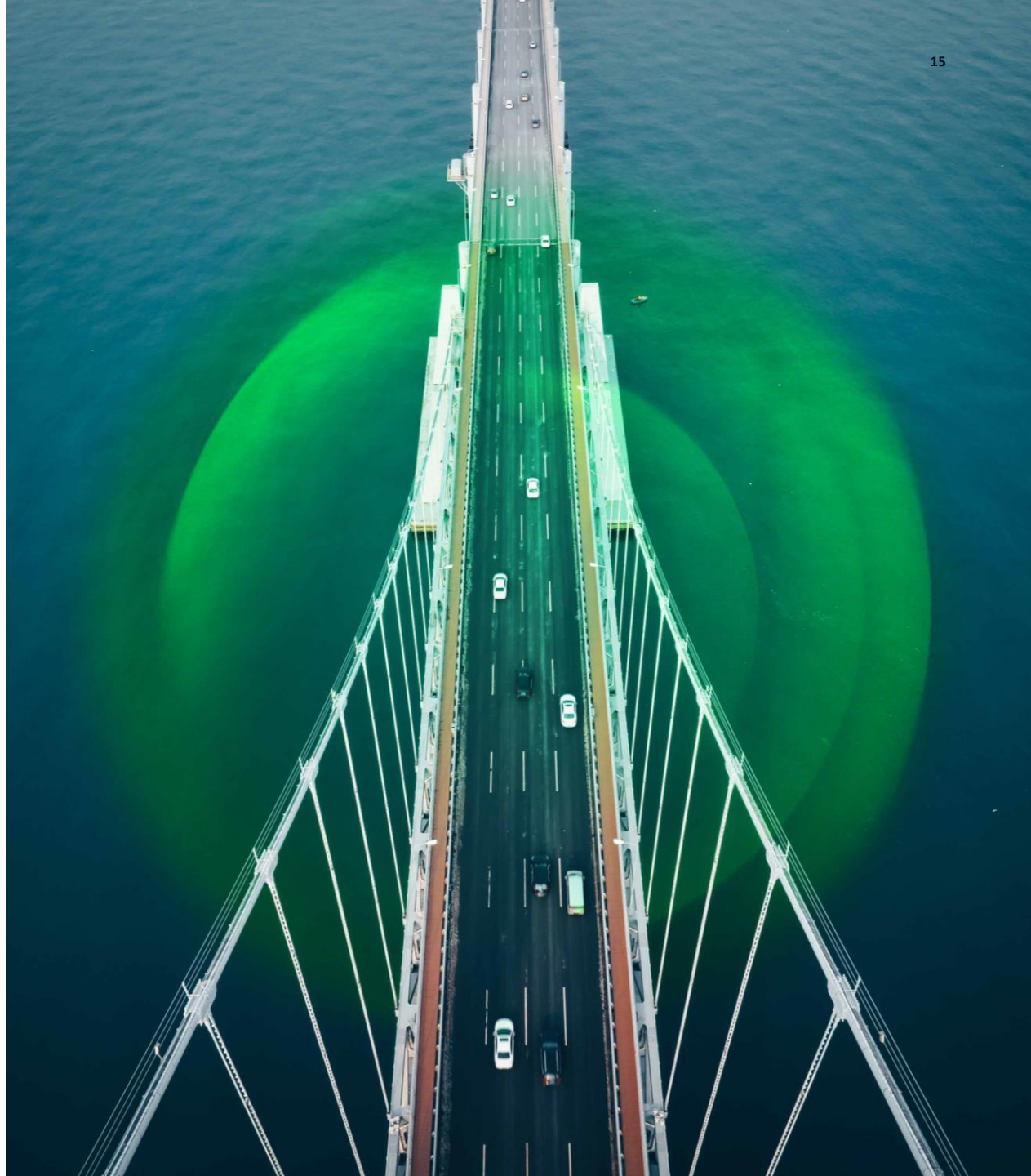


图4：各行业网络安全发展现状

网络安全战略规划示例

- 每年分析并更新网络安全计划
- 成立一个由高级业务和IT领导人组成的治理机构，负责监督网络安全计划
- 利用风险量化工具来衡量和确保网络安全投资回报
- 展开企业和/或董事会层面的事件响应情景规划
- 获取外部支持/外包服务以管理网络安全计划

网络安全活动实施示例

- 每年对全体员工开展网络安全意识培训
- 每年更新并测试网络安全事件响应计划
- 制定涵盖数据存储、处理和传输流程的数据保护综合评估计划
- 制定网络风险监测计划，用以监测并跟踪合作伙伴和供应商的安全状况
- 将客户反馈意见纳入企业网络安全和数据隐私治理偏好

行业

在本次调研所涉及的六个行业中，有三个行业实施了五项及以上网络安全活动（略高于整体平均水平），它们分别是政府及公共服务（GPS）；能源、资源及工业（ERI）；以及科技、传媒和电信（TMT）行业。

有两个行业（能源、资源及工业和生命科学与医疗）开展了五项及以上网络安全战略规划，略高于整体平均水平。

同时，金融服务行业正在开展八项网络安全战略规划中的四项，略高于整体平均水平。然而，该行业在实施网络安全活动方面落后于整体平均水平，仅一项活动实施高于整体平均水平。

据本次调研数据显示，消费行业在实施网络安全活动方面略微落后于其他行业和整体平均水平，在十项关键网络安全活动实施中，有七项略微落后于整体平均水平，且所有网络安全战略规划的开展水平均低于整体平均水平。

企业规模

本次调研还表明，拥有20,000名及以上员工的企业更有可能：

- 认识到风险管理、数字化转型、数字信任和技术现代化相关业务战略的重要性。
- 认识到网络安全在业务战略中的重要性。
- 开展网络安全规划并实施关键网络安全活动。

前瞻洞察

无论所处行业或规模大小，每个企业都有望朝着更高的网络安全水平和成熟度发展。成功并非仅取决于企业的网络安全投资能力。相反，采取积极行动和树立良好文化才是提高网络安全水平的关键。

本次调研中，我们将收入在5亿美元至10亿美元之间的企业定义为小型企业，收入在100亿美元及以上的企业定义为大型企业。

网络安全支撑业务发展

为网络安全构建更大的商业案例

无论企业的网络安全成熟度如何，都不存在能够保证绝对安全和风险降低的网络安全架构或方法。相反，高成熟度企业最显著的特点是其能够从网络安全投资中获取价值。

高绩效企业在领导层参与、规划和行动方面投入更多，从中获得的商业价值也更多。高成熟度企业从网络安全中获得的效率、韧性和敏捷性助益更大，并更能洞察到网络安全带来的潜在助益。

网络安全带来信心提升等多项助益

过半高成熟度企业（55%）称网络安全使其有信心尝试新事物，而中、低成熟度企业的这一比例分别为45%和40%。

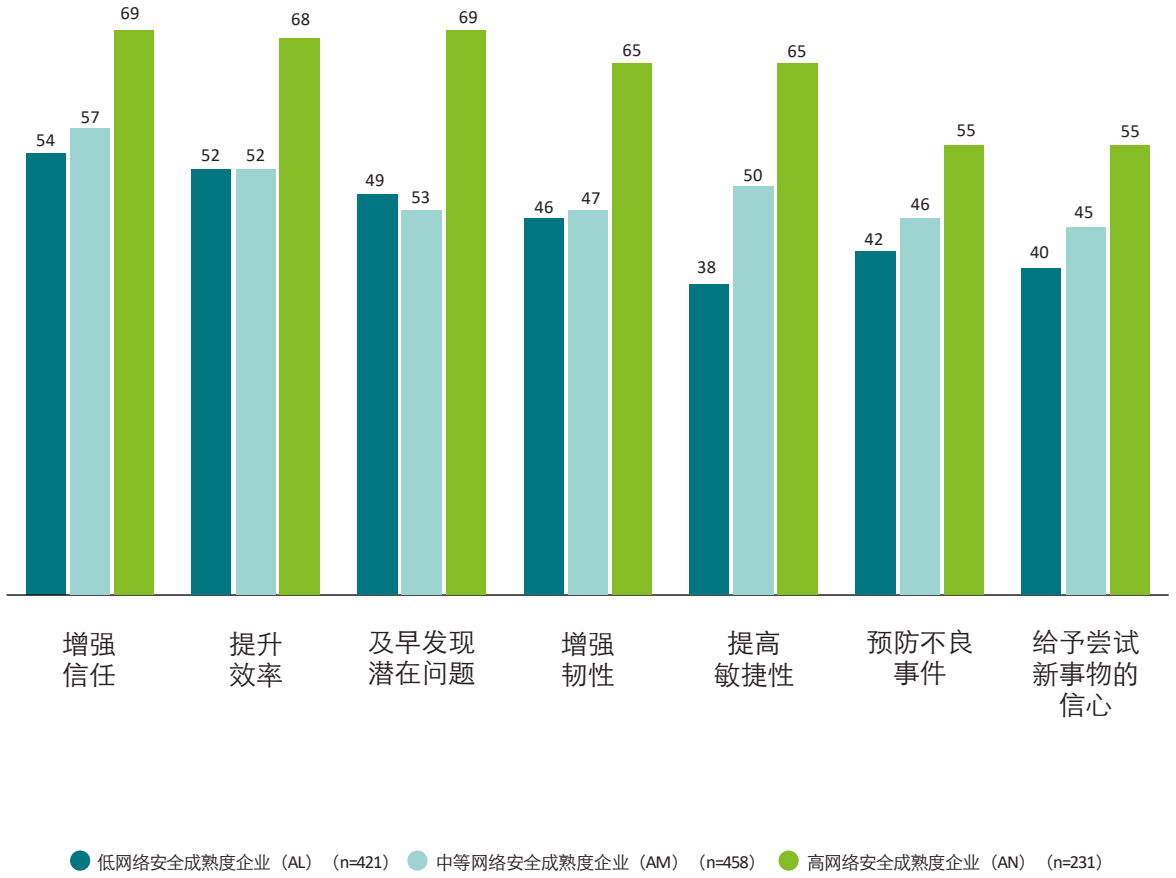
近70%的高成熟度企业表示网络安全有助于其增强业务信任并促进业务效率提升，这一比例远超中低成熟度企业。

无独有偶，大多数高成熟度企业（65%）认为网络安全为其带来了经营韧性和敏捷性，这一比例再次远超中低成熟度企业（图5）。

图5：探究网络安全无限潜力

网络安全对企业活动产生的具体影响

（百分比）



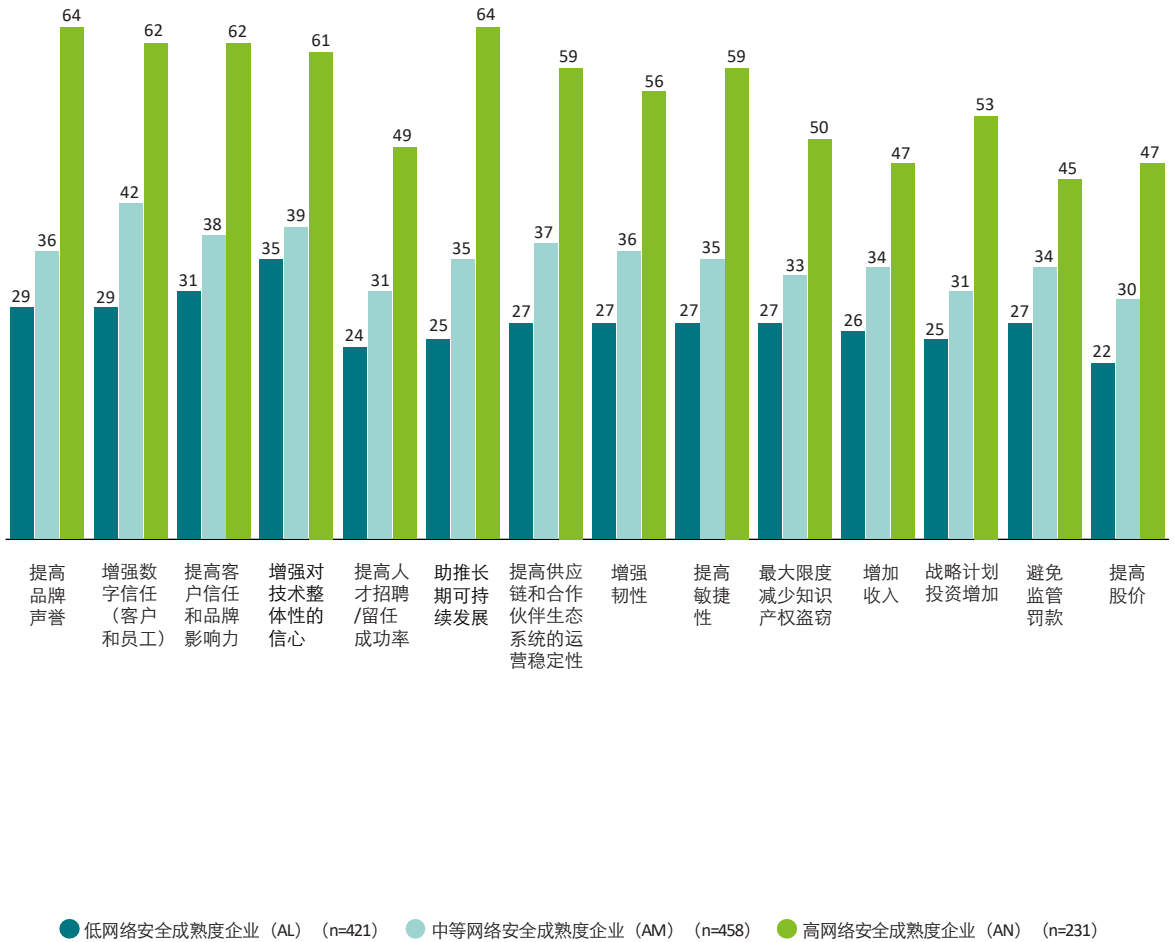
55%

的高成熟度企业称网络安全使其有信心尝试新事物。

图6：网络安全带来的实质性助益

网络安全计划对以下领域带来积极影响

（百分比）



高绩效企业也更多地表示其网络安全计划带来了以下积极影响：提高品牌声誉（64%）、增加收入（47%）、提高供应链和合作伙伴生态系统的运营稳定性（59%）、提高人才招聘和留用成功率（49%）、助推长期可持续发展（64%）、提高客户信任和品牌影响力（62%）。

信任对于构建网络安全而言至关重要。网络作为一个关乎业务成果实现的“生态系统”，需要企业与所有利益相关方建立信任。举例而言，一支值得信赖的工作团队可将客户满意度提高两倍，而信赖某品牌的客户其回购率高达88%。建立客户信任还可为合作伙伴带来积极影响，并使市值提高4倍，受客户信任的企业其业绩表现终将比竞争企业高出400%。

据本次调研数据显示，全球性企业十分清楚网络安全与信任提升等助益之间的关联。虽然投资于网络安全的各大企业纷纷表示在多项战略价值衡量指标上受益显著，但高绩效企业在每项价值衡量指标上均获得了更高助益（图6）。

客户期望

“我个人认为，客户不愿为（我们产品中的）网络安全功能支付太多额外费用，但他们*期望*能拥有该服务。这将成为拉开行业竞争差距的一点。”

——某汽车协会首席信息安全官

400%

建立客户信任可为合作伙伴带来积极影响并提高市值，受客户信任的企业其业绩表现最终会超越竞争对手。

高网络安全成熟度企业在另一领域超越了中低成熟度企业：他们看到了第三方网络安全服务所蕴藏的价值。

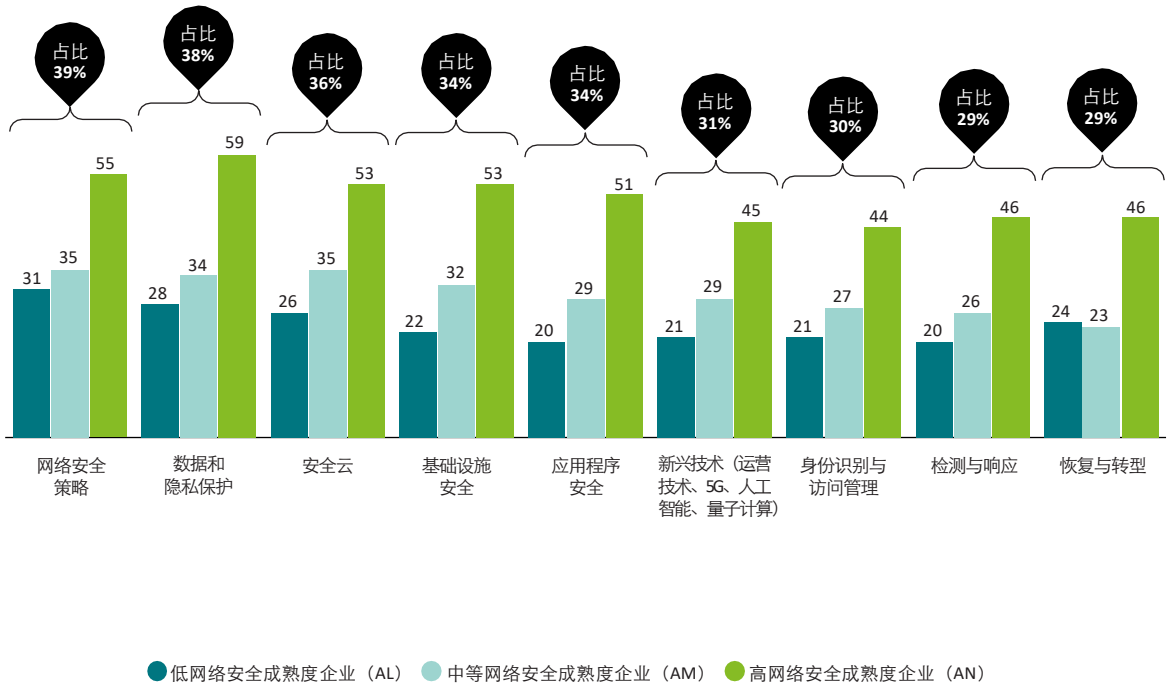
大多数高绩效企业表示他们从第三方提供的网络安全策略、数据与隐私保护、安全云、基础设施安全以及应用程序安全服务中获得巨大价值。

同时，仅有少数中低成熟度企业表示获得了上述服务价值。

为实现第三方网络安全服务价值，企业应思考如何管理其日益庞杂的服务生态系统，这点至关重要。（图7）

图7：获得供应商服务价值

企业认为具有价值的第三方网络安全服务（百分比）



经验之谈：紧跟领先企业步伐

鉴于高绩效企业通过网络安全投资获得巨大商业利益，其他企业应以之为榜样，并据之制定一套指导原则，从而提高自身的网络安全水平。

基于高成熟度企业从网络安全中取得诸多成果，贵企可能是时候深入探究以下问题：

我们是否拥有适宜的技术和合作伙伴生态系统——我们又该如何管理日益庞杂的第三方网络？

我们是否以恰当的方式在恰当的领域进行投资——我们是否拥有正确框架来了解网络安全提升企业价值的具体方式和方面？

我们是否以恰当的方式在恰当的领域进行投资——我们是否拥有正确的“价值框架”来了解网络安全提升企业价值的具体方式和方面？

构筑未来网络安全的五大深度洞察

1 全面参与

据我们所知，高绩效企业更鼓励企业全员参与网络安全活动。虽然根据调查，高成熟度企业在遵循领先实践方面优于中低成熟度企业，但其实双方在企业参与度方面的差异最为明显。

领导层支持：高成熟度企业拥有由高级业务和IT领导人组成的治理机构来监督其网络安全计划的比例是低成熟度企业的近三倍，中等成熟度企业的近两倍（高、中、低成熟度企业的这一比例分别为60%、36%、22%）。

情景规划：同样，高成熟度企业实施企业和/或董事会层面的事件响应情景规划的比例是低成熟度企业的三倍，中等成熟度企业的两倍（高、中、低成熟度企业的这一比例分别为60%、30%、20%）。

2 聚焦数字化转型关键事项

高成熟度企业更为普遍地将网络安全视为推动数字化转型的关键。（图8）
聚焦数字化转型关键事项对于提升运营敏捷性和实现业务成果至关重要。但每一项均伴随着巨大的网络风险，高成熟度企业对此或更有体会。

例如，人工智能在助力实现企业网络安全战略和数字业务目标的同时，也可能带来数字技术普遍伴随的潜在网络风险。除本报告提出的领先实践外，我们近期发布的《企业人工智能应用现状分析报告》也强调了采取特定的风险缓解措施如何有助于取得更优成果，如降低成本和进入新市场。人工智能相关的风险是企业面临的严峻问题。该报告还发现，人工智能决策缺乏可解释性和透明性、数据隐私或同意管理不善、以及对人工智能系统的安全担忧等等都是影响企业的伦理道德风险。[5]

管理这些风险会对企业的人工智能应用产生重大影响。事实上，该报告还显示，50%的受访者提出人工智能相关风险管理是扩大人工智能项目规模的最大障碍之一。尽管如此，也仅有33%的受访者将人工智能风险管理纳入企业整体的风险管理范畴。然而，有33%的高安全价值产出的受访企业和29%的低产出的受访企业聘请外部供应商独立审核其人工智能系统。

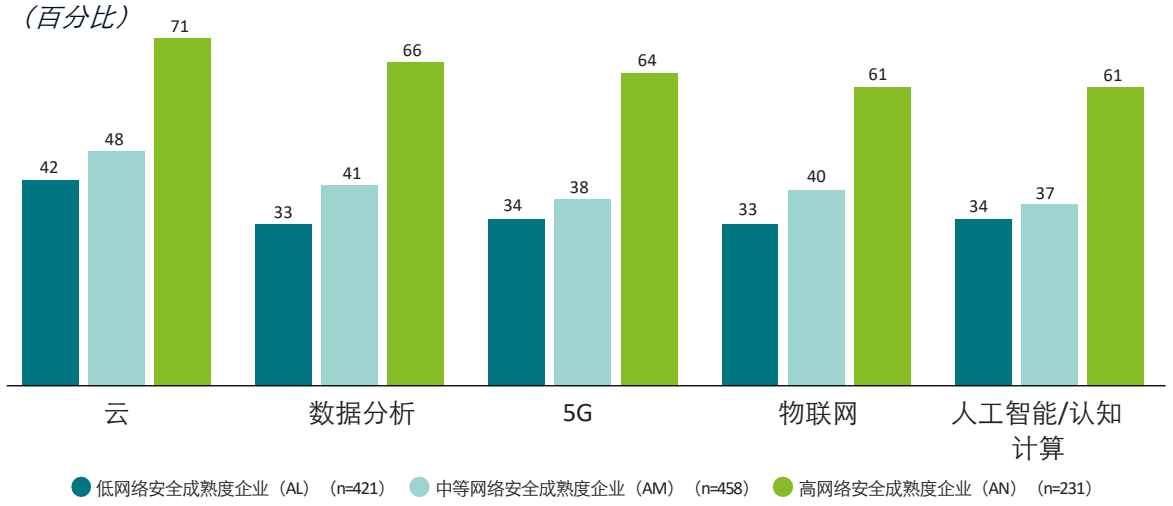
人工智能成果

“但总体而言，我们正不断提升（网络安全相关）知识和意识，并不断发掘量子计算、元宇宙以及人工智能的潜在价值，以及网络安全对业务发挥的巨大促进作用。”

——沙特NEOM项目首席信息安全官Mesfer Almesfer

图8：紧跟网络安全发展

不同成熟度企业看待网络安全对特定数字化转型举措的重要性



3 拥有强大的网络安全规划

事实证明，网络安全规划对于制定有效降低风险并推动商业价值的网络安全战略至关重要。本报告所评选出的高绩效企业似乎充分意识到了规划的重要性（图9）。

高网络安全成熟度企业更可能拥有强大的网络安全计划，具体包括：

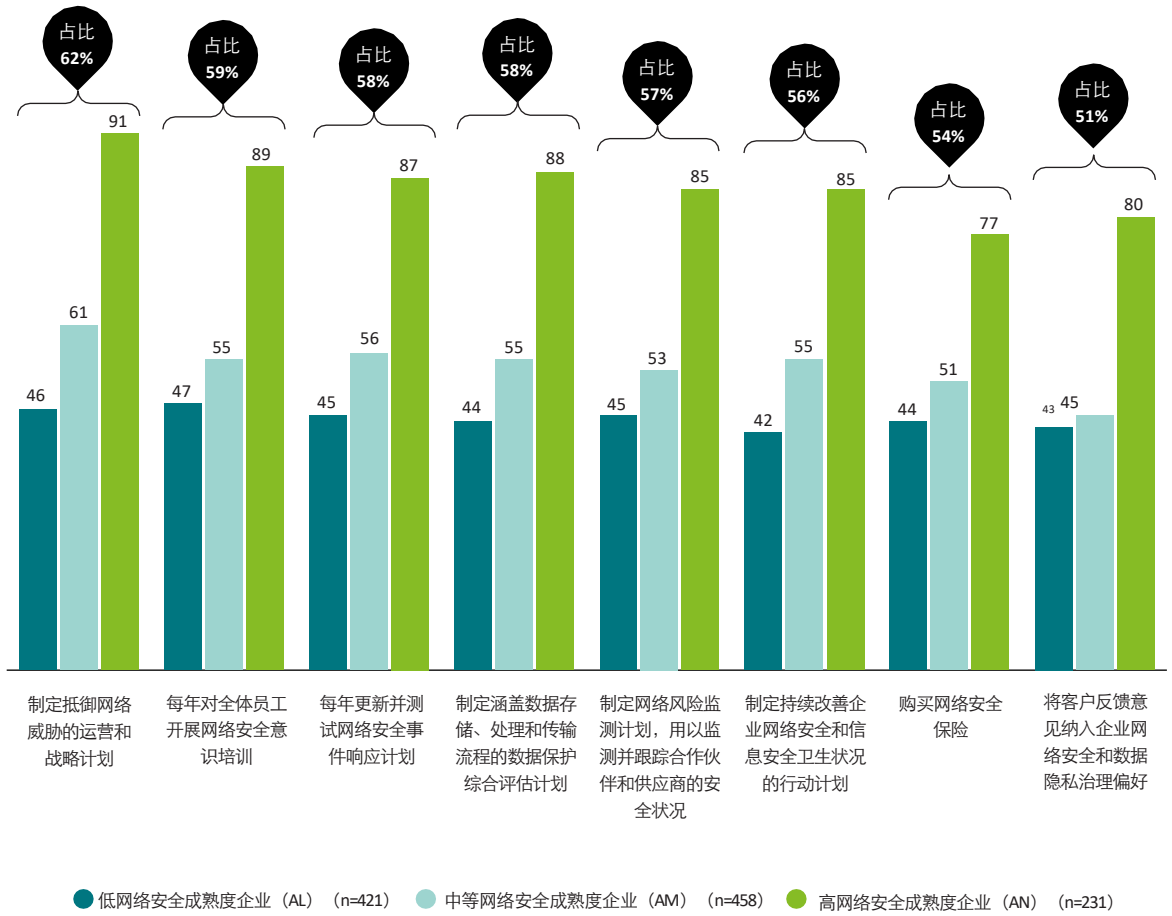
- 每年更新并测试**网络安全事件响应计划**（高成熟度企业的这一比例达87%）
- 制定抵御网络威胁的**运营和战略计划**（91%）
- 制定涵盖数据存储、处理和传输流程的**数据保护综合评估计划**（88%）

91%

的高成熟度企业通过制定运营和战略计划抵御网络威胁

图9：不同成熟度企业的网络安全规划现状

全面开展网络安全规划的企业*（百分比）*



4 招才育才

网络安全问题和活动最终都与人息息相关——无论是试图利用漏洞的攻击者，或是负责网络安全战略战术的决策者，抑或是负责数字业务流程和网络安全计划的一线员工。想要实现良好业绩，技能娴熟、经验丰富的网络安全人才不可或缺。招揽新型人才对于有效推动网络安全计划至关重要。例如，客户体验设计师可以提出网络安全计划相关见解，帮助识别交易过程、数据收集或隐私保护方面的潜在漏洞。

吸引和保留合适人才并非易事。网络安全从业者往往承受着巨大压力。正如本次调研中一位来自英国的金融界领袖指出，他被任命为“网络安全的高级分管领导”意味着网络风险实际上是由其与CISO首席信息安全官共担，而某些网络安全事件“可能会产生严重的个人后果”。这也是个有力佐证，对于网络安全已成为关乎业务实现的根本要务且不应再局限于单一职位或单一部门而言。

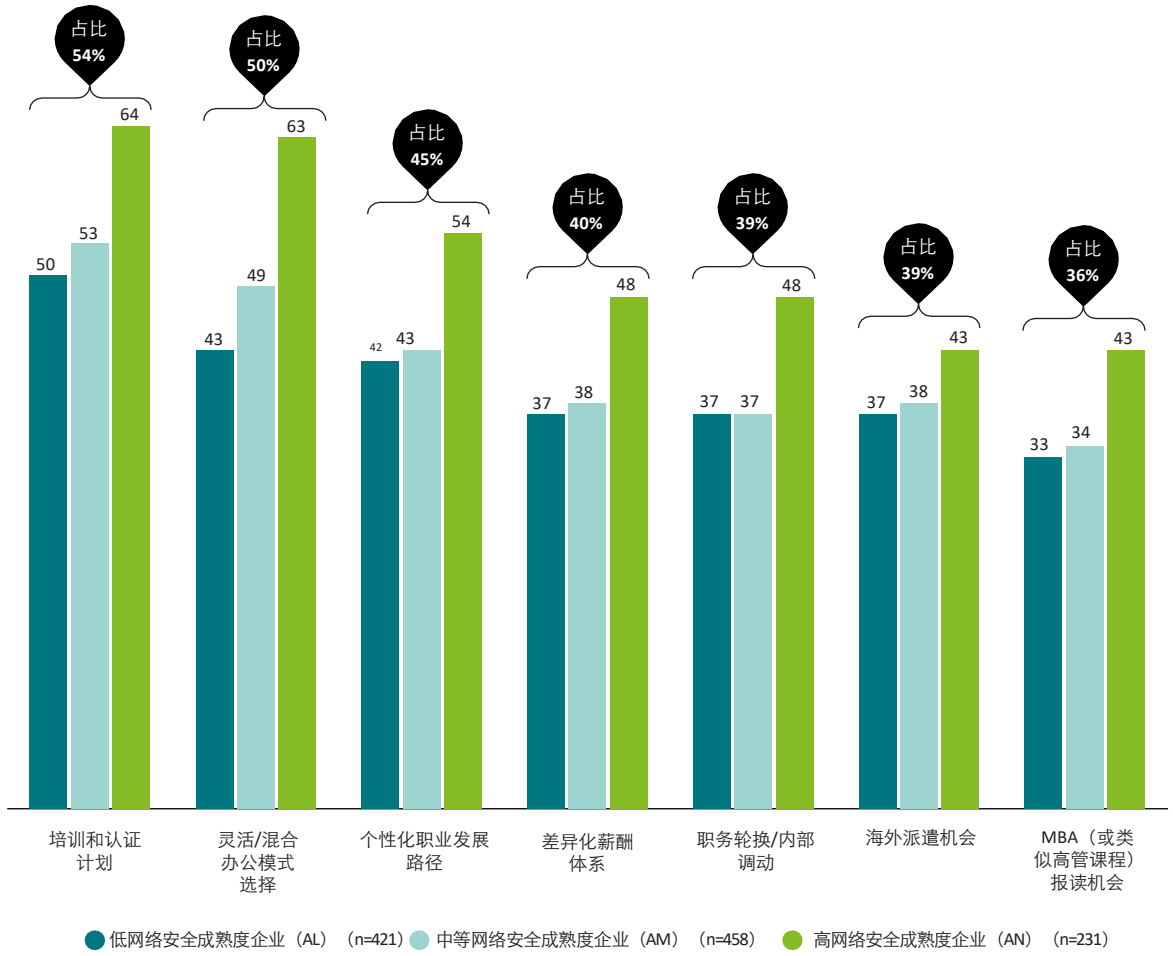
总体而言，高成熟度企业意识到经验丰富的人才对网络安全建设的重要性，并采取有效方法来保留有价值的人才。高成熟度企业更可能将缺乏资深网络安全专业人才视为管理网络安全的首要挑战（高、中、低网络安全成熟度企业这一比例分别为47%、38%、37%）。

对于高成熟度企业而言，解决人才挑战已成为实施强大网络安全计划的先决条件。随着企业更广泛而深入地参与网络安全活动，他们或将意识到其团队和能力已然触顶，并须引进更多具有先进和多样化技能的人才以支持更成熟的网络安全计划。

但低成熟度企业是否真的并未面临此等人才挑战——抑或只是不够重视掌握恰当技能的重要性？如果是后者，其应将人才招揽纳入企业优先事项，从而提升网络安全成熟度。（图10）

图10：企业如何吸引和保留人才

企业为吸引、保留和提升现有人才所采取的策略



5 构建包含多项工具和服务的多元生态系统

高成熟度企业敏锐意识到，想要引领网络安全的未来，仅凭一己之力无法做到。他们必须打造一个涵盖多项技术、能力和外部服务的可扩展生态系统，以构建面向未来并创造业务价值的网络安全能力。

与中低绩效企业相比，高绩效企业更有可能从第三方（图11）获得广泛产品和服务，包括：

- 应用程序安全
- 安全云
- 网络安全战略
- 数据和隐私保护
- 检测与响应
- 新兴科技（运营技术、5G、人工智能、量子计算）
- 身份识别与访问管理
- 基础设施安全
- 恢复与转型

行为转变

越来越多的企业使用自动化行为分析工具来检测和降低员工潜在的网络风险指标。在本次调研中，76%的受访者表示使用了此类工具，而在2021年调研中这一比例为53%。

工具和服务部署在提高网络安全就绪度的同时，也催生出对庞大生态系统的规划、管理和运营需求。与多家供应商合作解决复杂多变的问题，并作为集成环境的一部分运行、监控和升级网络防御能力，将对企业的网络安全管理工作提出重重挑战。

然而，与多家网络安全服务供应商合作也可能带来诸如数据泄露等新兴风险。在某些情况下，加强供应商的管理和监督或可有效降低此等风险。

预计未来两年网络安全服务供应商的数量将有所增加，同时也应简化和加强网络安全管理工作。企业或可考量另一种方法：与号召性机构（如行业组织）合作，深入了解有助于企业生态系统管理的技术发展和新兴实践。

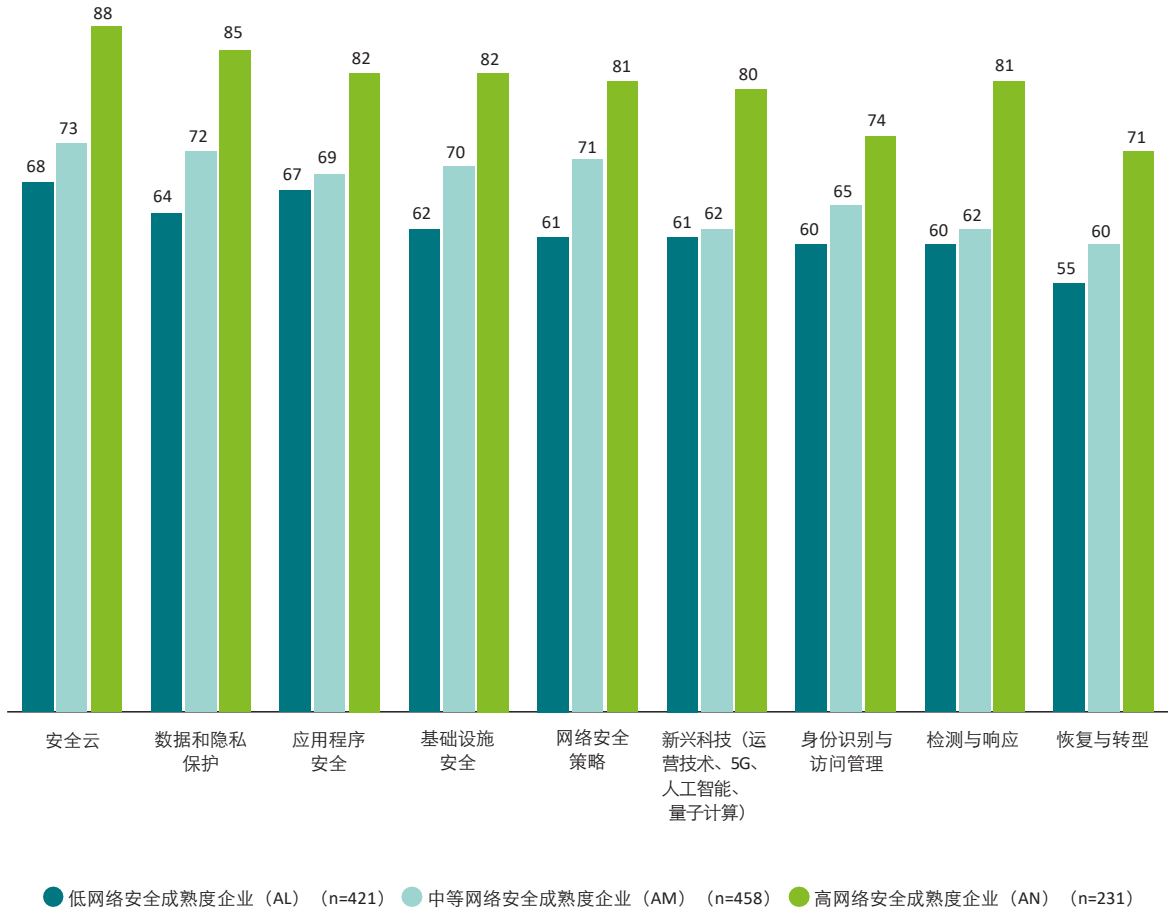
核心洞察

“仅凭自身之力构建网络安全战略实不明智，因为这样的战略不具扩展性，作用亦有限，最终结果多是纸上谈兵。我们与众多合作伙伴开展协作，旨在获得新想法和战略指导。”

—某汽车协会首席信息安全官

图11： 企业依赖第三方服务供应商

企业依赖第三方网络安全服务供应商提供以下领域服务



我们该何去何从?

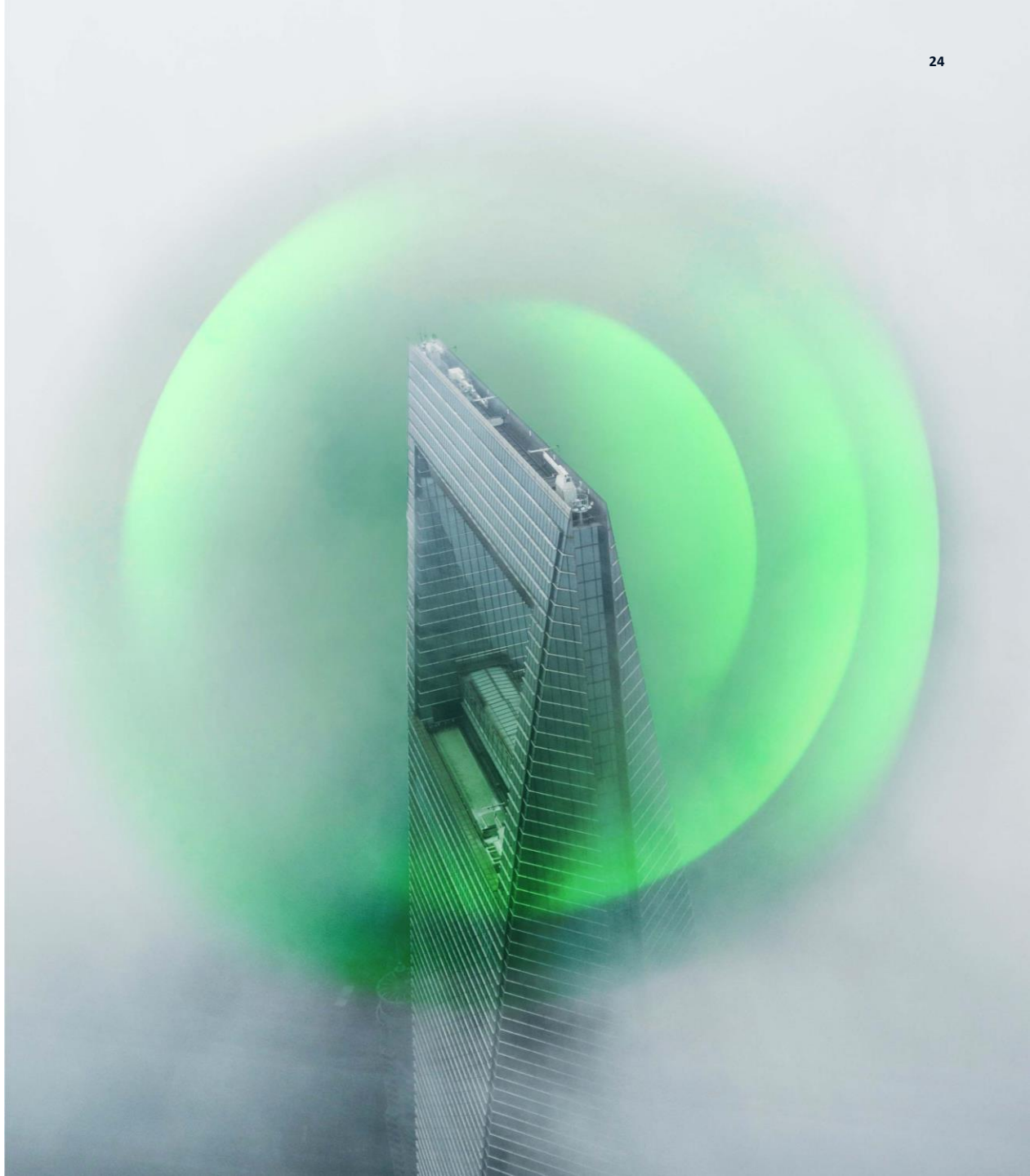
企业领导人应将网络安全作为推进业务目标不可或缺的工具，纳入其业务扩张和业务增长计划。

“发生事件后再考虑网络安全”的被动看法已经过时。对于任何企业而言，将强大的网络安全战略纳入业务计划，可进一步释放新兴技术的巨大潜力。新兴技术既可带来赋能未来商业模式的创新型解决方案，也将带来不可预知的网络安全挑战。您将如何在利用此等技术实现业务价值的同时，确保网络安全战略和投资与之同步?

对于低网络安全成熟度企业而言，零信任应成为新技术采用之基础。零信任策略旨在从安全架构中移除默认信任假设，并对每个行动、用户和设备进行验证，从而构建更强大、更具韧性的安全态势。零信任策略还可为企业终端用户带来一项巨大助益：无缝访问开展高效工作所需的工具和数据。

“对于像我们这样拥有大型IT架构的企业而言，向零信任转型势必困难重重。我们必须在管理日益庞杂的合作伙伴生态系统时，紧跟业务需求节奏进行转型，他们期望通过更广泛的设备互联实现多元协作，这些都要安全地开展。”

——壳牌集团首席信息官/首席信息安全官Allan Cockriel



“我们将部署更多样化的数字解决方案，包括诸如人工智能和超级计算的业务特定型或数据密集型解决方案，这需要我们持续更新自身网络环境，使之得到有效保护并符合监管要求。”

——巴斯夫集团数据保护官Charlie Huang

谈及创新，企业应首先制定相关战略，然后从网络安全角度慎重考量并选择支持性技术。例如考量数据服务和平台的使用如何与企业目标相一致，并提高企业自身的信任构筑能力，从而应对风险和挑战？从这些问题出发，运用恰当的解决方案解决对应的需求。

展望未来

了解新技术带来的风险和机遇是有效应对不断变化的威胁形势的方式之一。没有企业愿意看到自身因网络安全水平不足而被迫赶追快速发展的技术趋势。企业的技术变革准备越是不足，其网络风险管理能力越是低下。

典型示例之一便是5G，随着重要性的日益凸显，5G首次跻身今年数字化转型五大要务之列。5G在支持远程医疗、制造业的资产追踪和用于高级培训的增强现实等新用例的同时，也增大了网络威胁攻击面。自始便设计和嵌入网络安全对于5G的采用至关重要，但这也将带来巨大的复杂性。

同时，人工智能仍在数字化转型五大要务之列，该技术可助力企业应对网络安全在内的多重挑战。网络人工智能可以成为一种力量的倍增器，帮助帮助企业快速修复安全漏洞，使安全团队不仅能够比攻击者更快做出反应，而且能够预判攻击行为并提前作出反应。人工智能和自动化还可减轻安全运营中心分析师的负担，助其担任更具战略性和挑战性的角色。

越早为量子计算（4%的受访者将其列为未来几年的数字化转型优先事项之一）等前沿技术的采用做好准备越好。尽管量子计算可为企业释放巨大的潜在计算能力，但它也可能成为网络攻击者手中的“利刃”，并要求企业须就其采用做好充分准备。

设计即安全（Secure-By-design）

“事实上，我们正投资于‘设计即安全’项目，以确保安全成为我们价值主张的构成要素之一。我们在软件和产品生命周期的策略、工具和控制方面进行投资，以确保我们研发出伟大且安全的技术。这也是我们的客户所期待的。”

——壳牌集团首席信息官/首席信息安全官Allan Cockriel

勇往直前

网络安全发展与企业未来发展紧密相连。企业将网络安全考量事项、规划和行动纳入业务计划与否将直接决定该等计划的成败。

换句话说：网络安全是关乎企业发展战略的根本性议题。业无信则不兴，而网络安全正是实现和维护数字信任的基石。随着企业持续推进数字化转型，制定有效的网络安全策略将有助于企业构建适宜的数字生态系统，从而实现业务成果。

品牌声誉、客户信任和忠诚度、运营稳定性以及营收增长，这一切均取决于企业网络安全计划的制定和执行情况，即企业网络安全基础的高低。企业在开启全新上云之旅、开发新产品和服务、采用第三方服务或向员工提供新工具时，将网络安全作为首要考量事项至关重要。网络安全的重要性也将贯穿于所有数字化转型要务，如对洞察、平台、互联互通、有效体验和完整性的需求。

蓄势待发

网络安全计划关乎企业的未来发展以及目标实现。无论企业经营现状和未来目标如何，制定网络安全计划有助于企业从一开始就清楚地了解未来发展机遇与挑战。

致谢

谨此致谢Ian Blatchford、Scott Buzik、Luca Covolo、Deborah Elder、Jaya Gopalan、Jeremy Guterl、Matthew Holt、Dan Konigsburg、Daphne Lucas、 Diana Kearns-Manolatos、Emily Mossburg、Mike Nash、Kelly Nelson、Jud Payne、Sean Peasley、Ashley Reichheld、Heather Saxon、Daniel Soo、Scott Tillett、Niels van de Vorle、Marius von Spreti和Emily Werner对本报告提供的专业洞察和协助。

德勤中国风险咨询网络安全服务领导人

薛梓源
德勤中国网络安全及战略风险事业群
主管合伙人
电话: +86 10 85207315
电邮: tonxue@deloitte.com.cn

冯晔
德勤中国网络安全服务
主管合伙人
电话: +86 21 61411575
电邮: stefeng@deloitte.com.cn

东区

张震
德勤中国网络安全服务合伙人
电话: +86 21 61411505
电邮: zhzhang@deloitte.com.cn

江玮
德勤中国网络安全服务合伙人
电话: +86 21 23127088
电邮: davidjiang@deloitte.com.cn

阎光
德勤中国网络安全服务合伙人
电话: +86 21 23166282
电邮: alexyan@deloitte.com.cn

金洁
德勤中国网络安全服务合伙人
电话: +86 21 23166315
电邮: jerjin@deloitte.com.cn

北区

肖腾飞
德勤中国网络安全服务合伙人
电话: +86 10 85125858
电邮: frankxiao@deloitte.com.cn

何晓明
德勤中国网络安全服务合伙人
电话: +86 10 85125312
电邮: the@deloitte.com.cn

林松祥
德勤中国网络安全服务合伙人
电话: +86 10 85124888
电邮: chaphylin@deloitte.com.cn

南区大陆

何微
德勤中国网络安全服务合伙人
电话: +86 75 533538697
电邮: vhe@deloitte.com.cn

邓娜
德勤中国网络安全服务合伙人
电话: +86 75 533538151
电邮: tindeng@deloitte.com.cn

西区

马红杰
德勤中国网络安全服务合伙人
电话: +86 21 33138528
电邮: jacma@deloitte.com.cn

南区香港和澳门

Everson, Phill
德勤中国网络安全服务合伙人
电话: +85 22 8521222
电邮: philleverson@deloitte.com.hk

林普毅
德勤中国网络安全服务合伙人
电话: +85 22 1095353
电邮: bradlin@deloitte.com.hk

王凯民
德勤中国网络安全服务合伙人
电话: +85 22 2387908
电邮: harrywang@deloitte.com.hk

鄭若琳
德勤中国网络安全服务合伙人
电话: +85 22 2387119
电邮: eicheng@deloitte.com.hk

尾注

1. 德勤《2021网络安全前瞻调研报告》
2. Closing the cloud strategy, technology, and innovation gap. Deloitte US Future of Cloud Survey Report, 2022.
3. Future of Digital Trust: Driving forces, trends and their implications on our digital tomorrow. Deloitte. 2021.
4. The Four Factors of Trust: How Organization Can Earn Lifelong Loyalty.
5. 德勤《企业人工智能应用现状分析报告（第五版）》，2022年10月
6. Take 5: 5G cybersecurity, Part of Deloitte's 'Take 5 on 5G' article series.
7. 德勤《2022技术趋势》
8. Quantum Cyber Readiness Deloitte's perspective on transitioning to a quantum secure economy

Deloitte.

关于德勤

德勤中国是一家立足本土、连接全球的综合性专业服务机构，由德勤中国的合伙人共同拥有，始终服务于中国改革开放和经济建设的前沿。我们的办公室遍布中国30个城市，现有超过2万名专业人才，向客户提供审计及鉴证、管理咨询、财务咨询、风险咨询、税务与商务咨询等全球领先的一站式专业服务。

我们诚信为本，坚守质量，勇于创新，以卓越的专业能力、丰富的行业洞察和智慧的技术解决方案，助力各行各业的客户与合作伙伴把握机遇，应对挑战，实现世界一流的高质量发展目标。

德勤品牌始于1845年，其中文名称“德勤”于1978年起用，寓意“敬德修业，业精于勤”。德勤专业网络的成员机构遍布150多个国家或地区，以“因我不同，成就不凡”为宗旨，为资本市场增强公众信任，为客户转型升级赋能，为人才激活迎接未来的能力，为更繁荣的经济、更公平的社会和可持续的世界而开拓前行。

Deloitte（“德勤”）泛指一家或多家德勤有限公司，以及其全球成员所网络和它们的关联机构（统称为“德勤组织”）。德勤有限公司（又称“德勤全球”）及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体，相互之间不因第三方而承担任何责任或约束对方。德勤有限公司及其每一家成员所和它们的关联机构仅对自身行为承担责任，而对相互的行为不承担任何法律责任。德勤有限公司并不向客户提供服务。

德勤亚太有限公司（即一家担保有限公司）是德勤有限公司的成员所。德勤亚太有限公司的每一家成员及其关联机构均为具有独立法律地位的法律实体，在亚太地区超过100个城市提供专业服务。

请参阅 http://www.deloitte.com/cn/about 了解更多信息。

Designed by CoRe Creative Services. RITM1268180.