Deloitte.

德勤

全球网络安全前瞻调研报告 第4版

网络安全的前景

增强网络安全韧性
提升变革价值

筑牢网络安全打造价值引擎

网络安全需求瞬息万变。新兴网络安全威胁、前沿技术以及业务需求的不断演进，正持续重塑各行各业组织的战略优先级和可能性。

精准理解并预测网络安全未来趋势是一项长期战略要务，它不仅可以让我们通过前瞻性思维敏锐地洞察和识别新兴风险，同时也将深度挖掘其中蕴藏的无限价值潜力。

德勤第四版《全球网络安全前瞻调研》报告正式发布，为我们勾绘了一幅更加清晰、更加全面的网络安全蓝图。调研显示，网络安全与商业价值之间的关联持续增强。在推动技术驱动项目和实现业务成果的过程中，网络安全扮演着更加举足轻重的角色。同时，随着企业对网络安全的重视程度与日俱增，包括首席信息安全官（CISO）在内C级高管的角色正发生转变，他们的影响力和职责范围也在不断扩大。

我们很高兴与您分享本次调研的主要发现，并邀您一同探究相关成果。接下来的内容中，我们结合德勤在全球网络安全领域的丰富经验和深刻理解，为您呈现一系列由数据驱动的专业洞察。此外，报告还梳理了受访者的直接反馈和观点，旨在提供更加全面的多元化视角。诚邀您阅览本报告，如需进一步探讨相关内容，欢迎随时与我们联系。

Emily Mossburg
德勤全球网络安全服务主管合伙人

报告内容概览

网络安全战略转型的新时代

专注于商业价值和韧性

全球范围内的组织在面对持续的业务复杂性和变化，以及各种新兴威胁和风险的同时，网络安全与商业价值的紧密联系始终如一。对于各行各业的组织而言，网络安全始终是其持续实现其所期望成果的核心所在。

德勤发布的《全球网络安全前瞻调研》第四版，对近1,200位全球各行业领导者进行了深度访谈，聚焦于他们对网络安全威胁、企业活动及未来趋势的看法。受访者包括企业高管及IT、安全、风险和业务领域的其他高层管理者。报告深刻揭示了网络安全与企业影响的紧密关联。

对商业价值导向的聚焦日益增强

在我们先前的报告，即第三版调查中，德勤深刻洞察到网络安全正逐步演变为企业的独立功能领域，它超越了传统的IT范畴，成为推动实现业务成果的关键组成部分。

在本次的第四版调查中，我们观察到，网络安全战略不仅对于释放更大的商业价值至关重要，而且网络安全实践已深度融入技术转型实践。同时，网络安全领导层的声音，尤其是首席信息安全官（CISO）的影响力显著提升，同时对网络安全有深入洞察的企业高层也越来越多。

尽管对网络安全的重视程度持续提升，但仅有约半数（52%）的受访者对企业高层（C-suite）和董事会在网络安全领域的驾驭能力充满信心，认为他们能够妥善应对网络安全挑战。尤其在那些关注网络安全的企业高层（C-suite）受访者中，仅有34%的人表示非常有信心，这暗示他们对自己的能力持有较低的自信度，甚至低于外界的预期。

然而，当我们聚焦于网络安全成熟度分类为高（以德勤标准）的组织时，我们发现了两个关键点：网络安全在高层得到了认可，且组织的网络安全成熟度与其在应对网络安全问题时的信心之间存在显著的正相关性。实际上，在高网络安全成熟度的组织中，对企业高层（C-suite）和董事会在网络安全领域驾驭能力的信心跃升至82%，相比之下，网络安全成熟度为中和低的组织中，这一比例分别为52%和39%。

调查结果表明，平均而言，86%的受访者正在中等或大规模地采取行动，以增强网络安全策略和行动，将网络安全视为企业不可或缺的组成部分。同时，平均而言，85%的受访者预计能够中等或大规模地实现其期望的业务成果。这凸显了网络安全在推动实施成功的策略中，起到核心作用，但并非所有组织都能同样地从中获益。

组织的网络安全成熟度越高，其潜在影响越大。调查发现，在具有较高网络安全成熟度的组织中，预期业务将取得积极成果的受访者数量几乎是其同行的两倍。这些高网络安全成熟度组织如何看待网络安全，以及他们采取的行动，为其他寻求提升自身网络安全成熟度的组织提供了借鉴和潜在路径。

更高的网络安全成熟度并不能使组织完全免受威胁，但它能增强组织在威胁发生时的**韧性**，从而确保关键业务的持续运行。

网络安全成熟型组织准备更加充分且更具韧性

在本期的调查中，德勤基于多个因素识别了具有高网络安全成熟度的组织。与上一期调查一样，我们评估了这些组织的网络安全战略规划水平、特定的网络安全活动，以及董事会层面的网络安全参与度。根据这些因素，我们发现，在这些网络安全成熟度更高的组织中，网络安全在支持和塑造技术驱动项目中的影响力增长了三个百分点。

然而，鉴于人工智能（AI）技术的迅速发展，跨国组织正面临更加复杂的攻击。与此同时，投资AI驱动的工具和网络安全解决方案的机会也应运而生。因此，我们更新了德勤的网络安全成熟度指数，以纳入受访者在网络安全计划中使用AI能力的程度（见第25页的“网络安全成熟度”）。

在这些高网络安全成熟度的组织中，首席信息安全官（CISO）和其他网络安全领导者作为专家受到邀请，帮助指导针对云驱动的业务计划、AI赋能活动、企业资源规划（ERP）现代化以及其他数字转型优先事项的投资。换句话说，网络安全在帮助企业获得技术能力方面的资金中发挥着重要作用。对网络安全的高度重视也意味着首席信息安全官（CISO）更多地参与了与数字转型相关的战略对话。

这些高网络安全成熟度的组织实施了一系列的基础的网络安全行动，如制定战略和运行计划、监控网络风险等，最值得注意的是，组织在遭受网络攻击后能够迅速恢复的能力。更高的网络安全成熟度并不能使这些组织完全免受威胁，但它使它们在威胁发生时更具韧性，从而确保关键业务的连续性。

与总体调查受访者相比，高网络安全成熟度的组织预计平均能多实现27个百分点的业务成果。尽管他们报告在过去一年中遭受了11次或更多的网络攻击（比总体受访者高出8个百分点），并也承担了负面后果（平均比总体受访者高出7个百分点），但他们仍保持了这些预期。这可能是因为高网络安全成熟度的组织更善于识别到网络攻击，因此报告的攻击次数更多，并不一定意味着他们遭受的攻击就更多。

高网络安全成熟度的组织领导者们深刻认识到，关键在于为不可避免的网络攻击做好响应与恢复准备，确保业务迅速恢复运行，持续为客户提供服务。

随着组织韧性增强，组织准备应对或希望避免的挑战有哪些变化？与上一版调查相比，对技术完整性（即系统和数据的可靠性、准确性和可用性）丧失信心，已跃升至网络安全事件或数据泄露带来的负面影响之首，这在组织加速数字化转型的背景下变得日益重要。

运营中断，包括供应链或合作伙伴生态系统的中断，依然高居列表第二位，凸显了在合作伙伴和基础设施中保持业务连续性的重要性。然而，也出现了一个显著的变化，因为在上一版调查中，这是首要的担忧。声誉损失则上升至第三位（图1）。

组织今天采取的措施应聚焦于如何通过网络安全投资优化、保存、保护和创造组织价值。这包括通过确保数字产品和基础设施的数据安全和完整性，为未来的增长奠定坚实的网络安全实践基础。这一基础还应融入具备响应能力的基础设施和数字生态系统的基本要素，以促进未来的增长和业务韧性。本版调查显示出一个明显的趋势，即网络安全计划和首席信息安全官（CISO）在所有这些价值流中通过更加集成的技术转型策略获得更大的战略影响力，尤其是在最成熟的网络安全组织中。

有效的网络安全策略应当不局限于传统的事件响应，而应深入探讨企业如何将网络风险、安全与信任融入其整体战略的核心。采取全面且以业务为导向的视角，使你能够将更广泛的业务目标与运营需求相连接。这种方法确保网络安全不仅是被动的应对措施，而是成为组织战略、技术和运营框架中主动且不可或缺的组成部分。此外，德勤的研究表明，市场上最成熟的网络安全组织正通过类似以业务为导向的方法获得显著价值。

组织痛点所在：（图1）

网络安全事件和数据泄露正给调查受访者带来以下主要的负面影响。

由网络安全事件和数据泄露引发的负面后果	第三版（排名）	第三版（占比）	第四版（排名）	第四版（占比）
对技术完整性的信心丧失	6	55%	1	66%
运营中断 *（包括供应链或合作伙伴生态系统）*	1	58%	2	66%
声誉损失	4	55%	3	65%
人才招聘/留用的负面影响	7	54%	4	64%
收入损失	2	56%	5	64%
客户信任丧失/品牌负面影响	3	56%	6	63%
知识产权受到侵害	8	54%	7	63%
监管罚款	10	52%	8	63%
股价下跌	9	52%	9	63%
战略计划的资金削减	5	55%	10	63%

> “我们的威胁面正在迅速扩大。随着我们使用新技术连接工厂，新的风险也随之出现。一旦我们将供应商的机器人与制造商的维护服务连接起来，或者向生产线组件推送软件包，情况就会变得复杂得多。”
>
> ——Kevin Tierney，通用汽车首席网络安全官

我们是如何得出这些见解的

德勤还对来自不同行业和地区的高级网络安全决策者进行了深入访谈，以获取更详细的信息洞察，并帮助验证我们的观察结果。我们的研究方法涵盖了与网络安全未来相关的每一个方面，从战略到战术，从文化到技术实施。

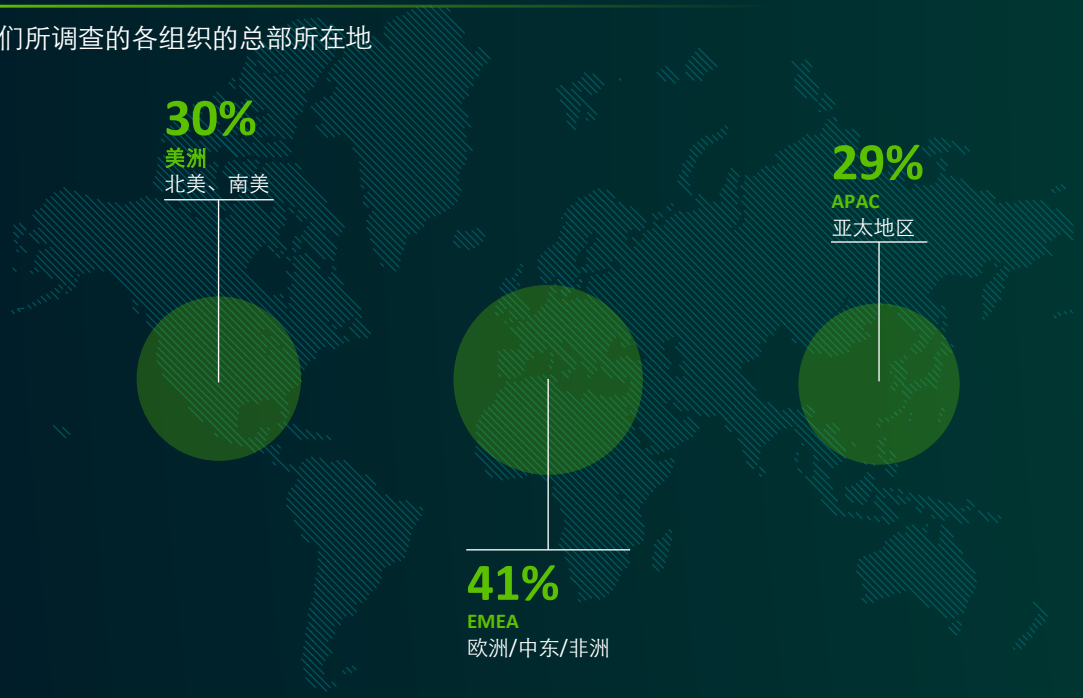
本次研究的核心，我们致力于探索自上一份报告发布以来，网络安全领域发生的变化，同时采用前瞻性的视角，以期更清晰地描绘出网络安全的未来图景。我们还力求更深入地了解当今企业高层（C-suite）对网络安全的敏锐度。在整个调查过程中，我们力求揭示洞察，以更好地理解企业正在经历的与网络安全相关活动给企业带来的商业价值和影响，以及领先企业为增加价值而采取的特别行动。

研究背后

德勤根据当今商业与技术环境的复杂性，设计了《全球网络安全前瞻调研》报告的第四版，重点关注那些已经认识到网络安全重要性，但在实际中却不知如何发挥其价值的企业领导者的需求。

德勤的这项研究基于对近1,200名网络安全决策者的调查，这些决策者至少在董事级别，包括企业高层（C-suite）及其直级下属，涵盖了不同的业务和IT职能。调查反映的数据来自43个国家和六个行业，且拥有至少1,000名员工和每年5亿美元收入的组织。

我们所调查的各组织的总部所在地



网络安全影响
战略价值

努力扩大业务影响

展望网络安全的未来，通往网络安全成熟度的路径正变得日益清晰。那些沿着这条路径前行的组织，将网络安全风险策略、安全实践和信任构建措施深度融入其业务与技术转型中，这一切得益于具备高度网络安全意识的企业高层（C-suite）和具有重大影响力的首席信息安全官（CISO）的支持和推动。这些组织预期会取得显著的成功，从而在快速变化的数字环境中，更有效地推动业务转型。

随着组织不断的提升网络安全成熟度，它们可以在业务活动、技术运营中优先考虑网络安全事项并与得到管理层支持，从而与同行拉开差距。通过优先考虑这些网络安全与业务活动和技术运营的关联度，它们将能够更有效地实现我们在上一版调查中看到的优先战略成果。这种方法不仅加强了它们的网络韧性，还确保了网络安全工作与整体业务目标的协调一致，确保它们能够以安全和可持续的方式实现战略目标。

在本报告中，我们将基于调查数据、网络安全成熟度指数以及全球领导者们的见解，深入探讨高阶洞察。我们将展示那些表现卓越的组织是如何在网络安全领域脱颖而出的，并为全球的网络安全从业人士提供指导，帮助他们提升其工作的网络安全的成熟度。

我们将探讨如何做到..

1. 网络安全仍然是战略业务价值的关键要素，而且关注度正在加强。
2. 随着企业高层（C-suite）对网络安全的认识不断提高，首席信息安全官（CISO）的影响力正在与日俱增。
3. 网络安全与技术驱动的项目和数字化业务转型深度融合。
4. 具有更高网络安全成熟度的组织对其网络安全实践和投资更有信心，并从中获得了更大的收益。

网络安全仍然是战略业务价值的关键要素——且关注度正在加强

在当今深度互联的数字环境中，网络安全的基础重要性毋庸置疑。企业可以通过各种活动/行动和战略手段来加强网络安全的准备程度，从而提高业务价值。

采取行动仅为第一步

大多数受访者都认真审视网络安全行动的必要性，其中86%的受访者在中等或较大程度上实施了具体活动/行动，以提高网络安全。这种水平的行动表明，绝大多数组织都了解开展这些活动和实施强有力的网络安全计划的必要性。这也表明，随着他们需要开展的网络安全活动清单不断增加，他们正在保持网络安全水平的同步提升。

这些受访者正在集中精力开展各种网络安全管理活动，包括但不限于：降低风险、加强网络安全控制、改进事件响应、提高员工意识以及有策略的实施网络安全计划。

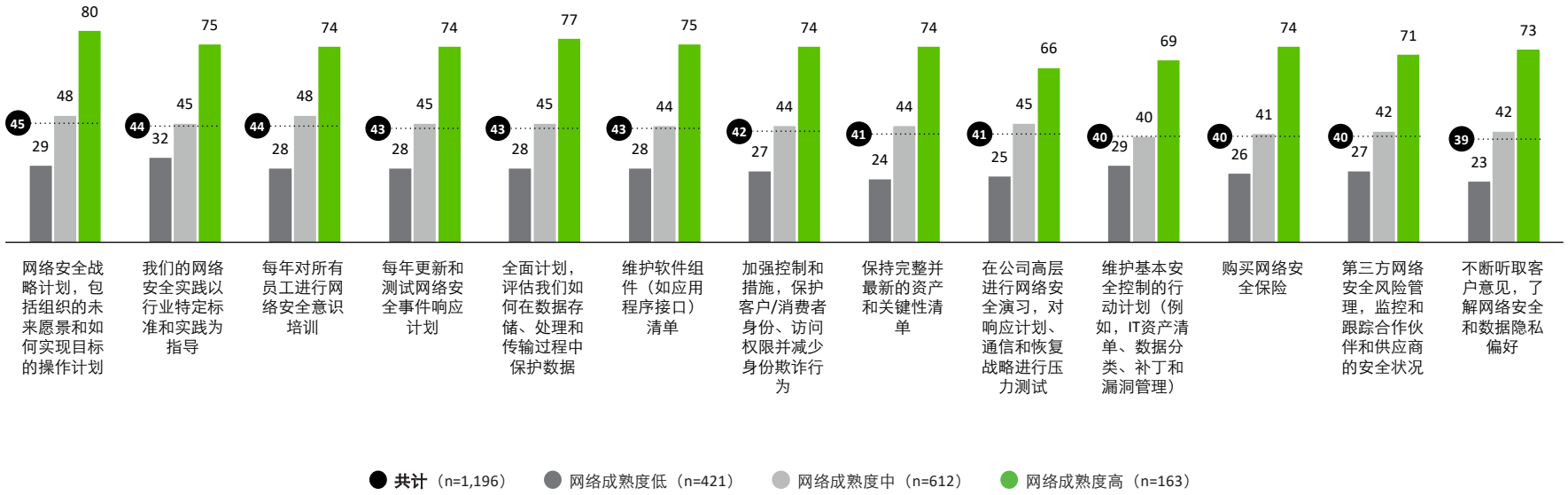
当我们从网络成熟度的角度对这些活动进行观察，我们会发现，与网络成熟度较低的组织相比，网络成熟度高的组织采取这些行动的程度更高（图2，另见网络成熟度，第25页）。

> “这实际上是关于做好基础工作，并持续提升这些基础工作的成熟度，每天都保持卓越，持之以恒。比如基础控制、资产管理、漏洞管理等。在这些方面，你必须达到几乎无需思考就能做好的程度，它们必须自然而然地发生。”
>
> ——来自生命科学与医疗保健组织的某位CISO

网络安全活动及其与成熟度的关系（图2）

与网络成熟度较低的组织相比，网络成熟度高的组织参与这些关键网络安全活动的程度更高。

（百分比）

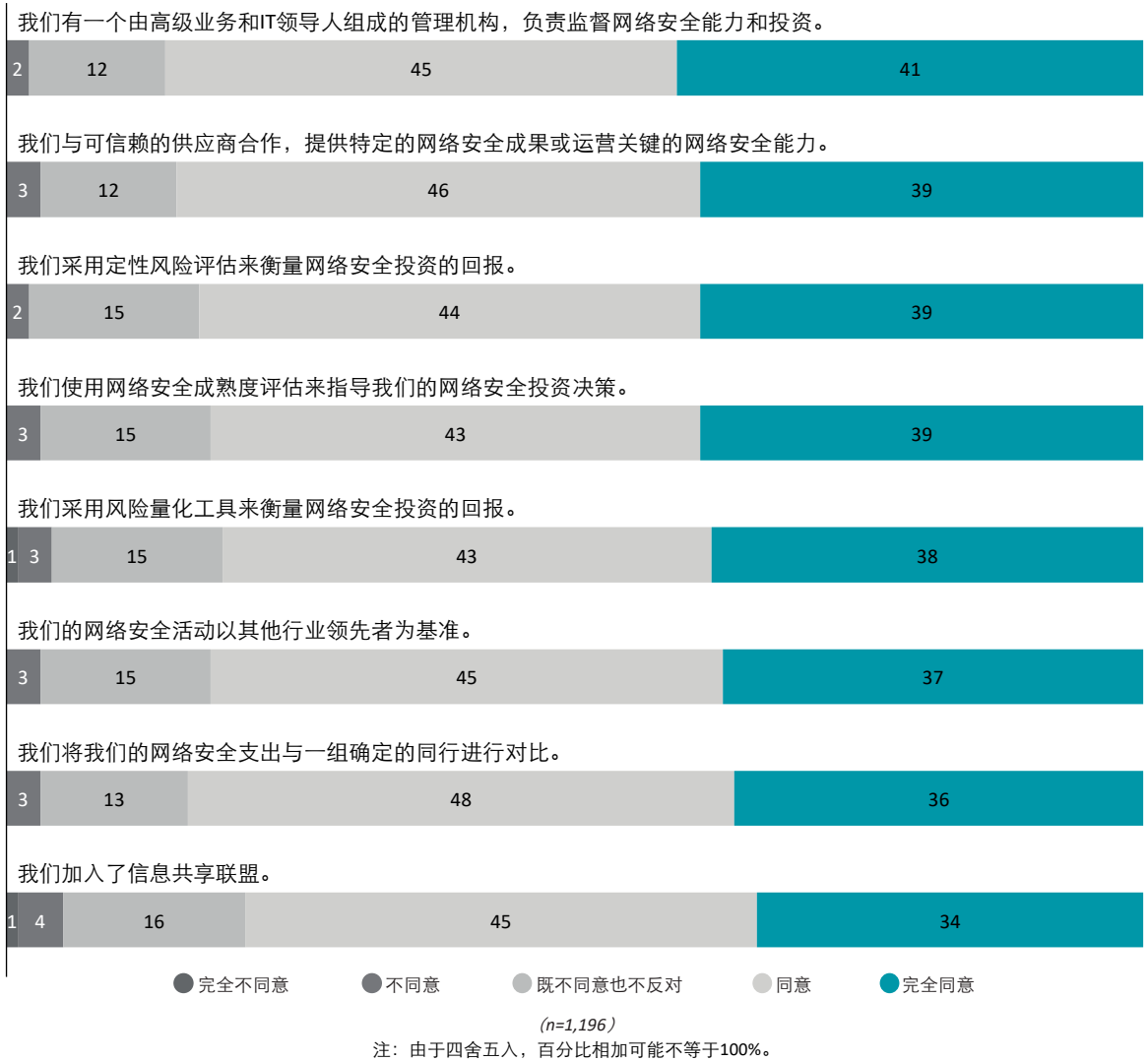


86%

受访者报告在中等或较大程度上开展了具体活动/行动，以加强网络安全。

制定网络安全战略计划（图3）

受访者表示正在采取的加强和改善网络安全的具体战略措施。



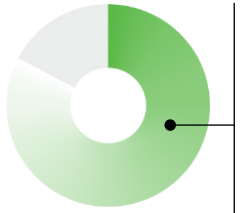
（n=1,196）

注：由于四舍五入，百分比相加可能不等于100%。

在战略指导下，网络安全的执行在整个业务中更加一体化

绝大多数组织还在采取一系列战略性网络安全行动，包括：制定基准和衡量标准、与可信赖的供应商合作、加入信息共享联盟以及建立由高级业务和IT领导人组成的管理机构，以监督网络安全能力和投资。

总体而言，83%的受访者同意或完全同意这些措施是其整体网络安全战略的组成部分。这种共识的程度表明，网络安全战略将继续融入业务中。



83%

受访者总体上同意这些措施是其整体网络安全战略的组成部分。

面对日益增长的网络安全威胁加大网络安全投资，全球超过半数的受访者（57%）预计在未来12至24个月内增加其网络安全预算。同时，58%的受访者表示，他们预期开始将网络安全支出与其它项目的预算进行整合，例如数字化转型计划、IT项目和云投资。这种投资水平和预算整合凸显了网络安全活动与企业运营日益交织的特性。这也强调了一个现实，即网络安全资金往往被视为零和游戏，在转型项目中，网络安全常常被忽视，以在零和环境中节省成本。

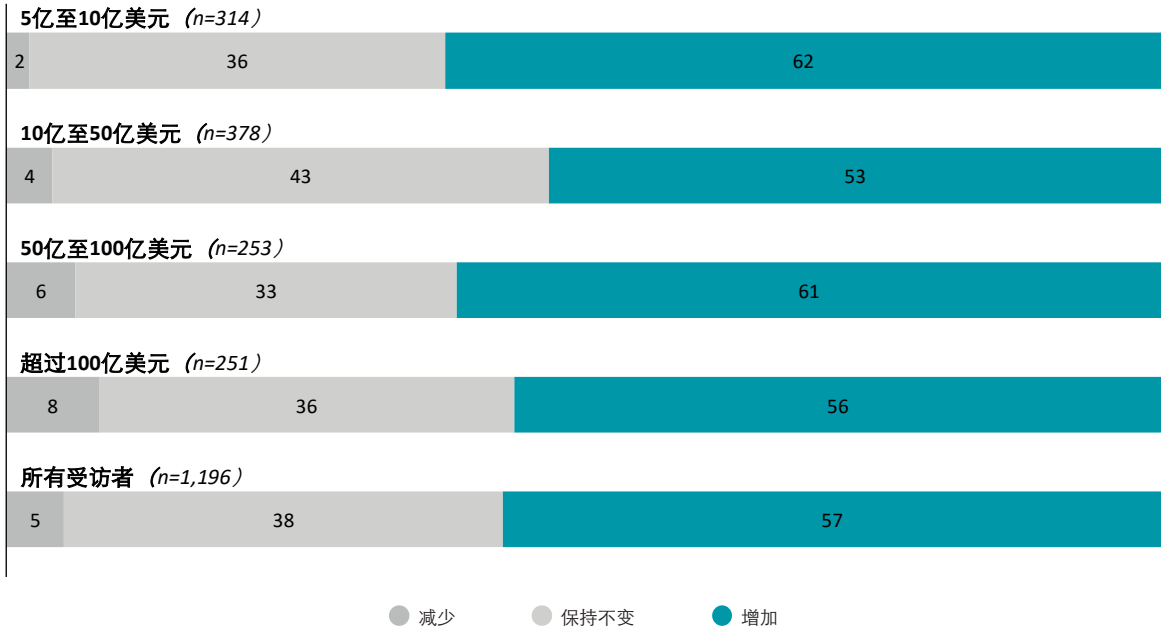
持续优先考虑网络安全，并在业务和技术运营以及领导层之间建立网络安全连接能力，对于组织脱颖而出并成功实现战略成果至关重要。一个网络安全成熟的组织明白，网络安全不仅仅是一个信息技术问题，而是一个业务成功的关键所在，需要在组织的所有职能和层级中进行整合。通过培养这种强大的网络安全连接能力，组织可以增强与网络安全相关的协作、信息共享和决策制定。

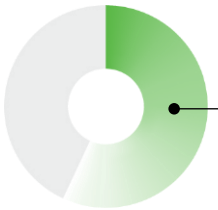
这种方法使领导者能够根据业务目标做出明智的战略决策，并有效降低网络安全风险。最终，那些优先考虑网络安全并构建强大网络安全连接能力的组织，即将网络安全纳入组织职能和领导角色的组织，能够在日益数字化的世界中更好地保护其资产、声誉和整体韧性。

支出在增加（图4）

57%的受访者预计在未来12-24个月内增加网络安全预算。

（单位：美元和百分比）





57%

受访者预计在未来12-24个月内增加网络安全预算。

“由于公司的规模、拥有的数据类型、在线业务和供应链实践等因素各不相同，因此它们的威胁特征也各不相同。每家公司都必须制定强有力的威胁情报战略，包括了解谁在关注他们、为什么，以及他们是如何运作的。了解潜在攻击者的动机和策略对于制定有效的安全措施至关重要。”

——Gary Harbison，强生公司首席信息安全官

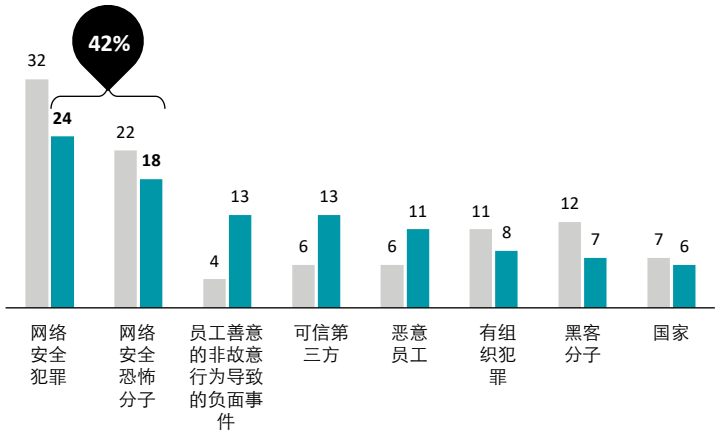
我们发现，平均而言，受访者每年在IT方面的总体支出在1.47亿美元到2.66亿美元之间。其中，19%（3,900万美元）用于网络安全相关活动，而受访者预计在未来12至24个月内，这一比例将增加3%。

正在突破防御的威胁（图5）

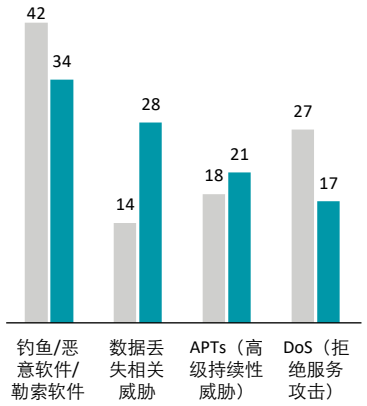
网络安全漏洞的来源，以及有多少组织正在遭遇这些漏洞。

（百分比，第三版Vs第四版）

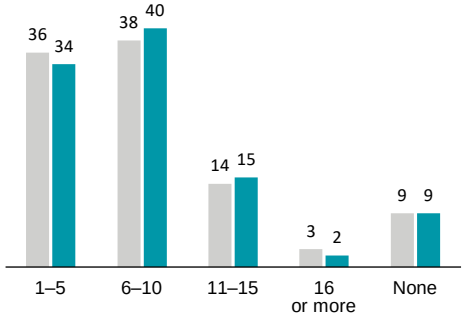
攻击者/来源



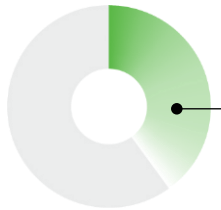
工具/技术



漏洞事件次数



第3版（n=1,110）　第4版（n=1,196人）



40%

受访者表示，在过去一年中公开报告了六至十起网络安全漏洞事件。

攻击现实日益严峻，包括与生成式人工智能（GenAI）相关的新威胁和网络风险

随着各组织所面临的网络威胁日益增多且多样化，预计投资也将随之增加。与上一期调查类似，网络犯罪分子和恐怖分子是最主要的威胁行为者。42%的受访者表示，上述威胁行为者中，他们最关注的是黑客活动分子（旨在发表与政治或社会事业有关的声明的威胁行为者）、网络罪犯分子（为牟取经济利益而实施恶意活动）和内部人员（个人恩怨和利益相关）。

在网络攻击者使用的工具和技术方面，钓鱼攻击、恶意软件和勒索软件的组合被34%的受访者报告为最主要的威胁来源。这一比例比上一次调查下降了8个百分点，与此同时，与数据丢失相关的威胁报告却大幅上升，从上次调查的14%上升到本次调查的28%。

同时，40%的受访者表示，他们在过去一年中公开报告了六到十起网络安全事件，这一比例相比上一次调查增加了两个百分点。攻击事件持续上升的趋势并不令人惊讶。对威胁行为者来说，可利用的攻击面很大，并且还在持续扩大。

调查还追踪了受访者如何应对因生成式人工智能（GenAI）出现而产生的新网络安全风险。分析显示，与不太成熟的组织相比，网络成熟度高的组织对这些风险的认识更为明显。在网络安全成熟度最高的组织中，受访者认为会影响其网络安全战略的四大GenAI相关风险如下：

- GenAI输出的可解释性（82%）
- GenAI算法带来信息完整性风险（81%）
- 为GenAI和人类协同工作制定有效的控制措施（81%）
- 数据投毒（例如，通过破坏训练数据集来影响GenAI输出）（80%）

随着越来越多的组织实现流程自动化，并与供应商和其他第三方共享数据，新的安全漏洞也随之出现。这些日益复杂的数字基础设施和生态系统带来了新的攻击机会。

“一切事物和每个人都如此紧密相连，风险正在成倍增加。考虑我们整个供应链网络。考虑所有公司安全能力的全面差异。我们对自己公司内部和员工的安全措施感到相当自信。但问题是，我们如何确保与我们网络接触的每一个人都具备同等的安全防范和控制能力呢？”

——Patrick Milligan，福特汽车公司首席信息安全官

因为人们对网络安全计划所带来的效益期望越来越高，技术完整性是受访者最关心的问题。在持续不断的网络威胁下，企业正在经历一系列负面影响，包括对财务、运营和品牌三个领域的影响（图6）。总体而言，在所有这三个领域中，最受关注的两个问题是对技术完整性丧失信心和运营中断（图1，第7页）。这种持续的关注强调了制定强有力的网络安全战略计划的重要性，该计划能够维护关键技术和运营，并增强组织的韧性。

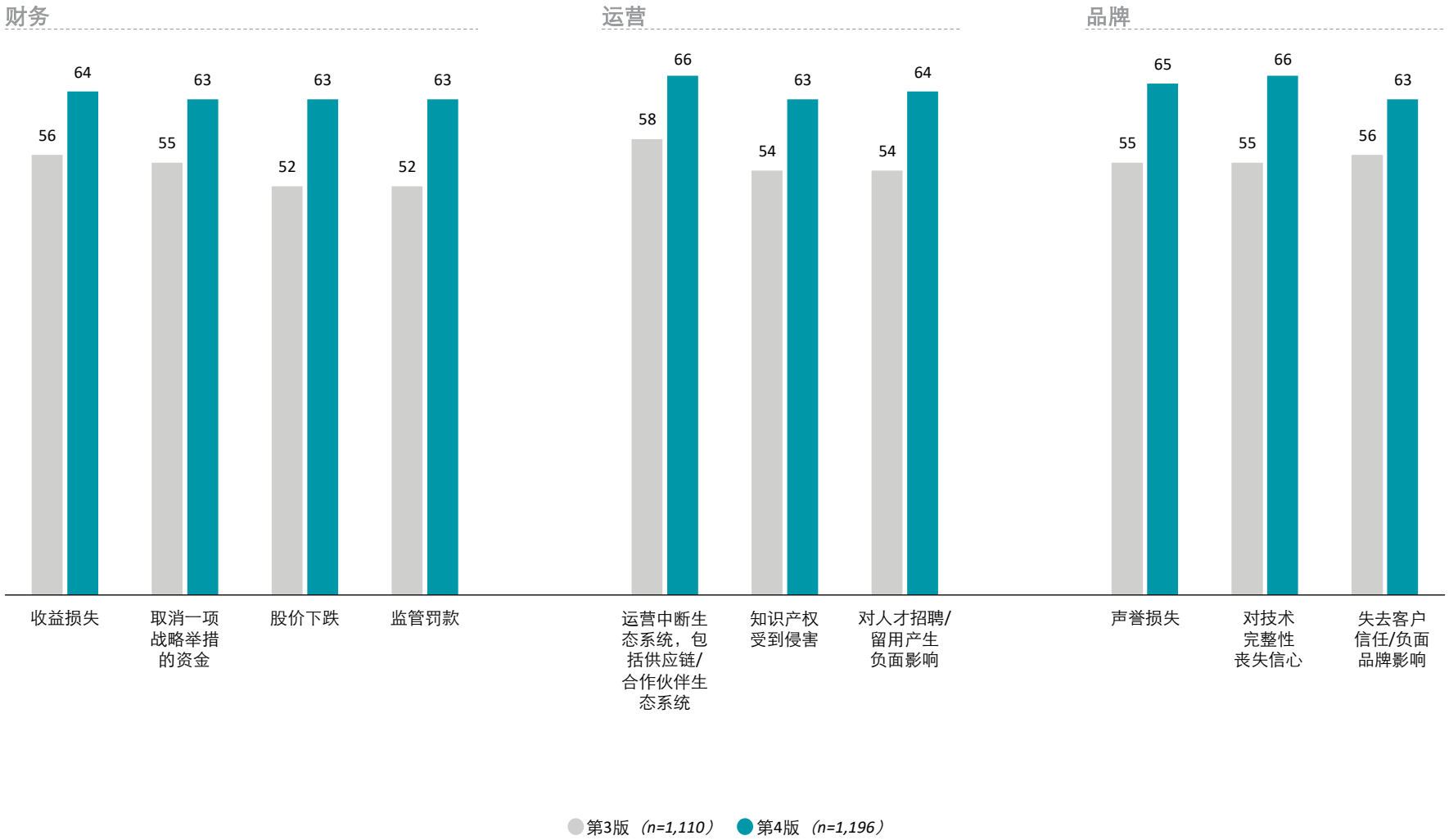
受访者经历的所有负面影响比前一版报告中的程度更高。在第三版报告中，平均56%的受访者在中等和较大程度上经历了所有这些后果，而在第四版中，这一比例上升到了64%。

这一增长表明了两个潜在的现实。首先，组织可能更全面地报告了网络攻击的影响，这表明了意识的增强。其次，由于生成式人工智能（GenAI）和其他先进技术的出现，攻击面和频率已经增加，这凸显了网络安全在未来日益增长的重要性，并明确要求采取行动，制定强有力的网络安全战略计划。

通过三个视角更深入地了解网络安全事件的负面影响（图6）

受访者认为在财务、运营和品牌领域，网络安全事件影响最大的方面。

（百分比）



网络安全事件和数据泄露的这些负面影响，与组织期望通过其网络安全举措实现的效益（积极的业务成果）形成了鲜明对比。调查显示，网络安全举措预期的三大成果是：（1）保护知识产权；（2）提升威胁检测与响应能力；（3）提高效率和敏捷性（图7）。

这些预期效益表明，许多受访者从网络安全投资中看到了运营韧性的增强，但各行业之间存在一定差异：

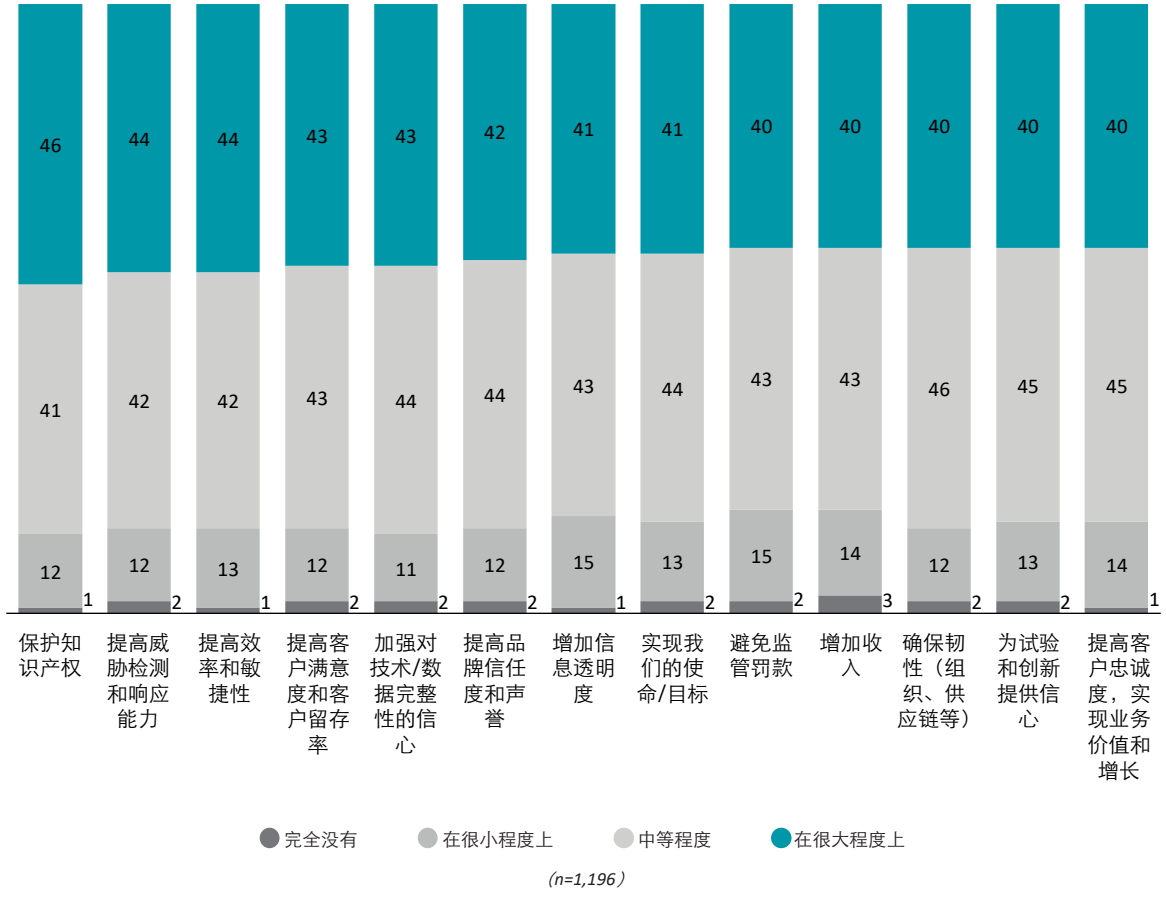
消费者	能源、资源与工业（ER&I）	金融服务业（FSI）	政府与公服务（GPS）	生命科学与医疗（LSHC）	科技、传媒和电信（TMT）
增强对技术/数据完整性的信心	提高效率和敏捷性	改进威胁检测和响应，同时保护知识产权	保护知识产权	提高客户满意度和客户留存率	提高效率和敏捷性

人们对网络安全的期望显然非常高。作为网络安全职能的主要负责人，这些期望主要指向了首席信息安全官（CISO），他们面临着艰巨的任务，即管理并实现业务的预期。对于任何组织而言，网络安全事件和数据泄露都是不可避免的，但网络安全的承诺在于最小化风险和负面影响，并尽可能实现利益最大化——最终目标是使组织更加安全、更具韧性，并利用可信数据推动业务增长。

网络安全的预期成果（图7）

受访者预期从网络安全举措中获得的益处，以及他们期望这些益处实现的程度。

（百分比）



（n=1,196）

首席信息安全官CISO的在领导层中的影响力与日俱增

受访者表示，在他们的组织中，首席信息安全官（CISO）往往对我们调查中询问的大多数网络安全活动负主要责任，首席信息官（CIO）也发挥着关键作用。这些CISO通常向首席信息官或首席技术官（CTO）汇报工作。但调查显示，约有五分之一的CISO直接向首席执行官（CEO）汇报工作。这是业务一致性的一个重要信号，以及在企业高层（C-suite）和执行领导层中的影响力。

首席信息安全官（CISO）在其他方面的影响力似乎也在增长。首席信息安全官（CISO）或同等职位的领导者，越来越多地参与到有关技术能力的战略性业务对话中，这反映出技术能力在推动业务价值方面日益重要。

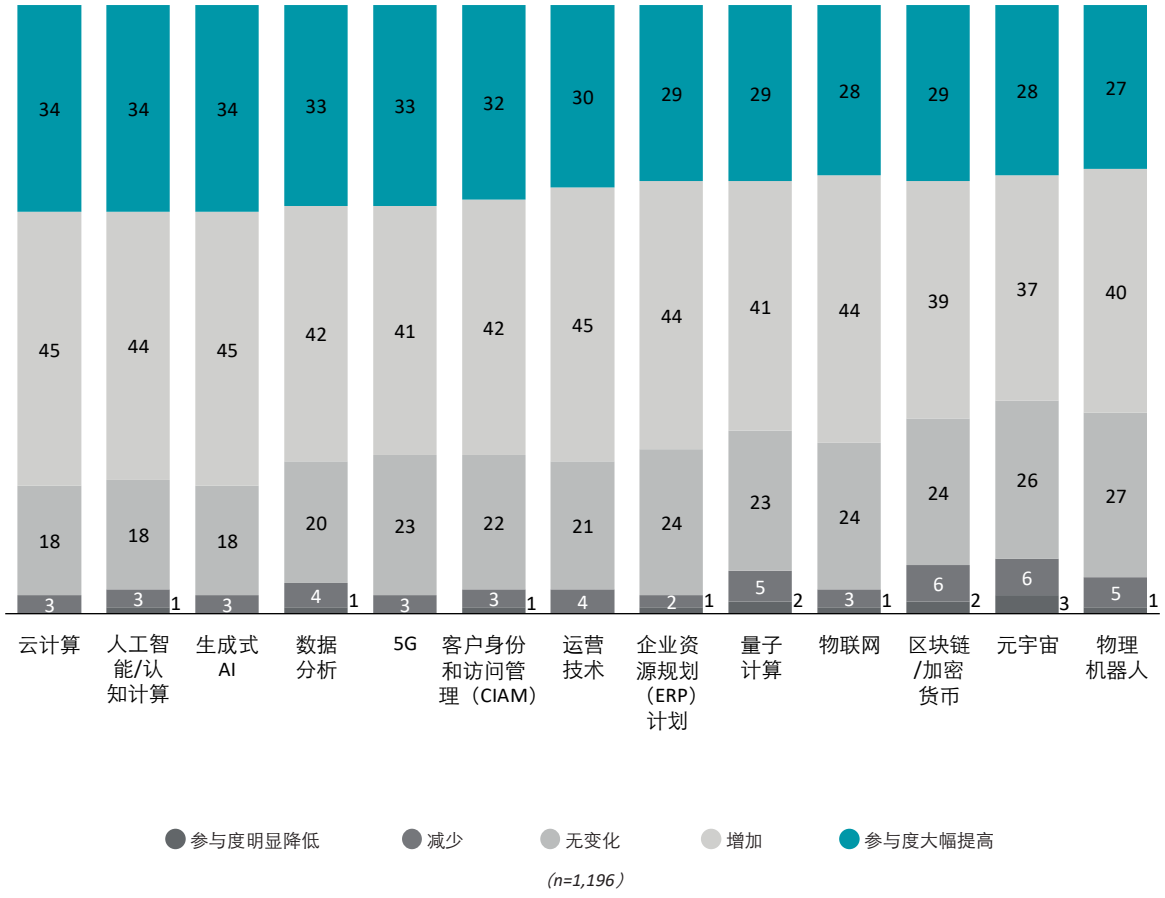
首席信息安全官（CISO）的参与不再是可有可无。

大约三分之一的受访者表示，在过去一年中，首席信息安全官（CISO）在以下技术能力相关的战略对话中的参与度显著提高：云计算、人工智能/认知计算、GenAI、数据分析、5G以及客户身份和访问管理（图8）。

将首席信息安全官（CISO）纳入战略对话（图8）

首席信息安全官（CISO）参与讨论的业务关键型技术能力领域，以及他们参与的程度。

（百分比）



（n=1,196）

随着首席信息安全官（CISO）在领导层中的影响力与日俱增，以及组织努力提升其在网络安全方面的知识和技能，我们预计首席信息安全官（CISO）将成为一个重要的合作伙伴，负责向董事会和企业高层（C-suite）提供关于安全漏洞、风险场景以及提升韧性的必要措施的指导和教育。未来，首席信息安全官（CISO）不仅要领导组织的整体网络安全战略，还要提供战略指导，与其它企业高层（C-suite）紧密协作，确保安全措施与业务目标相协调。

在关注网络安全的企业高层（C-suite）高管中，只有34%非常有信心企业高层（C-suite）和董事会能够充分驾驭网络安全。这一比例比所有受访者的平均信心水平低18个百分点（图9）

“对我们来说，最大的转变是在构建解决方案之前，而不是之后，引入安全讨论。我们希望真正实现“设计中的安全”，而不是经常发生的“评估中的安全”。前者往往要求安全成为企业整体战略中更为关键的组成部分。”

——来自某政府和公共服务机构的网络和IT安全总监

分析表明，网络安全成熟型组织明白，首席信息安全官重要的职责就是让企业高层（C-suite）和董事会参与进来，也是有效解决网络安全风险的关键。他们认识到，通过扮演更具影响力的角色，首席信息安全官可以提供有价值的见解和指导，并确保网络安全作为需要持续关注和投资的战略性业务问题而得到应有的重视和资源。德勤认为，鉴于网络威胁、技术能力以及网络安全与业务整合的不断发展，CISO角色的重要性正在逐渐提升，但我们建议各组织加快行动，提升CISO的角色重要性。

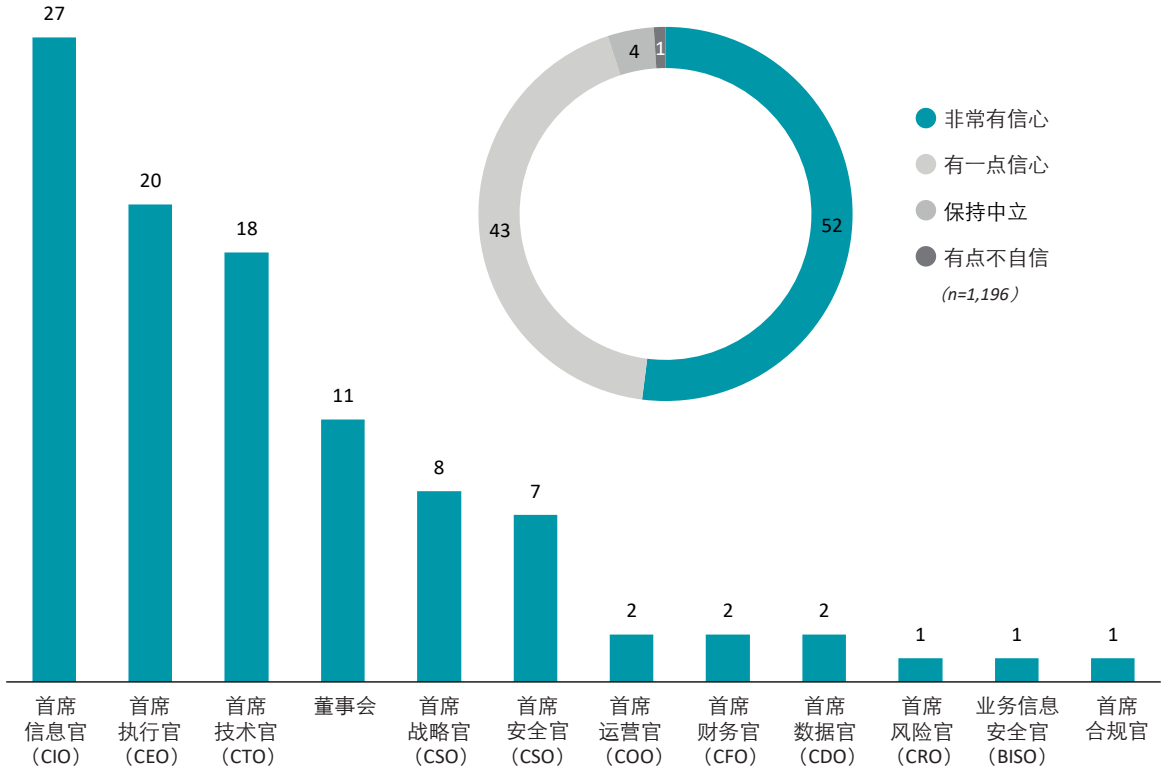
尽管大多数人认为首席信息安全官（CISO）的角色正在演变，且他们已经在企业高层（C-Suite）中占有一席之地，但仍缺乏对企业高层能够自信地驾驭当前复杂网络环境的信心。这种较低的信心水平可能表明，随着CISO有效地向企业高层沟通提示有关的风险/威胁以及组织应对风险的能力，企业高层对当前网络环境的复杂性有了清醒的认识。同时，这也可能反映出受访者整体上对组织的网络安全成熟度和韧性存在过度自信，即他们可能高估了组织在网络安全方面的准备程度和恢复能力。

企业高层（C-suite）的网络安全意识及首席信息安全官（CISO）报告的一致性（图9）

了解领导者对企业高层（C-suite）的信任程度，并总体概述首席信息安全官（CISO）的汇报对象。

（百分比）

首席信息安全官/网络安全负责人向以下领导汇报工作



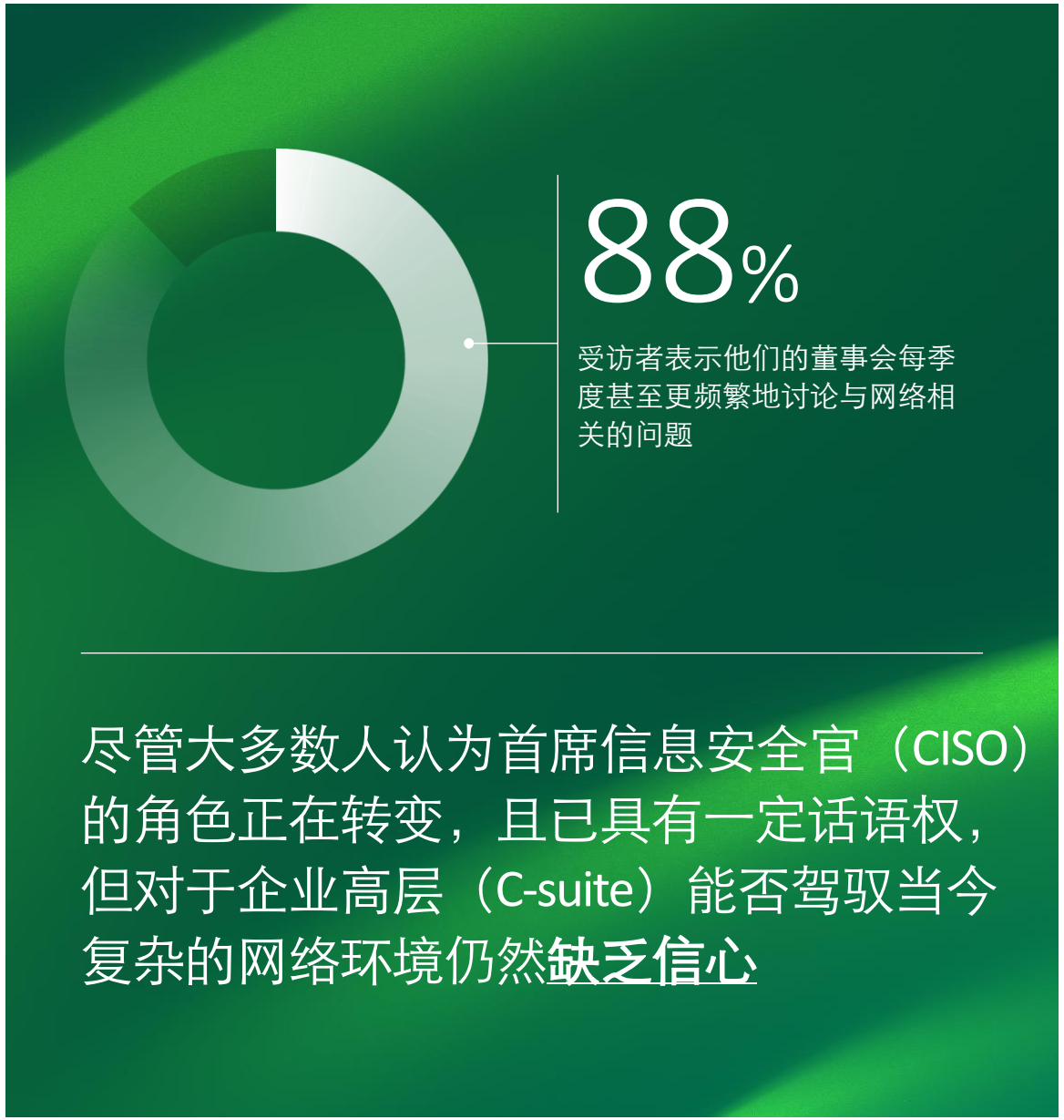
对企业高层（C-suite）和董事会在网络安全领域有效应对的信心

（n=1,196）

虽然网络安全是大多数组织董事会议程上的常规话题，88%的受访者表示他们的董事会每季度甚至更频繁地讨论与网络相关的问题，但显然还需要加强意识教育，首席信息安全官（CISO）需就战略风险和相应措施方面提供建议。在这一点上，德勤的*《Tech-Forward Boardroom》*报告建议，为了提升董事会的讨论水平，技术领导者可以将技术术语转化为业务需求，与首席财务官（CFO）更紧密地合作以阐明业务影响，持续进行结构化报告和基准测试，共同向董事会汇报，通过深入的技术研讨会进行研讨，创建反馈循环，并在小型董事会会议中推广这些活动。

“我们每季度都会向董事会汇报标准的最新情况，而这在几年前是不存在的。我认为，不仅仅是讨论的频率，讨论也更有深度了。我们对董事会现在有疑问的关键议题进行了更多的深入探讨。我们最终会安排更多时间进行深入探讨。”

——某金融服务公司首席信息安全官



网络安全已与技术驱动型项目和数字化业务转型深度融合。

网络安全的边界正在变得模糊，就像数字化转型的界限一样。随着组织与合作伙伴和其他第三方共享数据和系统访问权限，安全和隐私问题变得至关重要。最终，业务、客户、数据和数字信任的增长都取决于网络安全。因此，许多组织正在将网络安全整合到业务和技术职能中（图10）。

“我一直将网络安全视为一种助推器。如果你想在高速公路上快速行驶，你需要确保你有保险杠和制动器，而且你知道你的车有很多部件都在正常工作，否则你将无法在路上行驶。网络安全可以充当这些保险杠或制动器，为汽车提供支撑（以便您能以正常速度行驶）。”

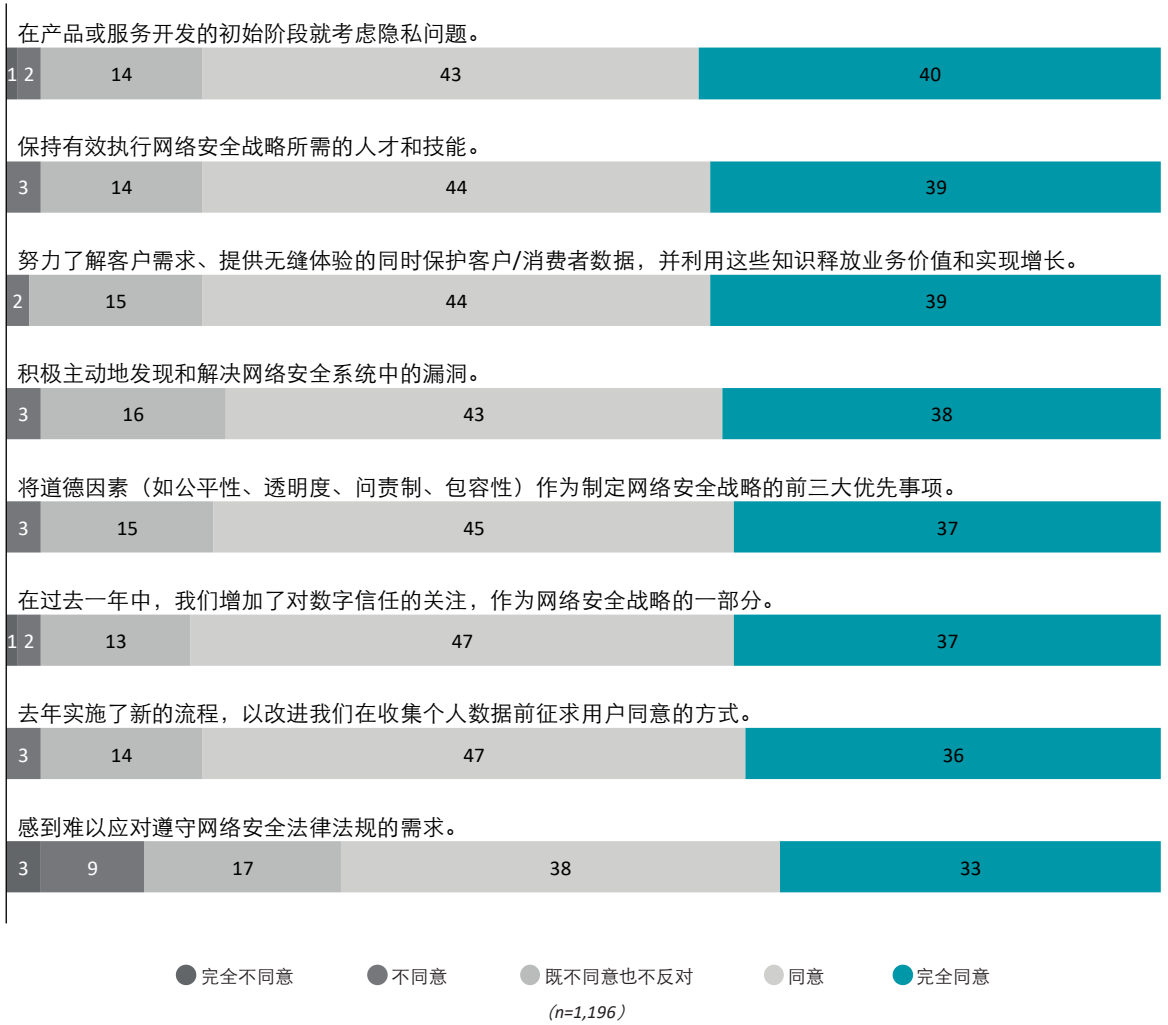
——Vivek Khindria，Loblaw网络安全、网络和技术风险高级副总裁

将网络安全整合到整个业务中

各组织不仅在加强和保护其技术能力，而且还在改变创造新产品的方式。例如，超过80%的受访者表示，他们正在将隐私元素融入产品开发的早期阶段，这有助于保护客户数据并提高数字信任度。这些考虑因素表明，DevSecOps流程的成熟度正在达到一个新水平，网络安全领导者已成功融合进产品设计和开发团队（图10）。

优先考虑隐私、信任和道德（图10）

大多数受访者正在采取措施将网络安全与产品开发、保护客户数据等关键领域的需求进行整合。*（百分比）*



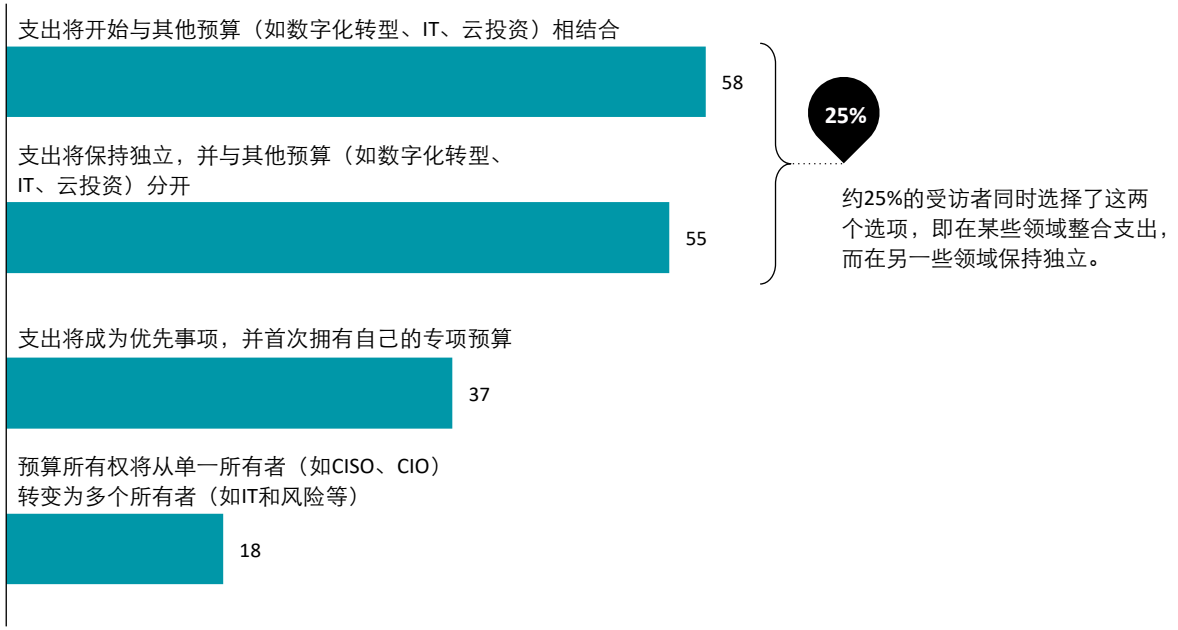
将网络安全融入业务的更多方面也体现在支出方面。如前所述，大多数受访者（58%）预计，网络安全支出将开始与数字化转型、IT计划和云投资等其他计划预算进行整合。与此同时，大多数受访者（55%）也认为网络安全支出将保持独立（图11）。

这两种观点并不矛盾；在被问及网络安全支出的未来时，25%的受访者选择了两个选项——既包括整合支出，也包括独立支出。这种双重性反映了德勤在各组织中的观察结果，即网络安全支出通常来自专门的网络安全预算以及IT、数字化转型、业务领域和产品的预算。换句话说，网络安全支出的规模涉及许多优先事项，这就要求领导者探索不同的、往往是并行的模式来为其提供资金。

网络安全支出与数字化转型的交叉点（图11）

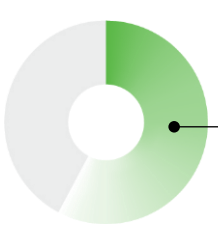
您认为不断变化的数字化环境会如何影响贵组织的网络安全支出？请选择所有适用选项。

（百分比）



（n=1,196）

注：由于四舍五入，百分比相加可能不等于100%。



58%

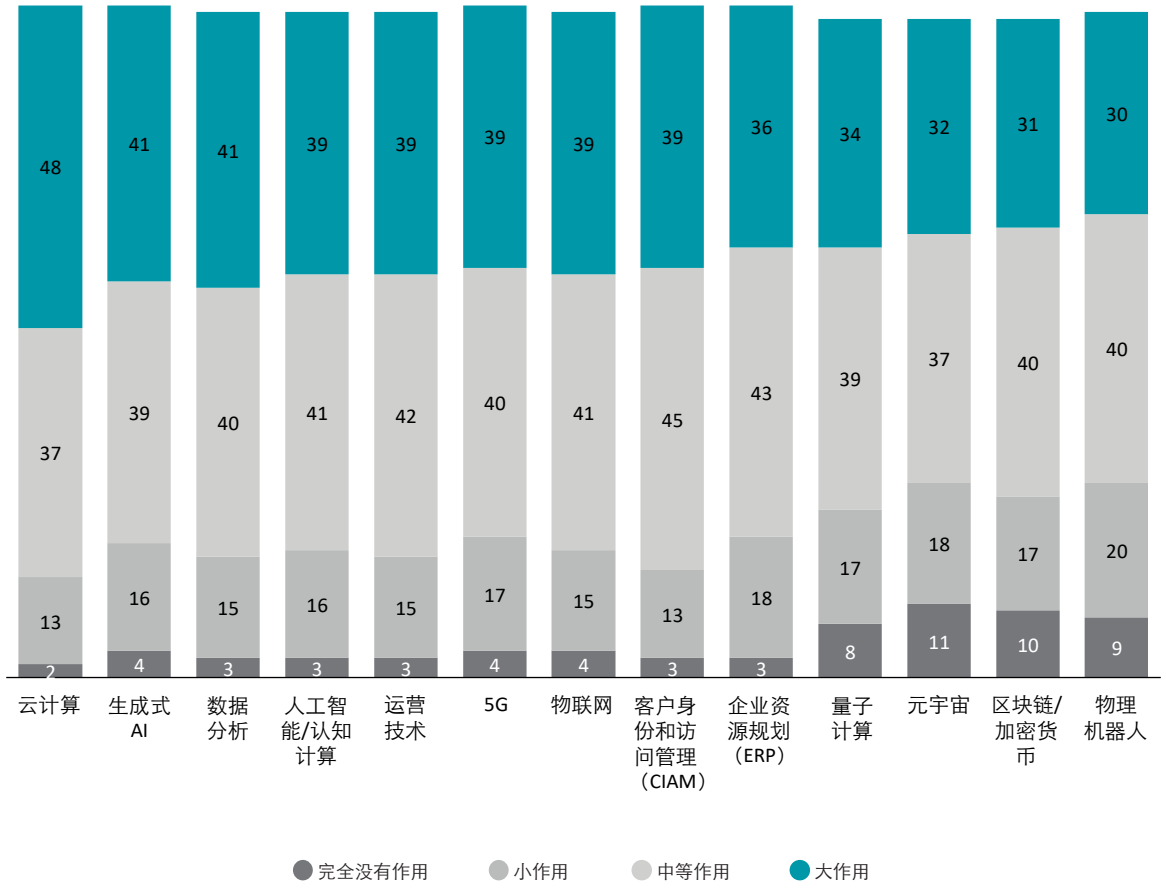
受访者预计网络安全支出将与其他预算相结合。

网络安全预算整合的趋势与另一个新现象紧密相关：网络安全是推动业务目标的关键因素。我们的调查结果显示，网络安全在确保组织对技术能力的投资方面发挥着重要作用，尤其是在云计算（48%）、GenAI（41%）和数据分析（41%）等优先领域（图12）。

网络安全在保障技术投资中的作用（图12）

网络安全如何影响技术能力预算决策。

（百分比）



（n=1,196）

注：由于四舍五入，百分比相加可能不等于100%。

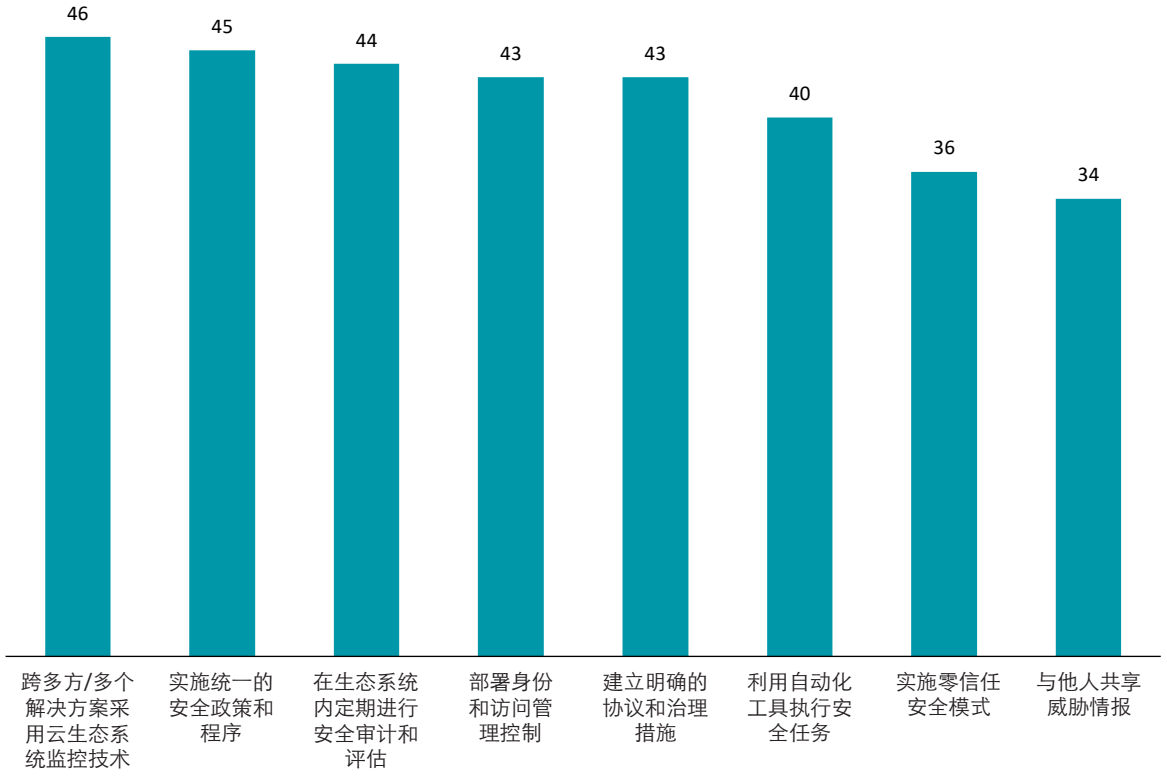
“对于我们这家在全球运营的集团来说，加强安全是推动数字化转型的一项至关重要的活动。我们建立了一个名为‘JFE-安全整合与响应团队’的内部组织，分配预算和人员等资源，并在人力、技术和物理方面实施了必要的措施。我们的目标是在各种业务活动中增强网络安全措施，包括产品、系统和服务的开发、设计、制造和提供。通过这些措施，我们不仅加强了整个供应链的网络安全，并最终为在全球范围内全面提高社会的网络安全做出贡献。”

——Akira Nitta，JFE Steel首席信息安全官

为降低云生态系统的复杂性而采取的网络安全措施（图13）

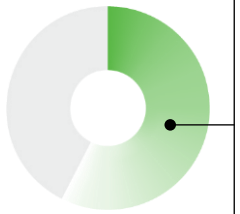
您的组织正在采取哪些网络安全措施来减少云生态系统的复杂性?

（百分比）



(n=1,196)

在云技术方面，网络安全作为推动者发挥着重要作用，不仅有助于提高安全性，还能简化组织的整体云环境。为降低云生态系统的复杂性，受访者采取的首要网络安全措施包括：定期进行安全审计和评估（44%）、实施一致的安全政策和程序（45%），以及在多方/多个解决方案中使用云生态系统监控技术（46%）（图13）。



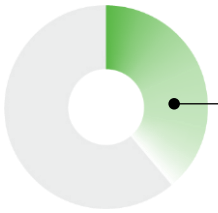
46%

受访者表示在多方/多个解决方案中采用了云生态系统监控技术。

关注人工智能网络安全解决方案

鉴于人工智能在当今的重要性，我们在本次调查中将其纳入了网络成熟度指数。各组织关注的利用人工智能提高网络安全能力的主要方式包括数字基础设施监控、高级模拟和自动化安全。

人工智能生成的内容使攻击者能够以更低的时间投入定制内容的创建。目前，人工智能生成内容的浪潮正以企业为目标，通过冒充可信来源来利用漏洞。这一问题正在迅速加剧。但这并不意味着企业在面对即将到来的人工智能生成内容的浪潮时无能为力。领先企业正在采取积极措施，确保自己不会成为受害者。（来源：*Deloitte 2024 Tech Trends: Defending reality: Truth in an age of synthetic media*）。



39%

受访者表示正在其网络安全项目中大量使用人工智能功能。

随着人工智能在未来不断发展，网络安全的未来也在演变。两者正在共同进化，因为组织正在利用新型人工智能解决方案来减轻网络安全负担。在受访者中，平均有39%的人正在其网络安全项目中大量使用人工智能功能。同时，受访者也表达了对人工智能的担忧，表示需要更新网络安全战略，以跟上技术不断创新的步伐（图14）。

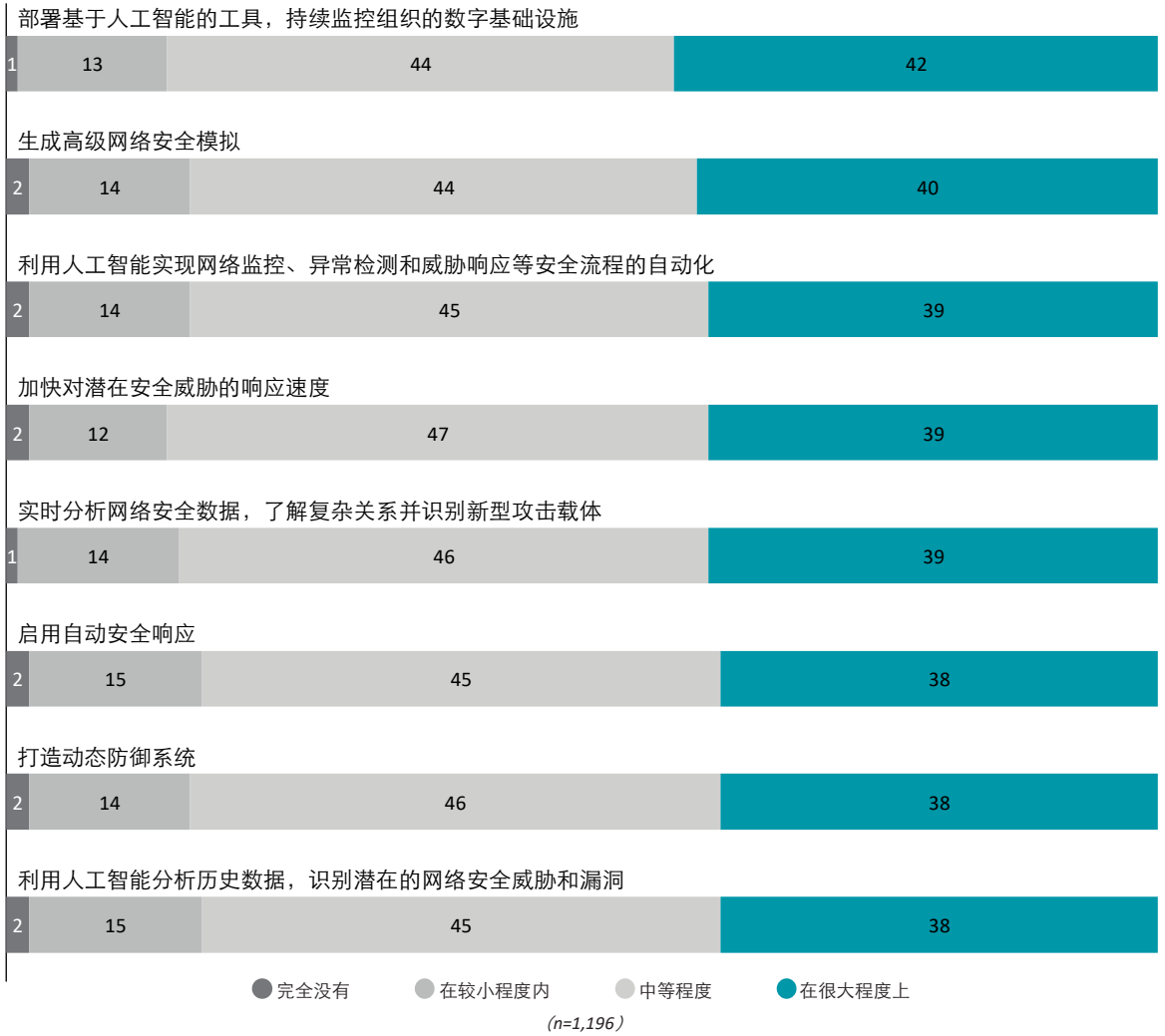
“当然，重点是防止恶意入侵。但我们还必须关注这些新技术（如AI）的影响，以及它们将如何改变我们的环境。我们如何确保以安全可靠的方式应用和使用AI，并利用AI在我们的网络安全框架中更好地提供安全保障？”

——GPS机构，网络和信息技术安全总监

人工智能能力成为关注焦点（图14）

受访者处于何种阶段处以及如何看待人工智能在其网络安全计划中成为一种工具。

（百分比）

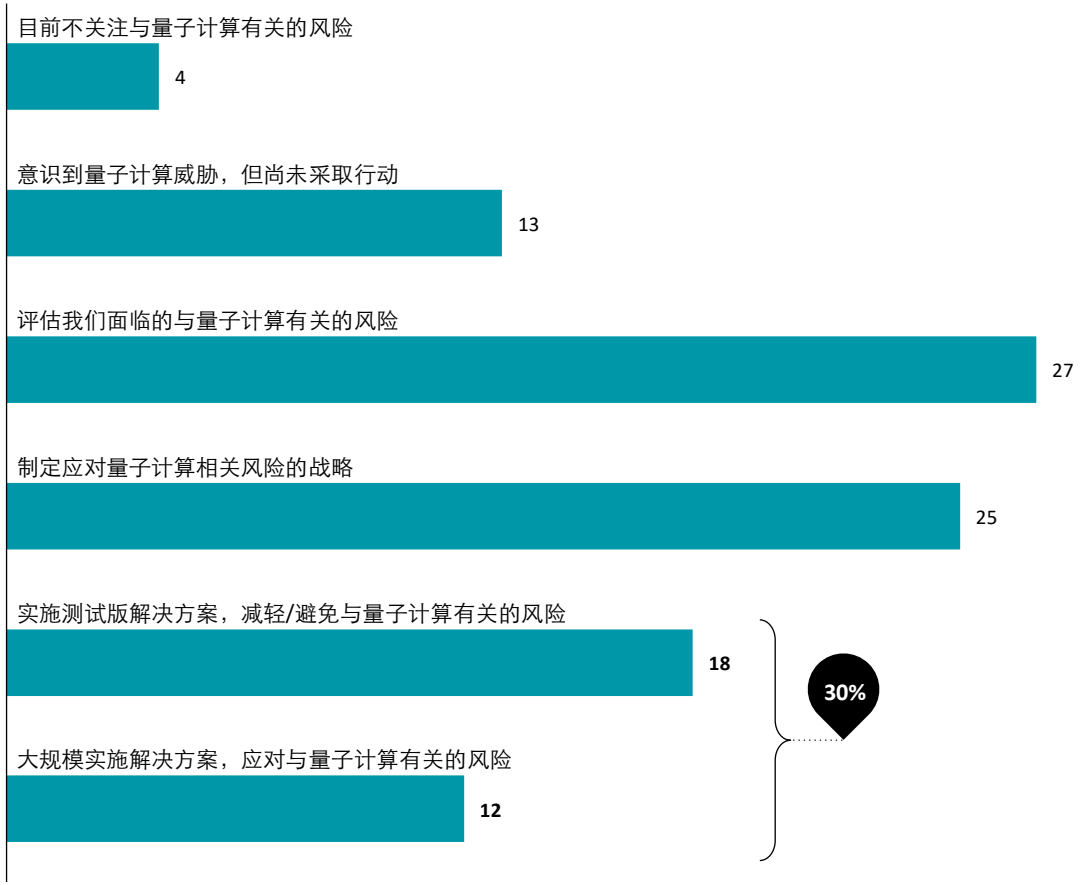


（n=1,196）

量子计算（图15）

各组织如何看待即将到来的量子计算时代以及量子网络安全就绪的必要性。

（百分比）



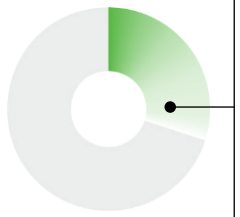
(n=1,196)

迎接下一波新兴技术浪潮

随着组织继续应对与人工智能相关的风险和机遇，其他颠覆性技术也在不断发展，并稳步迈向广泛应用。随着量子计算逐渐成为现实（预计在未来几年内成为主流），并为网络攻击者破解密码提供了一个强大的新工具，量子计算网络安全准备工作正成为许多组织更加关注的焦点。

数据显示，近83%的受访者正在评估与量子计算有关的风险或采取某种行动，无论是制定战略、实施试点解决方案，还是大规模实施解决方案。虽然大多数受访者（52%）仍在评估他们所面临的风险并制定与量子计算相关的风险战略，但其他受访者（30%）正在采取果断行动，作为早期采用者实施解决方案。

这些数据表明，这一问题的发展势头非常明显，领导者可以通过了解潜在风险、审查数据和系统管理、优先处理与业务运营相关的漏洞以及制定加密算法、更新路线图来应对挑战。这样做可以让他们在往往需要多年时间的计划中抢占先机，并在更广泛的企业转型过程中以及通过更新合同机制有序地引入新算法。



30%

受访者正在采取果断行动，作为早期采用者实施解决方案。

网络成熟度较高的组织更有信心，并能从其网络安全实践和投资中获得更大的收益。

网络成熟度指数

德勤借鉴了我们与全球数千家组织合作的经验，将高网络安全成熟度的组织与低网络安全成熟度的同行区分开来。

为了识别这一独特的网络安全领导阶层，并更全面地了解网络安全对企业成功和价值的支持程度，我们采用了四套领先实践来对组织进行评级或指数化：

- 健全的网络安全计划，包括防御和应对网络威胁的战略、运营和战术计划（规划战略的完整清单，见图3，第11页）。
- 关键的网络安全活动，例如定性和定量风险评估、行业基准测试和事件响应情景规划（网络安全活动的完整清单，请参见图2，第10页）。
- 董事会的有效参与，例如组织的董事会定期处理网络安全相关问题。
- 在网络安全计划中部署人工智能能力，重点关注那些在很大程度上采取了八项网络人工智能相关行动中至少五项行动的组织（完整的行动清单请参见图14，第23页）。

本次调查新增了最后一项标准——人工智能能力，旨在反映技术和业务的演变，以及对于变得网络成熟意味着什么。当我们仅使用前三个标准（与上一版相同的指数）时，我们会发现网络成熟型组织增加了三个百分点——从21%的组织增加到24%——这是一个可观的增长。

不过，通过将人工智能因素纳入本版的网络成熟度指数，我们可以定义出更精英的组织群体，这些组织处于塑造网络安全未来前沿。

在本次调查中，高网络成熟度组织占调查对象的14%。与中和低网络成熟度组织相比，高网络成熟度组织是如何对待网络安全问题的，这为企业领导者提供了重要经验，可用于提升组织的网络和业务价值。

对网络安全职能寄予厚望

高网络成熟度组织的受访者高度关注网络安全措施可能带来的潜在效益。平均而言，高网络成熟度组织的受访者期望其网络安全措施带来积极成果的可能性是低网络成熟度组织受访者的2.4倍（是中网络成熟度组织受访者的1.6倍）（图16）。

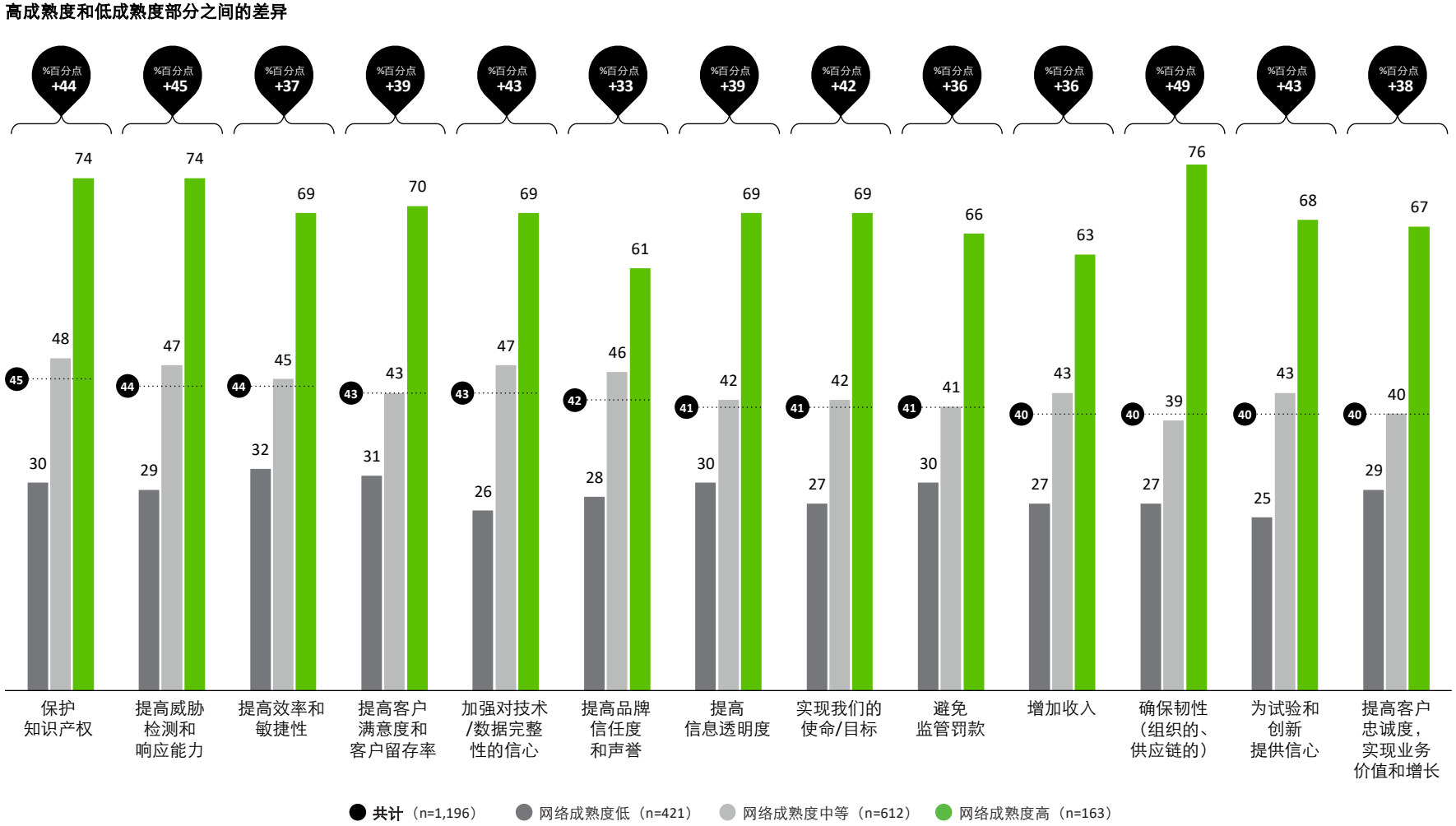
这些积极成果包括：确保组织韧性（76%）、改进威胁检测和响应（74%）以及保护知识产权地位（74%）——在这些方面，高网络安全成熟度组织的受访者的期望与低网络安全成熟度组织的受访者相比有显著差异。

这种情况反映了网络的挑战和前景。最具有网络安全成熟度的组织在所有指标上的期望值都显著更高。虽然他们认识到网络安全应发挥的重要作用，但这种认识也给他们带来了更大的压力，要求他们必须做好各项工作。

网络安全驱动成果（图16）

组织期望从其网络安全工作中获得的收益。

（显示所有三个网络成熟度组别的百分比）



威胁检测和响应方法不断发展

任何组织都无法避免网络安全数据泄露和网络安全事件的负面影响，即使是那些在网络安全方面成熟度较高的组织也不例外。平均而言，我们的分析表明，高网络安全成熟度的组织在检测网络威胁和遵守相关报告要求方面的能力更强。例如，25%的高网络安全成熟度组织的受访者报告称，在过去一年中发生了11次或更多的网络安全事件，这一比例比总体受访者高出8个百分点。虽然这看起来像是一个负面因素，但或许是因为这些组织可能拥有更强的威胁检测能力，使它们能够更有效地识别和应对威胁。

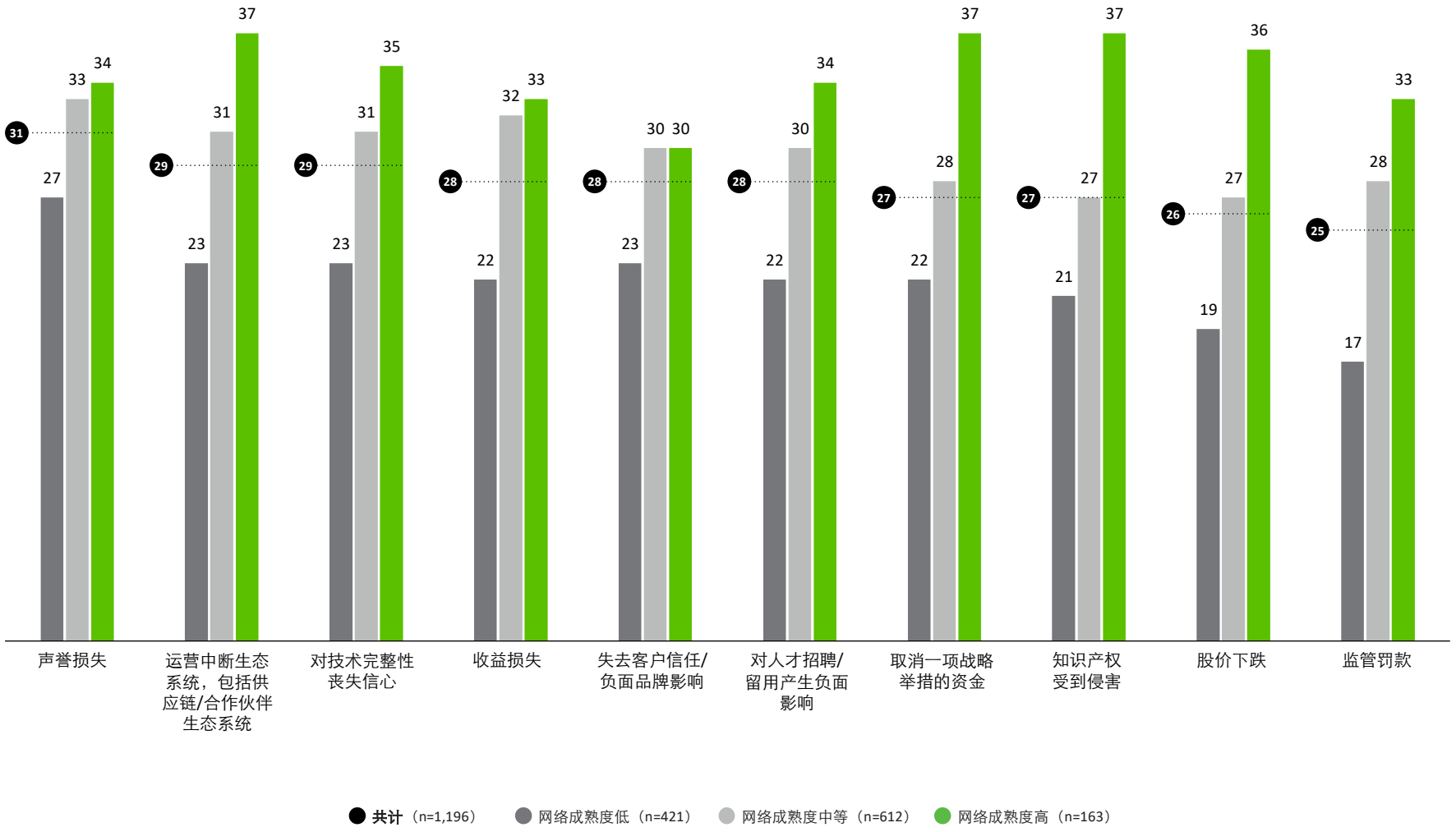
除了对网络攻击和事件有更高的认知外，这些组织还了解与漏洞和事件相关的真实成本。平均而言，高网络安全成熟度的组织比低网络安全成熟度的组织更有可能承认财务、运营和品牌影响的严重性，这一比例高出13个百分点。

这种更深入的理解反映了一个“良性循环”，为网络安全在整个业务和技术领域的持续整合提供了潜在的催化剂。它还有助于提升首席信息安全官（CISO）的角色，以保护和维护未来的价值，提高运营效率和韧性，并支持创新和收入增长目标。

按成熟度分组的预期负面后果（图17）

网络成熟度高的受访者发现的网络安全事件更多，部分原因可能是他们的威胁检测能力更强。

（百分比）



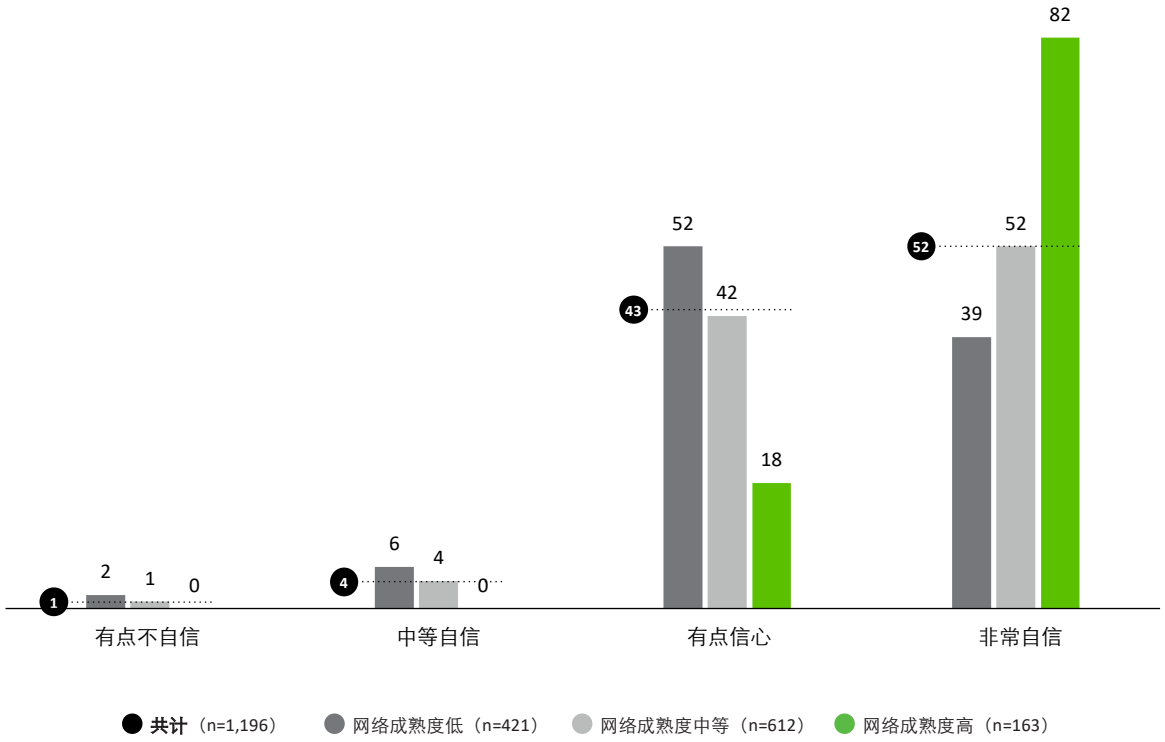
建立高管层对网络安全驾驭能力的信心

在网络安全成熟度高的组织中，企业高层（C-suite）驾驭网络安全的信心越高。高管层和董事会有效应对网络安全需求的能力表示非常有信心的比例，是网络安全成熟度低的组织中受访者的两倍（图18）。

信心达到最高水平（图18）

高管层和董事会应对网络安全问题的能力有多大的信心。

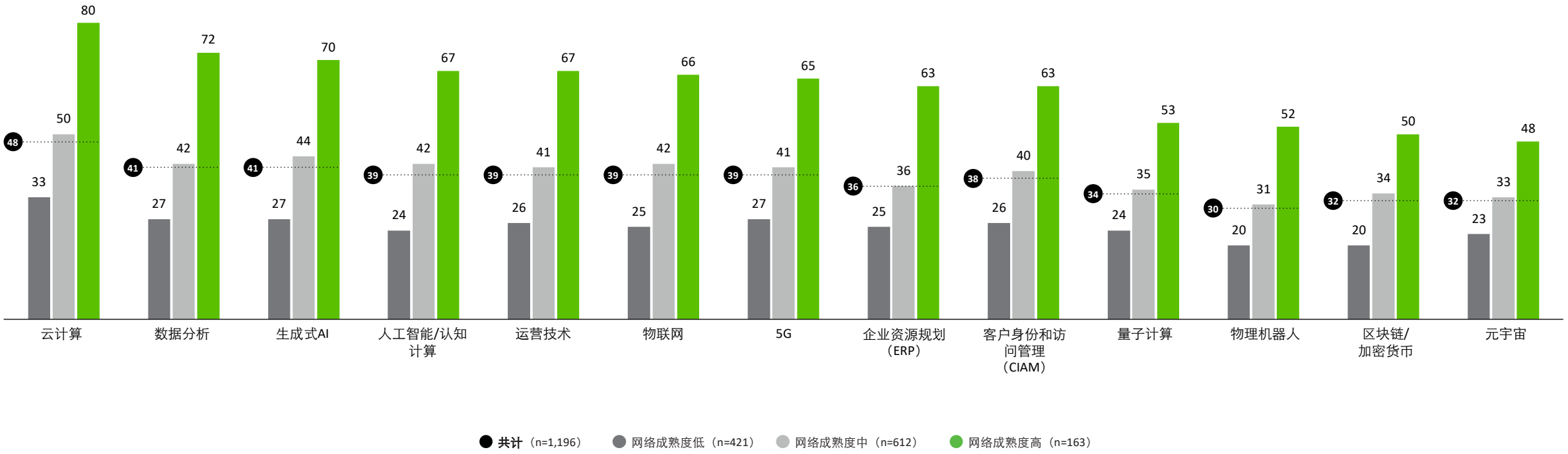
（显示的是所有三个网络成熟度组别的百分比）



高网络安全成熟度的组织似乎更擅长利用网络安全来为技术能力获取投资，也更善于让首席信息安全官（CISO）参与数字化转型的战略对话。

平均而言，高网络安全成熟度组织的受访者表示网络安全在为其技术能力获取投资方面发挥重要作用的可能性，比低网络安全成熟度组织的受访者高出2.5倍。他们获取投资的主要领域包括云计算、数据分析、生成式人工智能（GenAI）、运营技术（例如，工业控制系统）和人工智能/认知计算（图19）。

更高的成熟度意味着网络安全在技术驱动的能力中扮演更重要的角色。（图19）
与其他组别相比，网络成熟度高的组别认为网络安全在确保技术能力投资方面发挥着重要作用。
（显示的是所有三个网络成熟度组别的百分比）



在关于技术能力的战略讨论中，与低网络安全成熟度的组织相比，高网络安全成熟度的组织中，CISO或网络安全领导者的参与显著增加的可能性要高出2.3倍。在高网络安全成熟度的组织中，CISO参与最多的领域包括云计算、人工智能/认知计算、物联网（IoT）、生成式人工智能（GenAI）和数据分析（图20）。

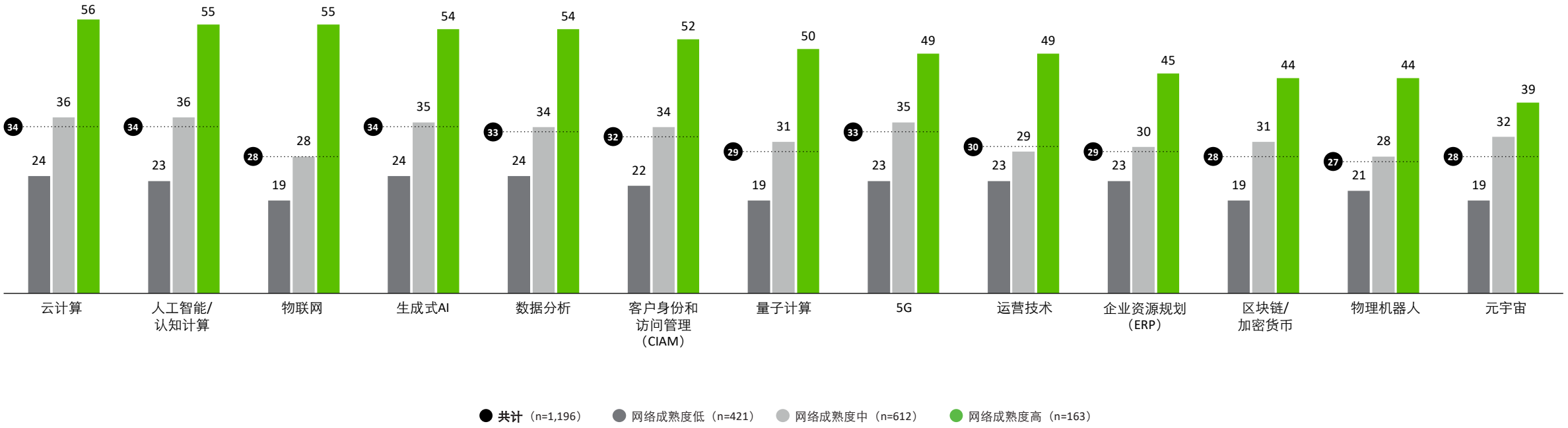
“首席信息安全官（CISO）的角色正在演变。他们需要引入正确的策略，积极引导公司做出数据驱动型决策。由于这需要与高层领导更多地互动，CISO不仅需要具备技术方面的专长，还应具备高管级别的思维和商业敏锐度，以展示网络安全策略将如何影响业务。”

——Gary Harbison，强生公司首席信息安全官

随着网络安全成熟度的提高，首席信息安全官（CISO）更多地参与战略讨论（图20）

网络成熟度高的组别，其首席信息安全官更频繁地参与所有领域的对话。

（百分比）



洞悉
网络安全未来

全方位构筑企业网络安全防线

为顺应未来网络安全新格局，企业必须深入理解和精准把握网络安全领域的新兴趋势。更为重要的是，企业应当付诸实际行动，创造巨大的商业成效。通过聚焦以下关键要素和可行措施，企业可极大地提高网络安全成熟度，打造差异化竞争优势。

夯实网络安全基石，打通合作渠道，提高抗风险能力

随着网络安全的战略价值日益得到重视，企业管理层需认识到，网络安全不仅仅是一个IT问题，更是贯穿于企业各个部门和层级，需要全面协调融合的核心业务问题。它要求企业不断推进网络安全功能在商业与技术领域的融合，并将其列为重中之重。

随着管理层对网络安全的认知不断加深，以及网络安全功能与其他领域的融合愈发明显，企业日益聚焦网络安全带来的业务价值，旨在全面提升其团队协作、信息共享和决策水平。这将有助于企业高层深刻洞察实际业务情况，并据此制定战略决策，确保各项决策和行动与业务目标紧密契合，且能有效防范网络风险。

企业应将网络安全视为核心要务，深化网络安全在各领域的融合，更好地保护关键资产和品牌声誉，全面提升自身抗风险能力，在日益高涨的数字化浪潮下领航前行。

曾经被视为企业IT的首席安全卫士，**首席信息安全官（CISO）的角色**正在演变，现在不仅帮助保护整个企业，从核心业务运营到品牌声誉，还支持创新和业务的未来。

提高领导层的参与度和敏锐度，从首席信息安全官（CISO）到其他企业高层（C-suite）和董事会

网络的未来网络明确指出了一个当务之急：确保CISO积极参与有关技术能力和业务的战略对话。CISO不再仅仅是企业IT的安全守护者，而是成为企业战略的重要参与者，负责保护企业的核心业务运营、品牌声誉，同时支持创新和业务的未来发展。

并且，CISO应与其他具备网络安全知识的高层领导一起参与。有效应对网络安全风险，并将其置于业务目标的背景下，需要整个高级管理层和董事会定期参与网络安全对话。由于网络安全是组织面临的首要风险，高层领导必须在其管理和监督中保持高度参与。通过CISO的积极参与并为董事会和组织提供宝贵的见解和指导，网络安全可以得到应有的关注和资源——作为一个需要持续投资的战略性业务问题。

以战略和治理为基础，主动驱动整合预算

这表明网络安全正在得到应有的认可，也表明更多的部门可能会将网络安全纳入其未来的资金计划中。

这种整合方法可以为整体安全带来更全面的战略和更好的结果。通过建立一个支持更广泛的议题并定义网络安全目标的明确治理框架，组织可以朝着其业务目标迈出关键步骤。这种方法意味着组织中的每个人都理解网络安全的重要性，投入适当的资源，并朝着共同的目标努力。

通过实施有效的治理，组织可以确保网络安全计划与其他重要的业务优先事项保持一致，但这种整合转型投资可能存在一些缺点。如果预算中没有明确将网络安全作为一个细列项目，那么网络安全可能会被削弱，因为此时它往往就会被视为成本的一部分，而不是一项增值投资。

“在制定战略时，我们正逐渐成熟的一个方面是体现在开始以结果导向。所以，我们总是思考未来数年后我们希望处于什么位置。我相信，在安全领域制定超过两年的战略会有很多变化，因为威胁会变化，技术也会变化，等等……因此，我们基于结果来构建战略，这一点非常关键。”

——某生命科学与医疗公司首席信息安全官

未来已至
制胜有方

未来已至。当前每一个决策和行动，都书写着网络安全的未来。新兴网络安全威胁、前沿技术以及商业决策正不断演变，懂得未雨绸缪、谋定而动，方能有效提升网络安全成熟度，向着更加长远的未来不断迈进。

随着企业对网络安全的认知日益加深，管理层也愈发积极地参与关于网络安全的战略讨论。网络安全逐步成为企业转型升级的核心要素，一个崭新的时代悄然拉开序幕。未来已来，您将如何书写非凡篇章？又将如何推动企业迈向卓越？

蓄势待发

联系我们，获取更多关于德勤第四期《全球网络安全前瞻调研》的专业洞见，了解具备成熟网络安全体系的企业如何提升业务价值，并在激烈的市场竞争中脱颖而出。

致谢

感谢Saurabh Bansode、Criss Bradbury、Deborah Elder、John Gelinne、Tanneasha Gordon、Matt Holt、Pratik Joshi、Diana Kearns-Manolatos、Isaac Kohn、Daphne Lucas、Mike Morris、Kelly Nelson、Iram Parveen、Sean Peasley、Abdul Rahman、Colin Soutar、Jan Vanhaecht、Marius von Spreti对本报告的支持和贡献。

德勤中国网络安全服务主要联系人

薛梓源
德勤中国网络安全事业群
主管合伙人
德勤中国网络安全–网络安全防御韧性及企业安全服务
主管合伙人
电话：+86 10 8520 7315
电邮：tonxue@deloitte.com.cn

冯晔
德勤中国网络安全–网络安全战略转型及数字隐私信任服务
主管合伙人
电话：+86 21 6141 1575
电邮：stefeng@deloitte.com.cn

Phill Everson
德勤中国网络安全–香港
主管合伙人
电话：+85 22 852 1222
电邮：philleverson@deloitte.com.hk

德勤中国网络安全–网络安全防御韧性及企业安全服务

内地

张震
电话：+86 21 6141 1505
电邮：zhzhang@deloitte.com.cn

马红杰
电话：+86 21 3313 8528
电邮：jacma@deloitte.com.cn

肖腾飞
电话：+86 10 8512 5858
电邮：frankxiao@deloitte.com.cn

金洁
电话：+86 21 2316 6315
电邮：jerjin@deloitte.com.cn

肖康
电话：+86 10 8534 2488
电邮：kenxiao@deloitte.com.cn

刘征
电话：+86 10 8512 4009
电邮：zhengliu@deloitte.com.cn

杨天
电话：+86 20 8715 8566
电邮：michayang@deloitte.com.cn

香港

王凯民
电话：+85 22 238 7908
电邮：harrywang@deloitte.com.hk

吴俊伟
电话：+85 22 852 6318
电邮：andycwng@deloitte.com.hk

Pramod Potharaju
电话：+85 22 852 6616
电邮：prpotharaju@deloitte.com.hk

崔汶俊
电话：+85 22 238 7946
电邮：cchui@deloitte.com.hk

莫嘉豪
电话：+85 22 740 8829
电邮：phmok@deloitte.com.hk

德勤中国网络安全–网络安全战略转型及数字隐私信任服务

内地

阎光
电话：+86 21 2316 6282
电邮：alexyan@deloitte.com.cn

何微
电话：+86 75 53353 8697
电邮：vhe@deloitte.com.cn

邓娜
电话：+86 75 53353 8151
电邮：tindeng@deloitte.com.cn

林松祥
电话：+86 10 8512 4888
电邮：chaphylin@deloitte.com.cn

江玮
电话：+86 21 2312 7088
电邮：davidjiang@deloitte.com.cn

何晓明
电话：+86 10 8512 5312
电邮：the@deloitte.com.cn

香港

林普毅
电话：+85 22 109 5353
电邮：bradlin@deloitte.com.hk

鄭若琳
电话：+85 22 238 7119
电邮：eicheng@deloitte.com.hk

蕭凱婷
电话：+85 22 852 5898
电邮：hattysiu@deloitte.com.hk

林道勛
电话：+85 22 531 1488
电邮：tonlam@deloitte.com.hk

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31个城市，现有超过2万名专业人才，向客户提供审计、税务、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”。德勤全球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。请参阅www.deloitte.com/cn/about了解更多信息。

德勤亚太有限公司（一家担保责任有限公司，是境外设立有限责任公司的其中一种形式，成员以其所担保的金额为限对公司承担责任）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，包括奥克兰、曼谷、北京、班加罗尔、河内、香港、雅加达、吉隆坡、马尼拉、墨尔本、孟买、新德里、大阪、首尔、上海、新加坡、悉尼、台北和东京。

本通讯中所含内容乃一般性信息，任何德勤有限公司、其全球成员所网络或它们的关联机构并不因此构成提供任何专业建议或服务。在作出任何可能影响您的财务或业务的决策或采取任何相关行动前，您应咨询合资格的专业顾问。

我们并未对本通讯所含信息的准确性或完整性作出任何（明示或暗示）陈述、保证或承诺。任何德勤有限公司、其成员所、关联机构、员工或代理方均不对任何方因使用本通讯而直接或间接导致的任何损失或损害承担责任。

CoRe Creative Services. RITM1965157