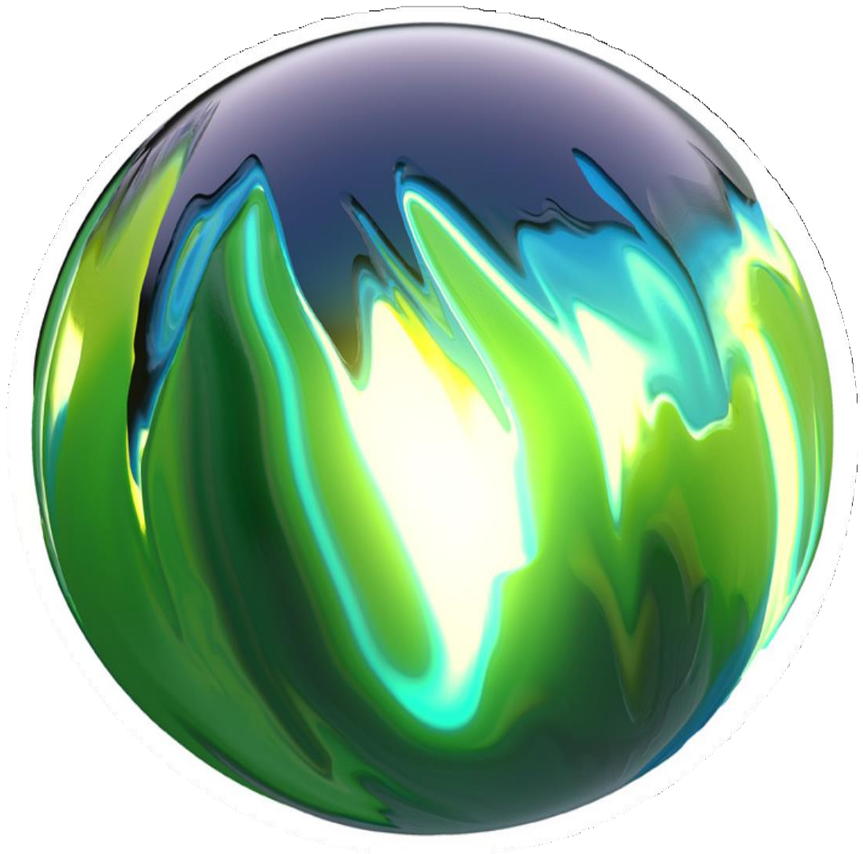
Deloitte.

德勤



2021网络安全前瞻调研报告

网络安全| 为未来赋能您的员工

MAKING AN IMPACT THAT MATTERS since 1845

网络安全前瞻调研报告

调研方法

德勤**2021网络安全前瞻调研报告**由德勤与Wakefield Research于2021年6月6日至8月24日间联合开展，采用线上方式就网络安全问题访问了近600位首席高管，其中包括约200位首席信息安全官、100位首席信息官、100位首席执行官、100位首席财务官和100位首席营销官，他们均来自年收入不低于5亿美元的公司。

洞悉复杂性

当下，我们生活在一个网络无处不在的世界，其中，数字化转型持续加速，远程办公日趋普及。科技创新及其驱动的创新文化，似乎已远远超出我们能够认知、衡量并应对这些成倍增长的风险的能力。

尽管风险环境日益严峻，数字化转型和迁移上云仍是客户的首要任务。数据在企业内的流动，它不仅仅能提高效率，还能推动新的价值创造方式，连通各业务线并丰富客户体验。我们的调查数据凸显了数据迁移的特点--94%的受访首席财务官表示他们正考虑将其财务系统或企业资源规划（ERP）系统迁移上云。

85%
年收入在5亿到300亿美金之间

87%
在1到20个国家运营

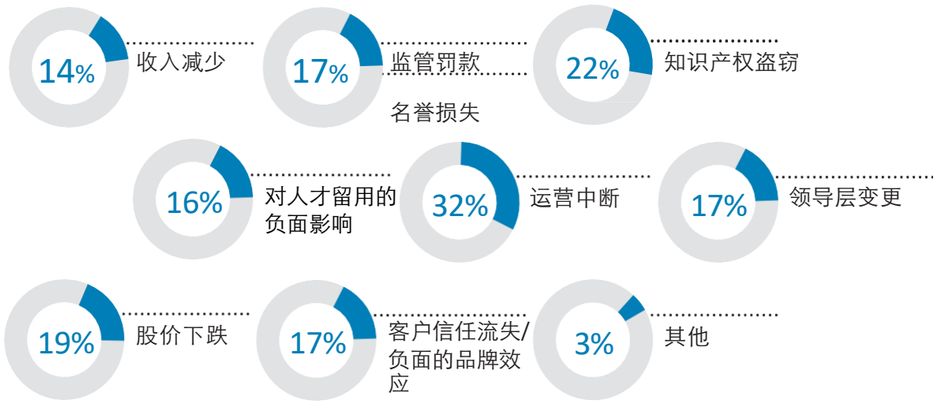
公司总部
40% 位于美洲
28% 位于欧洲、非洲和中东地区
32% 位于亚太地区

当前情况

当下，企业为保持竞争力，采用融合自建基础设施与混合IT架构，并与第三方云供应商开展合作等一系列信息技术举措。这些复杂的集成环境需要不同于传统内部IT架构的新型管理形式。受访的大多数首席信息官和首席信息安全官（41%）表示，如何转型以及了解日益复杂的混合生态系统是其面临的最大挑战。

新冠疫情不仅造成市场压力，还宣告着远程办公时代的到来。无论大型还是小型企业，都在迅速变革工作环境，随之而来的就是网络攻击面大大增加，但企业往往很少甚至没有时间考虑安全问题。毫无意外，攻击事件频繁发生。69%的受访者称在2020年初至2021年5月的期间，其企业受到的威胁有所增加或显著增加，各行业和各地区均是如此。在受访的全球首席高管中，有32%表示运营中断是最大的影响，其次是知识产权盗窃（22%）和股价下跌（19%）。

网络事件的最大影响*



*受访者最多可选择两项答案，因此各选项的百分比加总超过100%。

持续验证，从不轻信

在被问及管理企业网络安全的最大障碍时，受访者将跨越复杂边界的数据管理排在首位（44%），其次是更好地划定企业网络风险的优先顺序（31%）。所幸的是现在部署零信任方案（Zero Trust）已然可行，使用基于持续风险评估的实时访问决策替换简单的实体验证。在实施过程中，它是对当今网络生态系统网络边界模糊的有效应对，认为架构内每个组件都有弱点，每一层设施均需要保护。

得益于近期计算能力的提升，企业中零信任架构的出现和采用到企业中广泛的文化变革，揭示了网络安全的角色如何转变，其重要性如何提升。零信任不仅仅是一种技术修复，它是一套相互交织、洞悉敌对活动及相关业务风险、并变革于消减风险的方案集合。这种洞察需要IT部门和业务部门之间的协调，以及整个企业的安全意识提升和培训。

“我们正处在转型和快速发展的时期。企业面临的最大两项挑战分别是混合IT架构和转型。这将创造一个更加多元和复杂的环境。如何实现更多的可见性，尤其是对云部署，是企业的当务之急。”

— 德勤全球网络安全服务领导人
EMILY MOSSBURG

重构网络防御

黑客变得越来越老练，也越来越了解资产的市场价值——无论是医药知识产权、工程和产品专利、客户或其他关键数据——企业将继续增加其网络防御预算。在总年收入超过300亿美元的受访者中，近75%表示，今年在网络安全方面的投入将超过1亿美元。

随之而来的挑战即是，如何确保这些投入能够提高在日益复杂的混合网络生态系统中被放大的风险的透明度。除获得技术和经验外，还要求企业进行组织变革，以推动从企业到合作伙伴和第三方供应商的有计划的治理。技术在发展，首席信息安全官的职责也在改变。随着网络在企业中蔓延渗透，必须重新定位首席信息安全官在企业架构中的位置。除简化汇报线外，增进与首席执行官的关系也有利于加强首席信息官对业务优先事项的理解并及时捕捉创新。首席信息安全官，这一新的运营角色在企业内更高的参与度，能够确保网络安全团队将必须满足的要求、技术方案和控制措施完全嵌入到创新举措中。这不仅在一开始就将风险降到最低，还能将产品和服务开发的整体风险降到最低。

鉴于网络安全对企业深度文化影响，因此我们今年将调研范围从直接监管网络安全的负责人扩大到网络安全的最广大的拥护群体：首席执行官、首席财务官、首席营销官、首席信息官以及首席信息安全官。他们的观点彼此相似，但在不同地区和行业还是存在差异。

展望未来

尽管没有简单的组织或技术解决方案能够洞察支撑现代企业日益复杂的集成网络生态，但是，却有许多组织、文化和运营方面的措施，一旦结合使用，可以促使企业将网络安全嵌入其业务举措和企业文化的核心，嵌入其不断发展的技术生态系统。

下一代技术发展将继续打造更加互联互通的世界，在此次报告中，我们探索了其中部分措施并强调了企业洞悉现时技术复杂性和未来技术变革能力的重要性。

网络安全及转型挑战

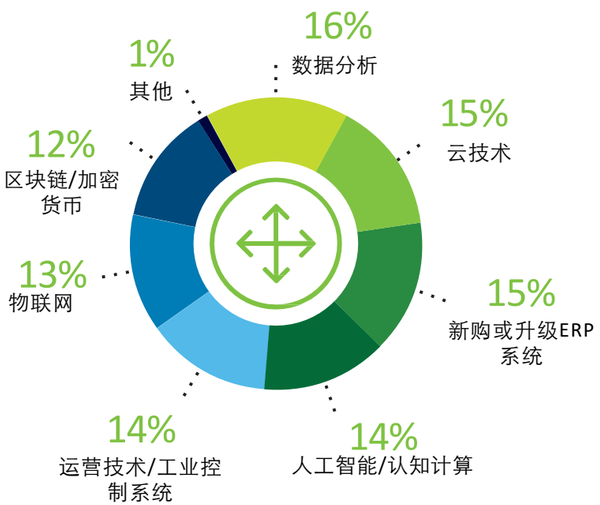
在任何行业，保持竞争力都需要快速开发新产品和服务并推向市场。

创新型业务模式不仅仅是简单地将现有流程数字化，其正在覆盖供应链并打造新颖的客户体验。这种转型也使企业面临新的网络风险，要求企业采用新的网络战略保护不断发展的业务模式。为管理这些风险，公司高管和董事会成员需拥抱变革，实施跨业务线的有效治理，并演进风险管理流程以实现对所有新接入业务的端到端可见度洞察，也包括由第三方承接运营的业务领域。能否成功取决于企业高级管理层的承诺， 以及在网络安全方面有效投入的同时，他们理解网络安全风险的能力。

在被问及如何对其未来一年的数字化转型举措进行排序时，16%的受访者将数据分析列为首要任务，15%选择云技术，另有15%选择新购或升级ERP系统。在今年的调研中， 增加了OT/ICS（运营技术/工业控制系统）的问题以及回应选项（14%认为其是首要任务），这表明整个行业正在努力实现工厂和运营技术环境的数字化和现代化。

真正具有颠覆性的是变革的速度和规模。新冠疫情爆发后，整个世界都转向线上活动，这种颠覆立刻变得更加明显。随着企业大量员工远程协作，所有企业部门几乎立刻转型。所幸大部分所需的生态系统，从云到 Shadow IT (影子IT设施) 到 ICS（工业控制系统），均已就位并准备好迅速扩张。但不太明显的是这种转变背后存在着网络风险，目前很少有企业掌握识别并缓释网络风险至可接受水平的的方法。

企业数字化专项举措优先级排序



“公司高管和董事会成员的主要目标必须是充分了解数字化转型给公司带来的实际风险， 能够与所有其他类型的风险一样同等地管理此种风险。”

—德勤网络安全服务全球网络战略及转型领导人
MATTHEW HOLT

认知网络风险

由于网络威胁会影响整个企业，可能使业务瘫痪并迅速摧毁来之不易的声誉，因此董事会务必要以他们能够理解的方式评估网络风险。他们需要将网络威胁与其擅长处理的风险进行比较，熟练分析网络风险情况，就像其了解资产负债表的健康情况一样。

一旦他们能够理解其所面临的网络风险的性质和规模，他们才知道如何分配资源才能最好地减轻风险。

此次调研发现，41%的受访者使用网络成熟度评估指导网络投资决策；35%使用风险量化工具；23%称其依赖于公司网络领导层的经验。当被问及对新的和/或现有应用程序进行风险分析/威胁建模的频率时，37%的首席信息官和首席信息安全官表示他们每季度进行一次，29%每月进行一次。尽管这些评估通常属于首席信息官和首席信息安全官的职责范畴，但更多的利益相关者也务必要了解这些工作的相关性和重要性。

全速前进?

面对规模竞争的压力，企业领导人通常过于关注数字化转型的结果，而无法充分考虑网络安全的风险。这种情况下，就算击败竞争对手，也会产生具有明显盲点的隧道视野效应。

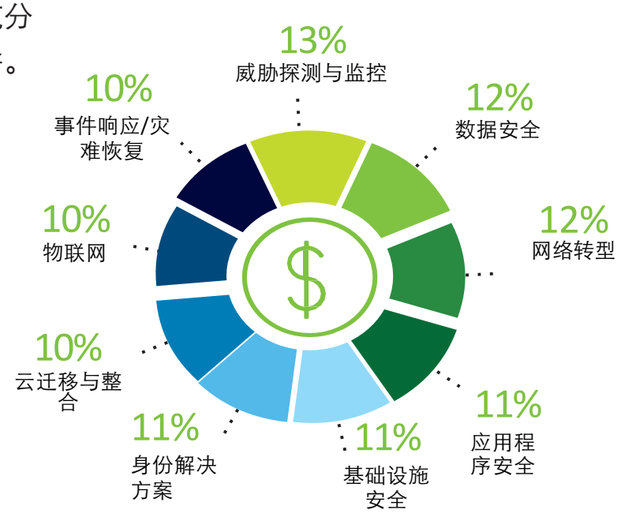
随着网络安全问题渗透到从客户触点到智能工厂以及员工的远程设备的各个角落，IT部门的职责不再局限于管理防病毒软件和密码安全，它不仅要保持网络运行，更需要更广泛、更深入的思考。

目前，首席信息安全官需要获得授权去影响所有业务线、收集整个企业范围内的信息并与董事会和高级管理层直接对话，还要投入资源和人力充分保障企业最重要的战略重点和资产。

这在面对首席财务官时很难说清楚，因为对大笔网络安全投资的结果通常是毫无结果。这也意味着零网络事件是花费很多的。那么，首席信息安全官该如何规划其网络安全预算?2019年，首席信息安全官和首席信息官表示他们的网络预算平均分配给各个网络安全项目。2021年，这一情况并未改变，受访者再次表示网络安全预算进行了类似的平均分配。首席高管应认识到，管理网络风险没有一劳永逸的解决方案。

因此，网络安全预算正在增加，着重倾向于威胁情报、监测和监控、网络转型以及数据安全。在全球范围内，首席信息安全官和首席信息官正不断投资于云上规模化网络解决方案；网络/技术韧性；人工智能驱动的威胁评估和识别，以构建企业的网络防线。

企业以近乎平均的网络安全预算分配应对各领域的风险



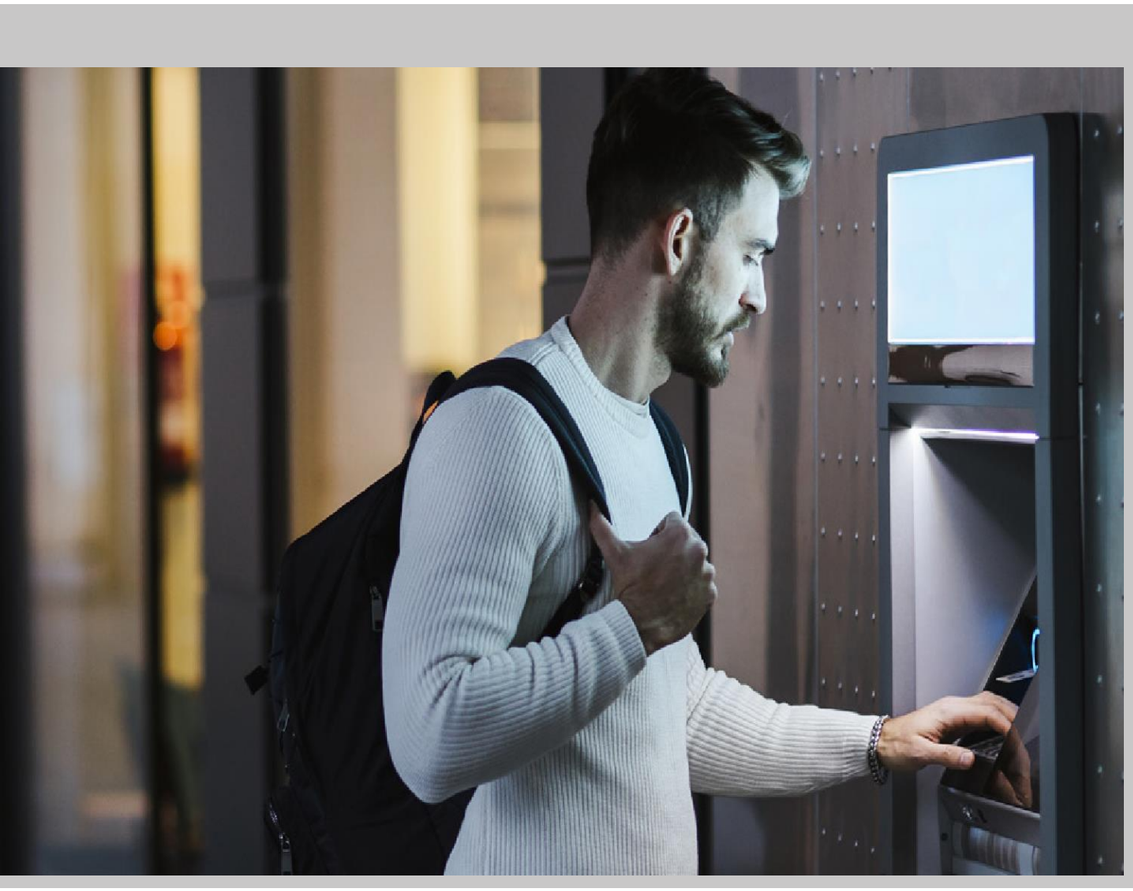
构建合适的网络安全团队

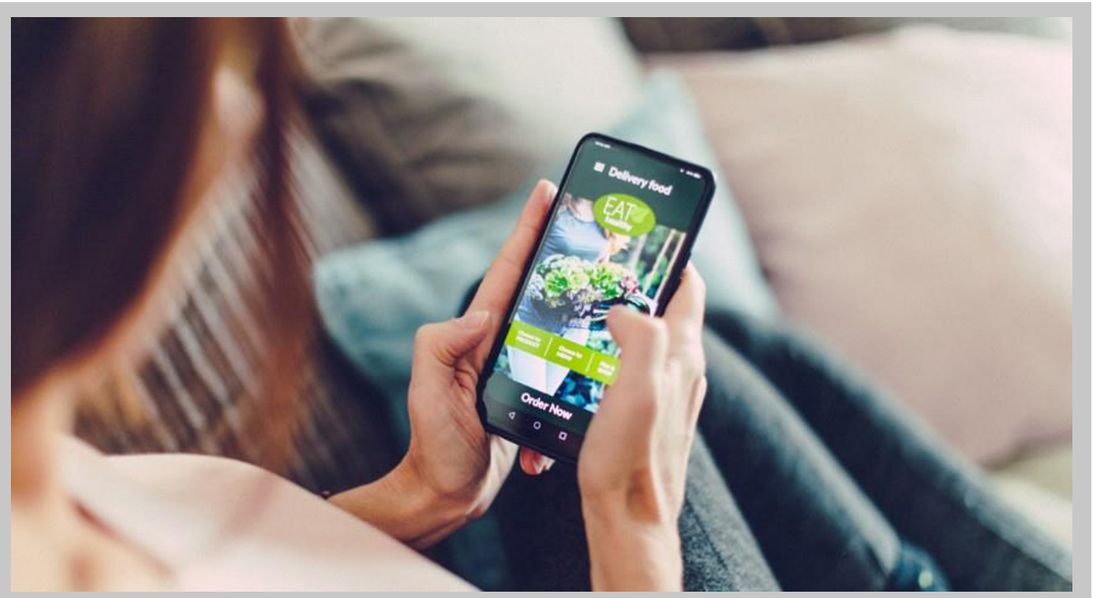
期望董事会成员或首席高管成为网络安全专家并不现实。但他们却可作出招聘决策，组建网络团队，帮助其了解网络安全问题，并以其能理解的方式提供相关信息。

个性化体验甚或侵犯权益？合乎道德地使用个人数据

我们都期望个性化、有针对性的体验，从食品配送到出差旅行和医疗保健的一切都能基于我们过往的互动轨迹。我们不希望自己总有被营销人员跟踪的感觉，无休止的硬塞一些我们不感兴趣的优惠券。

公司如何管理客户数据，在保护隐私的同时实现在线连接和个人体验，可能是盈利或亏损，乃至能否长期存续的差异因素。





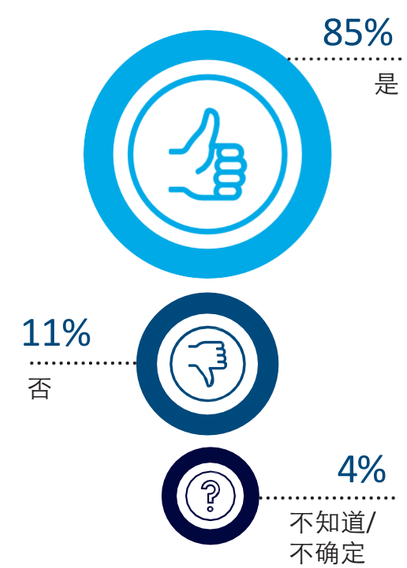
隐私设计

对于每一个面向客户的项目，务必要在项目最初考虑隐私和安全。反思与客户建立这种程度的接触度对业务模式的重要性，并仔细思考提供恰当服务水平所需的信息类型以及此等信息谁可以访问、如何储存和保护方式。在问到首席营销官是否能够衡量并证明对全球数据隐私条例的遵守情况时，绝大多数受访者（85%）回答可以。

避免数据膨胀

仅仅收集大量数据希望未来有用，这是对资源的浪费并可能导致失败。若客户没有看到明显的好处，他们是反感提供个人信息的。收集并有效使用个人数据打造真实、个性化和人性化的体验将推动企业发展。但另一方面，所拥有的数据越多，面临的风险也越多。关键在于如何平衡。在被问及是否收集个人数据时，受访的首席营销官中有一半表示收集数据打造个性化客户体验更为重要，另一半则表示不收集个人数据以防数据泄露更为重要。

您是否能衡量并证明对全球数据隐私条例的遵守情况?



价值与信任

如今，人们意识到其个人数据拥有内在价值。他们将交出个人数据视为一种投资，并想要知道有何回报：提供个人数据应使生活更加便利。像任何有价值的东西一样，个人数据必须安全可靠。同时，人们对机构提出更多要求，谋求选择如何及何时使用其个人数据。当公司可信的兑现他们的承诺时，客户关系会加深。

客户行为反映出他们对公司的信任程度。高信任分数与回头客密切相关——当客户认为公司诚实可靠，他们的复购率会上升540%，此外，还会在社交媒体上强烈支持。因此，受信任企业的表现大大优于其他企业，例如，受信任企业在过去一年的抗风险能力高出两倍。

根据我们的调研，91%的首席营销官认为其企业“极好”或“还行”地平衡了收集数据和建立信任。如此高的信任度让人不禁要问，其他首席高管也这么认为吗？这当然表明首席高管间需采用协同方式，以确保盲点不会被忽视。

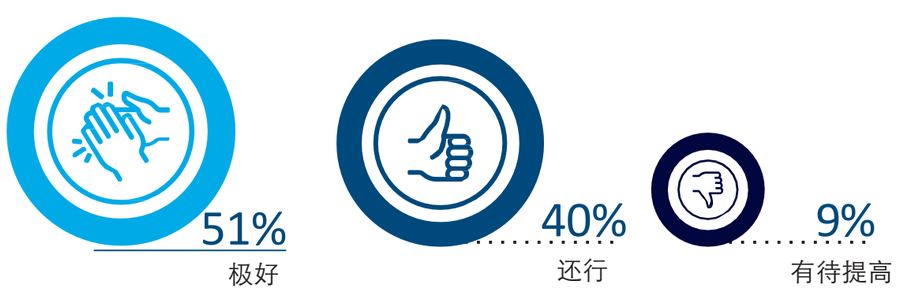
道德监管

消费者越来越愿意购买有绿色环保产品公司的产品，并积极响应社会问题。同时，他们也担忧公司如何使用其个人数据。

传统而言，公司听从监管机构的指引哪些该做哪些不该做。虽然遵守世界各地的各种法律至关重要，但如果无法解释分享数据的目的，仅仅假设人们愿意分享个人数据已远远不够。另外，解释要使用通俗易懂的语言。

无论公司处于哪个地区，那些将信任植入公司DNA并清楚地传达愿意遵守客户隐私权保护的公司将得到客户的忠实拥护。公司应编制简洁明了的用户协议，便于用户访问、删除或迁移其个人数据。当客户看到公司认真考虑数据政策并公开数据足迹时，他们更愿意与公司分享数据。

您认为贵公司营销部门在收集数据和建立客户信任之间的平衡如何?



*Deloitte HX TrustID research，2020年10月至2021年6月

让信任成为指明灯

阐述您试图打造的客户体验场景，以及为此所需（和不需要）的数据。企业中的相关主体都对建立客户信任负有责任。

01 以隐私设计开始

02 使用所收集的数据，不收集不需要的数据

03 打破孤岛，使信息变得可访问并可在企业中自由流动

04 建立无缝体验并坚守诚信

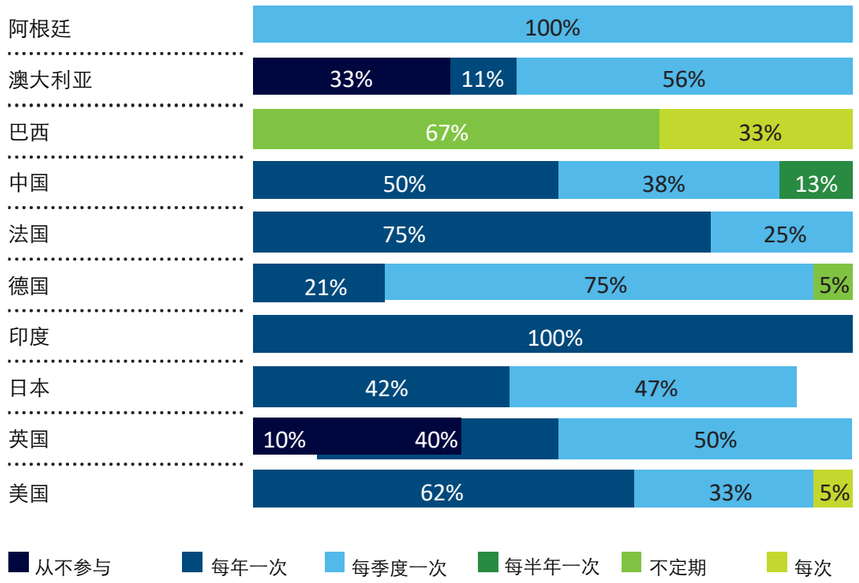
05 如果/当发生数据漏洞，则利用这个契机从错误中学习并建立更多

06 让公共关系部门参与所有工作

打破数据孤岛

首席营销官和首席体验官往往先根据品牌和营销要求制定决策，最后才与首席信息安全官确认数据收集得当与否（通常答案为“否”）。不同团队对数据收集持不同看法。一个团队认为其工作需要收集尽可能多的数据，而另一团队认为只需收集必要的数据并加以保护。而最佳实践是协力研究如何在收集用以提供无缝体验所需信息的同时，尽可能地降低公司及其客户所担风险。在利用数据将客户体验点连接起来之前，企业应有将数据孤岛链接的人才。反之，在设计隐私政策和沟通机制时，企业也应引入市场营销人才。这对品牌营销和信息传递而言日益重要，而他们可以提供帮助。

您多久参与一次贵企业的网络安全事件响应计划和测试?



关于数据泄露

尽管各企业采取了最高级的防范措施，数据泄露事件仍层出不穷。明智的做法是警惕数据泄露随时可能发生，并未雨绸缪。措手不及只会让情况变得更糟。您的事件响应态度将诠释贵司品牌的声誉。您应与您的网络安全团队一起开展事件响应计划演练和数据泄露场景测试，并协力制定恢复计划和相关沟通策略。

根据我们的调查，各首席营销官表示正全力协作其网络安全团队， 其中46%表示他们会每季度参与一次此等计划和测试。全球响应程度不一，较之于其他国家，阿根廷、德国和澳大利亚的首席营销官与其网络安全团队的协作程度更高。

当发生泄露事件时，您有义务将所发生情形充分告知客户。清楚地向客户简述您所采取的响应举措，并选择最恰当的信息传递方式：是否有必要由首席执行官亲自致函，公司提供礼品或给予其他补偿?

即使事态严峻，沟通得宜也可以加深与客户的关系。将客户利益放在首位，处理好棘手情况，可以帮助您的声誉迅速反弹，并取得客户更深的信任。

> “客户不会像企业那样从隐私、安全和身份等方面担忧其数据使用，而是会想‘该公司是否考虑到了我的最大利益?他们使用我的数据是对我有利还是对他们有利?他们是否在竭尽所能地保护我的个人信息？’”
>
> ——德勤网络安全服务全球数据与隐私保护领导人ANNIKA SPONSELEE

保护没有边界的网络世界

在传统环境中，IT资源均包含在明确的网络边界内。外部流量不得信任，而所有内部流量得以信任。现在呢？我们生活在一个高度互联的世界，一切事物的联系都日益紧密。对于大多数现代企业而言，网络边界基本上已经消失。

72%的受访者表示，其所在企业仅在去年就经历了1至10起网络攻击和数据泄露事件。如今企业面临的挑战是“如何才能完全消除固有的信任”？这对我们如何建立现代安全架构而言是一次颠覆性变革。幸运的是，零信任安全架构能够满足要求。

是什么推动了向零信任的转变？

01
数字化的快速发展导致IT的复杂性和成本提高。

02
如今，移动办公人士日益希望能够不受地方和设备限制开展工作。

03
数字产品和服务的发展转向云端。

04
对更优质便捷的业务协作和供应链集成的需求。

05
攻击方变得更加老练，能够入侵当前的网络防御系统。

关于零信任

零信任并非一种技术或单一的解决方案，而是一套基于“持续验证，从不轻信”这一基本原则的安全架构策略。其理念是将传统的基于边界或“城堡与护城河式” 的安全管理方式，转变为按需在单个资源与客户之间构建信任的安全管理方式。在零信任模式下，用户将基于经不断重新验证的内外部因素建立可信连接。

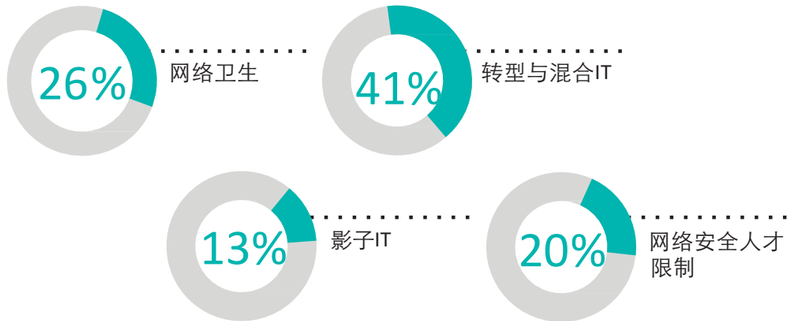
“当前存在一种误解，即认为采用零信任理念需实施大规模的‘淘汰和取代’计划。其实退一步，战略性地考虑采取迭代和增量法来实现你的目标状态，这点至关重要。”

——德勤网络安全服务美国零信任安全架构领导人ANDREW RAFLA

现状

本报告概述了首席信息官和首席信息安全官在企业网络风险管理方面所面临的挑战。其中最大的挑战是转型与IT混合架构中的网络安全清洁、人才限制和影子IT设施时代的到来。随着数字化转型加速，这些挑战只会变得愈发复杂。我们必须重新构建能够支持加速数字化转型的安全架构。现在是行动的时候了！

以下哪项是贵企业在基础设施网络安全管理方面所面临的最大挑战?



踏上零信任之旅

大多数企业已经有意或无意地走上了“零信任”之旅，所采用方法因战术、架构或战略的主导程度而不同。虽然零信任适用于所有行业和领域，但并不能提供一个 “万能”的解决方案。零信任是一项历时多年的倡议，是一次打破业务、IT和各网络领域之间数据孤岛的变革。任何零信任之旅都将面临荆棘阻碍，需要整个企业给予强有力的领导层支持、投资和认同才能确保成功。

您需要考量与企业相关的业务驱动因素、现有功能和用例。牢记网络安全基本原理至关重要：您想要保护哪些资产？这些资产在哪里？谁（身份）和哪些（设备）应能够访问这些资产，且须满足哪些条件？要回答这些问题，企业需确定执行IT资产管理和数据治理功能的优先顺序，以了解自身资产和数据的类别和重要性……并由此创建访问控制策略 。然后确定您的目标并将其嵌入端到端策略，这是实现所期望业务成果的最可靠方法。然而，这并非易事。受访者纷纷表示“数据管理/边界和复杂性加剧”是在企业在网络安全管理中面临的最大挑战。

零信任不仅仅是一项技术解决方案，更是一次文化变革。其对整个企业的影响不可小觑。沟通、员工专业培训、认知和运营流程调整等软因素是取得成功的关键要素。总而言之，此等计划需要结合所有利益相关者的承诺以制定与业务契合的战略，以及强有力的领导、专用架构、技术工作组和可落地试点计划的支持。

前行之路

科技巨头正引领零信任的成熟度之旅，并应用这些原则开发、运营和提供安全服务。其他领先企业正采用零信任战略以支持业务优先事项、数字化转型和企业风险战略。在对自身架构进行现代化升级时，了解领先企业如何创新及实现规模化部署也有助于您加速数字化转型。毋庸置疑，变革已然开始。您越早开始向零信任过渡，此次旅途就越安全。最好是坐在驾驶座里，决定您的目的地……实现零信任正当时宜。

巨大优势

通过降低运营复杂性和简化生态系统集成，它可以：

- 改善客户体验
- 提高业务敏捷性
- 提升业务弹性
- 减少威胁面
- 实现成本节约
- 优化与业务合作伙伴的协作
- 加速上云之旅

“是时候充分利用零信任原则，构建能够跟上并实现数字化转型的现代安全架构了。”

——德勤网络安全服务全球零信任安全架构领导人MARIUS VON SPRETI

“许多企业忽视了连接其环境中现有技术设备所带来的风险。整个生态系统的受攻击面正在增加。”

——德勤网络安全服务全球网络新兴技术领导人DANA SPATARU

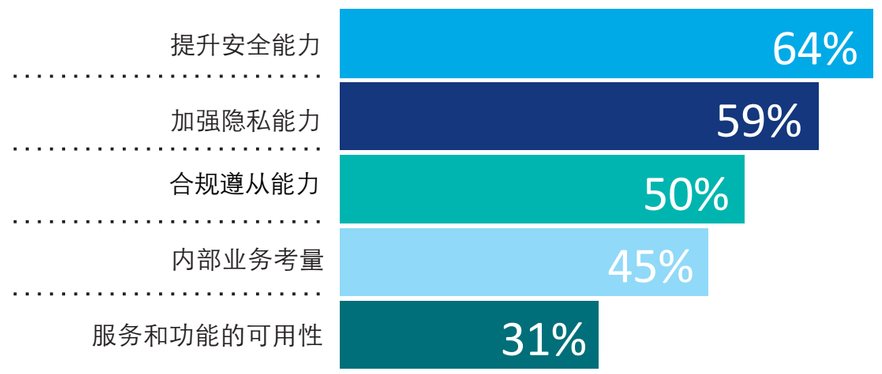
连接新兴技术领域

大众目光往往聚焦于量子计算、5G和数字孪生等前沿技术，但在制造业应用了数十年的既有技术（如运营技术）也属于新兴技术范畴。

无论一项技术是全新问世或是部署已久，“新兴”是指它与互联网的连接，也指现实世界与数字世界以几乎任何可以想象到的方式实现互联。我们正见证一场彻底颠覆医疗设备、交通运输及农业等各个行业的数字化转型。数字化转型不仅改变了几乎所有事物的制造及使用方式，也带来了前所未有的安全风险。

首席信息官和首席信息安全官对未来三年将推动其采用新兴技术的因素进行了排名，提升安全能力位居榜首（64%），其次是加强数据隐私能力（59%）和合规遵从能力（50%）。

以下哪项因素将推动您采用新兴技术?



*受访者可多选适用答案，因此各选项的百分比加总超过100%。

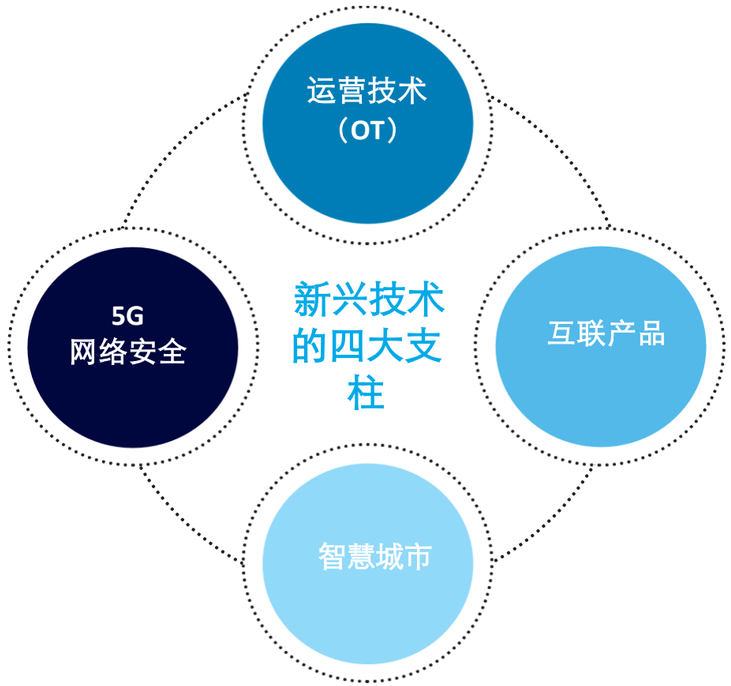
互联互通不断加速

传统上与互联网隔绝的运营技术（OT）领域最近经历了一波又一波的勒索软件攻击。随着越来越多的公司选择远程管理厂房和设备，此等攻击对生产的直接影响引起了人们对互联脆弱性的关注，而新冠疫情更是使得这一情况加剧。

重要的是要清楚，所有的互联生态系统——医疗设备、汽车乃至整个城市——都有类似的风险特征。医疗设备可能是基于医院原有的内部平台而造，而现在借助互联网便可在家使用。经互联赋能的电动汽车有望在全球范围内迅速取代化石燃料汽车。互联汽车需要分散于各地的众多供应商提供零部件，但这些供应商可能并未在其零部件中内置安全机制。随着城市大力推动服务与关键基础设施互联，其与云服务供应商、平台所有者等众多第三方合作亦是势在必行。上述情形均会导致互联生态系统的受攻击面增大、风险倍增以及责任不明等情况发生。

德勤网络专注于以下新兴技术特定领域：

这四大领域涵盖了我们在实践中遇到的绝大多数场景



虽不见，但相连

小型全数字化实体仍可从单一视角监控网络风险。但在短期内，此举对于拥有复杂互联生态系统的大型实体而言已不可取。对此，解决办法是让各方明确其权限下运营流程的安全责任和问责机制。即使没有整体视角，但当各方均高效负责其生态系统的一环，提高其安全性，则整体风险自然降低。

各企业达成整体安全目标的速度因技术类型及其复杂性而异，但核心理念是有效涵盖安全基本要素并安全地共享信息。现在，解决办法很简单。从长远来看，企业应牢记，各区域之间若能保持流程一致，将大大提高效率和效果。越早达成一致性，就能越快达到更高的安全成熟度。集中式和分散式模型均能奏效，但它们最终应该合并为一个综合网络风险视图。

业务核心

从治理角度来看，新兴技术栈或将十分复杂，应委任安全事宜的负责人，得到董事会的认可和支持，不仅有助于获取和管理技术，还有助于建立正确的战略合作伙伴关系。与传统IT不同的是，新兴技术与核心业务紧密相连，得到高管支持将变得更加容易。

举例而言，如果一家制造企业的OT设施遭遇网络攻击，人们很容易看出该问题将很快超出首席信息安全官的解决范畴。随着生产陷入停滞，运营主管即刻便感到担忧，收入损失会令首席财务官和首席执行官感到头疼，负面报导亦会令首席营销官感到困扰等等。

安全即资产

上述情况说明，新兴技术使企业业务管理者对网络安全的影响显著提升。当前市场环境日益互联，若首席执行官想要提升产品销量，构建安全机制可令其产品更具竞争力。企业应将对安全机制的关注重点从成本增加转向价值创造，这将开启如何减少业务中断以推进改进流程的对话。当然，安全机制是必要的，尽管它是讨论基础，但它也是次要论题。

“尽管人们普遍认为，近期发生的重大网络攻击事件是复杂性日益提高所导致的结果，但实际上大多数网络攻击的发生都是由于缺乏基本的安全控制和网络安全清洁计划。这并不复杂。”

——德勤网络安全服务全球网络新兴技术领导人DANA SPATARU

没有万能的解决方案

董事会、管理层以及网络风险管理者纷纷表示，网络风险一直是各行业中排名前三的企业风险。所有行业愈发意识到知识产权和客户信任的脆弱性。

各行各业正纷纷踏上数字化转型之路，而围绕网络安全和诸多地域及其他因素的监管成熟度仍有参差。虽然疫情期间涌现出许多共同主题，如供应链安全和远程办公加速了对零信任安全架构的需求，但目前尚无可适用于所有行业解决网络挑战的万能解决方案。

无论企业路在何方，保持对某些日益关键的领域的关注至关重要。为应对无处不在的网络威胁，许多政府正加大监管力度，部署前沿安全措施已是势在必行。在法规还没有涉及的领域，技术的日益互联和个性化也迫使生态系统在安全基础上重新构建。最后，意识到所有行业的脆弱性可以促进信息共享——适应和学习其他行业的做法将变得愈发重要。

监管激增

网络攻击已经导致某些行业的监管部门频繁出台新政。2021年5月，美国东海岸最大的成品油管道运营商Colonial Pipeline遭遇勒索软件攻击，该事件催生出一项要求能源公司加强网络安全的新行政指令。

在能源资源和工业（ER&I）领域，升级网络防御的紧迫压力与其他长期行政指令（如脱碳）并存。例如：由于时间紧迫，美国近期修订的2035年目标——能源领域的转型——将利用大规模的数字化加以实现。这包括转向5G和部署一系列互联技术，而这些技术本身也对网络安全提出更高要求。

个性化服务越多，风险越高

在生命科学与医疗领域，一种与患者直接交互的新型医疗服务模式正推动加强网络安全的需求。医疗服务提供商为监测患者的治疗进展，以及生命科学公司为提供以患者为中心的服务，他们使用远程设备和应用程序以改善健康结果，此举引发了人们对数据和隐私保护的担忧。

这种对应用程序的监控和使用可以快速积累汇集数据，赋能企业创建基于云的数据湖以收集有用信息，从而优化研发、治疗与支持以及产品发布流程并提升患者便利性。这些技术进步均可能带来网络安全威胁。生态系统的设计和构建需要考虑到数据的保护、加密、匿名化处理以及防止泄露。

总体而言，比起应对各地区不同监管要求这一难题，全球生命科学公司更担心遭遇网络攻击。对于企业而言，与客户沟通过程中建立并维持客户信任非常重要；对于业务而言，保护知识产权亦是至关重要。

知识共享

无处不在的网络威胁和疫情期间暴露出来的安全隐患改变了行内的信息共享方式。尽管遭遇网络攻击事件必然会导致声誉受损，但有企业认为主动公开事件详情也具有价值和意义，可以补救并修复品牌声誉。企业已经意识到，闭口不谈网络安全不仅不会带来竞争优势，甚至还可能危及整个行业。

各国政府已经认识到采取集体防御的重要性，并帮助建立了旨在共享信息的公共的/私人的合作伙伴关系（如美国成立了信息共享与分析中心(ISACs)）。其次，各大企业首席信息安全官期望相互学习。虽然他们更多是与同行交流，但无论是金融服务、石油天然气行业，还是生命科学、制造业等行业，均开始出现跨行业交流。此外，拥有丰富的经验的首席信息安全官们也经常从一个行业投身到另一行业。我们希望在不久的将来看到更多跨行业和地域的交流与分享。

“无论生命科学机构、大型银行还是能源公司，其真正面临的难题是选择关注重点。绝对安全是不切实际的幻想。领导层必须就如何划分资产的保护优先级做出基于风险的明智决策，并果断行事，然后不断地重新评估这些决策，因为企业内外的环境并非一成不变。”

——德勤全球客户与行业领导人SIMON OWEN

深度洞见

随着数字化转型渗透到企业方方面面，企业愈发清晰地意识到，其虽能推动人才和流程创新，却也能放大和传播风险。在企业被迫应对前所未有的全球挑战之际，德勤所开展的网络安全调研具有一定的借鉴意义。

世界风云变幻。混合办公模式正在成为“新常态”，云部署对各大企业而言日益重要，设备和应用程序互联互通不断加速。

除了在网络边界不明的生态系统中争取更大的可见度，我们别无选择。无论是业务中断、声誉受损还是股票估值缩水，所引致的风险都过高。正如复杂性是问题所在，解决方案也绝不简单。

责任上达

显而易见的是，未将网络安全纳入业务的企业可能错过数字化转型带来的机遇，也更易遭受攻击。

对此，我们关键建议就是充分赋权首席信息安全官，这意味着其直接汇报对象为首席执行官。此外，企业还必须确保首席信息安全官职责能够覆盖所有业务线。反之，首席信息安全官亦须以董事会易于理解的方式提供风险评估报告。但是，首席信息安全官不仅仅是汇报职责上达，其还需自始参与新业务的发展，以确保落地的系统实施适当的网络安全治理。

跨越孤岛

既然技术支持企业内部信息可以自由流动，我们也应展开信息交流。打破根深蒂固的数据孤岛，使各业务部门在网络安全领域展开合作至关重要。推动战略部、产品开发部、合规部、信息技术部以及营销部召开会议，从而在各项新计划伊始便了解所需的数据资产以及相关的安全和隐私要求。在计划之初便考虑到安全和隐私问题，防患于未然，也是避免后续问题的最佳做法。

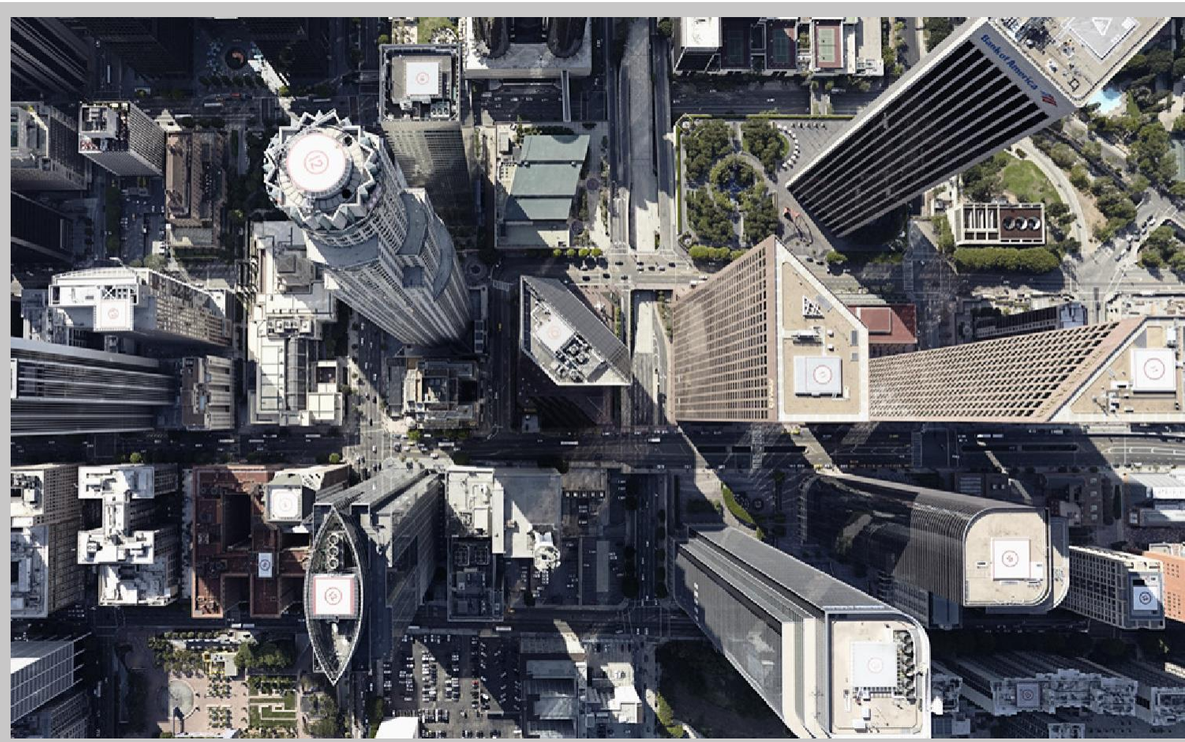
实施零信任安全架构

技术和组织复杂度高是既有事实。依靠过时方法验证用户和其他实体之举实不明智，很容易被黑客利用并带来可怕后果。幸运的是，现在我们可以将风险持续评估能力和访问控制实时审查能力集成于复杂的安全架构。

零信任既是一种技术创新，也是一种文化创新。改变人类自身行为离不开沟通与培训。零信任能够确保创新及业务战略得以安全实施，更令每个人都意识到其在推进数字化转型方面可带来持续益处。

安全即资产

数据是数字化转型的命脉。认识到数据的功能性（即业务成果和客户体验的驱动力）固然重要，但了解其如何创造长期价值也同样重要。具有出色数据治理、全面隐私政策和强健的安全机制的公司更能赢得客户和业务合作伙伴的信任。尽管企业很容易将网络安全预算仅仅看作一项开支，但在高度互联的今天，其对品牌和股东价值保值有着举足轻重的影响。实施安全管理并非一个项目，而是一个谨慎处理数据、通讯和端到端业务交互的承诺。



知识共享

虽然网络安全管理并无万能的解决方案，但企业在数字化转型道路上面临的许多威胁具有共通性。随着网络攻击日益常态化，各个行业或地区无一能够幸免，但我们可就如何在事件发生时进行有效处理相互学习。因此，与同行分享经验和知识是全面改善安全环境的关键。

风险与回报

无论您的网络安全预算多或少，采用上述方法将有助于您更高效地利用自身资源。

人们往往过于关注转型所带来的复杂性和大量风险，其实认识到其益处同样重要。当您获得转型的全局视角，体验到混合IT架构为企业带来的敏捷性，赢得客户信任并从容应对复杂性时，您将收获更大的回报。

德勤中国网络安全咨询领导人

薛梓源
德勤中国网络安全咨询主管合伙人
电话: +86 10 85207315
电邮: tonxue@deloitte.com.cn

东区

冯晔
德勤中国网络安全咨询合伙人
电话: +86 21 61411575
电邮: stefeng@deloitte.com.cn

江玮
德勤中国网络安全咨询合伙人
电话: +86 21 23127088
电邮: davidjiang@deloitte.com.cn

石沛恩
德勤中国网络安全咨询合伙人
电话: +86 21 33138366
电邮: nathanshih@deloitte.com.cn

张震
德勤中国网络安全咨询合伙人
电话: +86 21 61411505
电邮: zhzhang@deloitte.com.cn

阎光
德勤中国网络安全咨询合伙人
电话: +86 21 23166282
电邮: alexyan@deloitte.com.cn

北区

薛梓源
德勤中国网络安全咨询主管合伙人
电话: +86 10 85207315
电邮: tonxue@deloitte.com.cn

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

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

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

南区大陆

何微
德勤中国网络安全咨询合伙人
电话: +86 755 33538697
电邮: vhe@deloitte.com.cn

南区香港和澳门

郭儀雅
德勤中国网络安全咨询合伙人
电话: +852 28526304
电邮: evakwok@deloitte.com.hk

Kukreja, Puneet
德勤中国网络安全咨询合伙人
电话: +852 27408898
电邮: puneetkukreja@deloitte.com.hk

鄭若琳
德勤中国网络安全咨询合伙人
电话: +852 22387119
电邮: eicheng@deloitte.com.hk

林普毅
德勤中国网络安全咨询合伙人
电话: +852 21095353
电邮: bradlin@deloitte.com.hk

王凯民
德勤中国网络安全咨询合伙人
电话: +852 22387908
电邮: harrywang@deloitte.com.hk

Deloitte.

德勤

因我不同
成就不凡
始于1845

關於德勤
Deloitte（“德勤”）泛指一家或多家德勤有限公司，以及其全球成員所網路和它們的關聯機構（統稱為“德勤組織”）。德勤有限公司（又稱“德勤全球”）及其每一家成員所和它們的關聯機構均為具有獨立法律地位的法律實體，相互之間不因協力廠商而承擔任何責任或約束對方。德勤有限公司及其每一家成員所和它們的關聯機構僅對自身行為及遺漏承擔責任，而對相互的行為及遺漏不承擔任何法律責任。德勤有限公司並不向客戶提供服務。請參閱 www.deloitte.com/cn/about 瞭解更多資訊。

德勤是全球領先的專業服務機構，為客戶提供審計及鑒證、管理諮詢、財務諮詢、風險諮詢、稅務及相關服務。德勤透過遍及全球逾150個國家與地區的成員所網路及關聯機構（統稱為“德勤組織”）為財富全球500強企業中約80%的企業提供專業服務。敬請訪問www.deloitte.com/cn/about，瞭解德勤全球約345,000名專業人員致力成就不凡的更多資訊。

德勤亞太有限公司（即一家擔保有限公司）是德勤有限公司的成員所。德勤亞太有限公司的每一家成員及其關聯機構均為具有獨立法律地位的法律實體，在亞太地區超過100座城市提供專業服務，包括奧克蘭、曼谷、北京、河內、香港、雅加達、吉隆玻、馬尼拉、墨爾本、大阪、首爾、上海、新加坡、悉尼、臺北和東京。

德勤於1917年在上海設立辦事處，德勤品牌由此進入中國。如今，德勤中國為中國本地和在華的跨國及高增長企業客戶提供全面的審計及鑒證、管理諮詢、財務諮詢、風險諮詢和稅務服務。德勤中國持續致力為中國會計準則、稅務制度及專業人才培養作出重要貢獻。德勤中國是一家中國本土成立的專業服務機構，由德勤中國的合夥人所擁有。敬請訪問 www2.deloitte.com\cn\zh\social-media，通過我們的社交媒體平臺，瞭解德勤在中國市場成就不凡的更多資訊。