亚洲数字原生企业将安全作为实现可持续增长的首要任务

2024/25 技术洞察

执行摘要

数字原生企业 (DNB) 诞生于互联网时代，诞生之初便围绕最新的先进技术建立。

数字原生企业不受传统技术和流程的束缚，他们遍布于游戏、零售和教育等众多行业，随技术的发展步伐迎头向前，满足客户对在线工作、生活和娱乐的需求。

技术研究公司 IDC 表示，到 2026 年，预计 DNB 在技术上的支出将达到 1289 亿美元。

2024 年 3 月到 5 月，Akamai 与第三方研究公司 TechnologyAdvice 开展了一项在线调查，希望了解亚洲地区 DNB 的技术投资优先事项以及导致技术负责人夜不能寐的原因。

来自澳大利亚、东南亚、印度和大中华地区的 200 多位技术负责人参与了此次调查。

亚洲 DNB 的业务重点和技术关注点是什么？这些技术驱动型公司需要他们的解决方案提供商提供什么？是否所有数字原生企业都如出一辙？

无论是因为市场竞争日趋成熟，还是消费者群体快速增长，参与调查的 DNB 中近九成的企业都将在未来 12 个月内优先提高效率和生产力。

行业数据也表明 DNB 在快速采用云技术，两者不谋而合。据估计，2021 年到 2026 年花费在云技术解决方案上的支出增长率为 37%，高于非云技术软件 (16%) 和 IT 服务 (11%)。

此云原生模块化架构围绕独立运行并通过 API 进行通信的微服务构建，使该地区的 DNB 能够快速扩展并满足不断增长的客户数字化需求。

但是，这种情况会很快产生一个复杂的软件、系统和服务集合体，可能导致 DNB 更容易遭受网络攻击。

无论该地区的 DNB 在云技术之旅中处于哪个阶段，他们都敏锐地意识到，在云基础架构性能方面的最大不足是安全性。

实际上，这些企业中日趋复杂的 IT 基础架构可能会成为增强网络安全态势时的致命弱点，因为大多数受访企业认为这项挑战比预算或合规问题更重要。

对于考虑采用云技术或寻求进一步迁移到云端的企业来说，这种技术复杂性不断增加所带来的发展痛点还可能起到警醒作用。

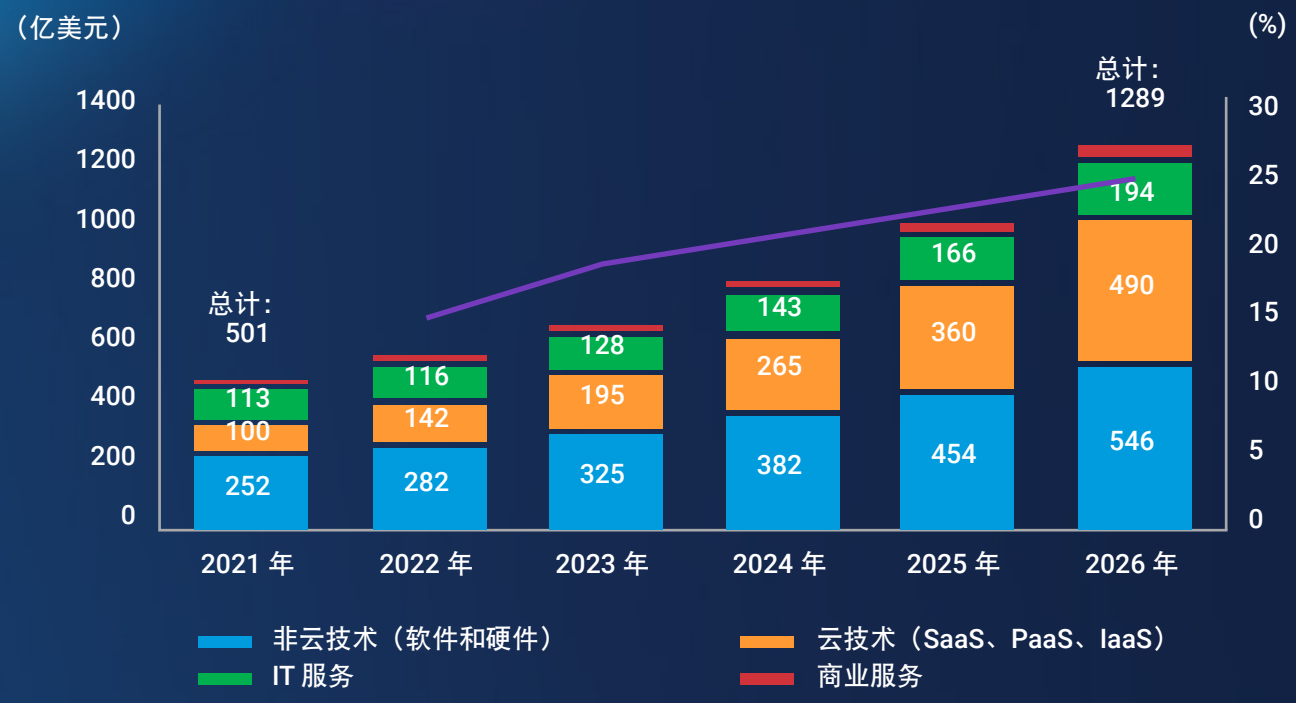
请阅读本文，详细了解降低这些风险的可行策略。

DNB 利用云技术提高速度和效率

《IDC Digital Native Business, Start-Ups and Scale-Ups CIS》研究报告表明，数字原生细分市场是“一个快速增长的新兴企业群体。很显然，他们的技术中心化程度很高，并且会在技术上投入大量资金，因为技术是该行业的业务模式基础”。

无论行业或市场如何，DNB 都会将技术作为一项差异化优势并实现更高的敏捷性。

就其本质而言，DNB 在构建技术基础架构时采用了云原生设计原则。实际上，DNB 在云技术方面的支出越来越多，预计 2021 年到 2026 年的增长率将达到 37.3%。



所选细分市场增长率

- 云技术（SaaS、PaaS、IaaS）的年复合增长率为 37.3%
- 非云技术（软件和硬件）的年复合增长率为 16.7%
- IT 服务的年复合增长率为 11.5%
- 商业服务的年复合增长率为 10.4%

市场总体年复合增长率

20.8%

资料来源：IDC 于 2023 年 4 月 19 日发布的新闻稿“Asia/Pacific Digital-Native Business Tech Spending from 2022-2026 to Grow at a CAGR of 20.8% and Hit US$128.9B in 2026, IDC Forecasts”

DNB 技术基础架构围绕微服务的可组合架构构建，能够实现灵活性、敏捷性并缩短产品上市时间——这对于跟上数字领域的快速增长步伐至关重要。

该调查显示，该地区中有四分之三的 DNB 都在部署云技术，因为他们优先提高效率和生产力。

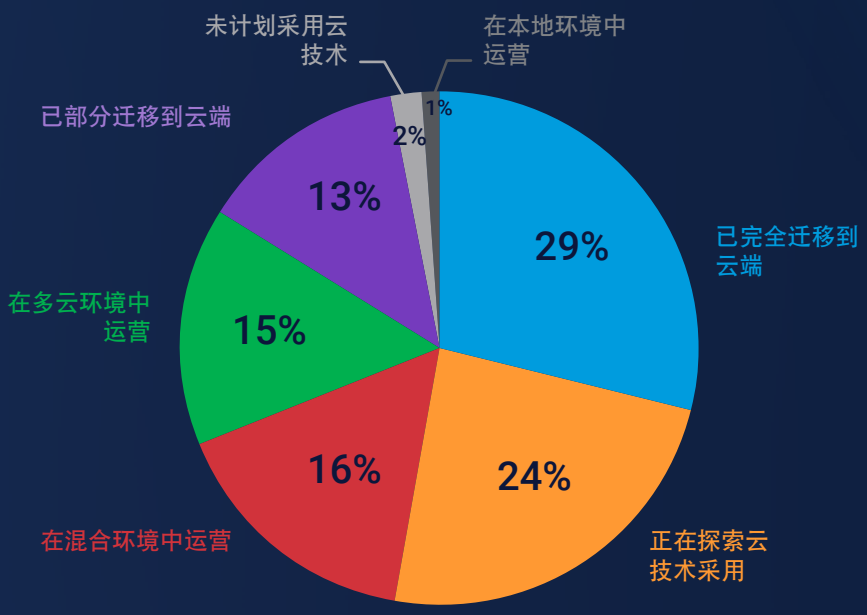
共有 74% 的受访企业已完全迁移到云端，或者正在采用云技术。

但 26% 的受访企业尚未计划采用云技术，或者仍然处于探索阶段，该情况在整个地区都保持一致（在澳大利亚、印度和东盟国家，相关比例分别为 19%、20% 和 29%）。

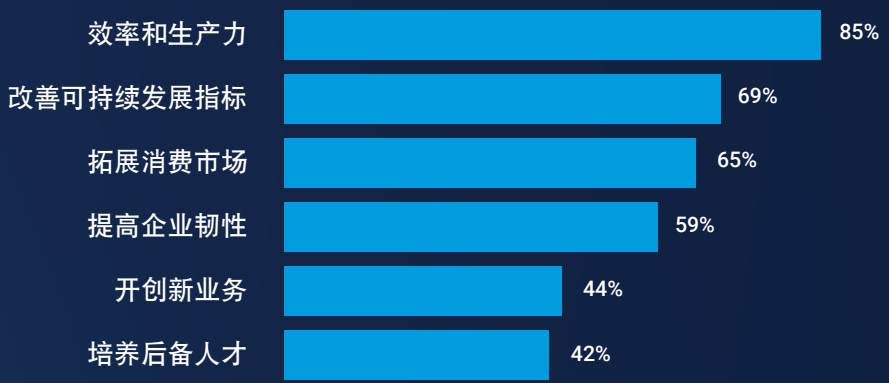
之所以会出现这种不愿意采用云技术的局面，其原因可能在于高度监管行业中的大型现有企业，以及长期以来对云技术保持谨慎态度，这继续阻碍着云技术的采用。

但随着 DNB 加大对云技术的投资，这种情况正在得到缓解。云技术支出的高增长率证明了这一点。

贵企业处于云技术采用之旅的哪个阶段?



未来 12 个月的首要业务重点



为网络生活保驾护航

人们常说的是 DNB 如何精通技术。但这种精通可能仅限于专业领域。

虽然 DNB 可能诞生于云端，但他们也可能难以充分发挥云、数据和人工智能 (AI) 等新兴技术的全部潜力。

我们将受访企业在云迁移过程中遇到的挑战与他们在云技术之旅中所处的阶段进行了对比。

无论是已完全迁移到云端的受访企业，还是仍在探索云技术采用的受访企业，都很难对花费在云技术方面的支出一清二楚。

虽然大多数云服务提供商的定价是透明的，但其费用明细可能很复杂。DNB 需要掌握正确的知识和时间来预测并解读微服务和多云部署的费用，这些服务和部署会基于各种因素而进行不同的扩展。例如，可扩展性事件的驱动因素是什么——最终用户的需求还是流程之间的信息传递？

在云迁移过程中遇到的三大挑战

	管控安全隐患	选择合适的云服务提供商	评估技术可行性
已完全迁移到云端	45%	53%	57%
正在探索云技术采用	63%	62%	52%
在混合环境中运营	74%	49%	54%
在多云环境中运营	50%	44%	47%
已部分迁移到云端	45%	41%	41%

其他挑战：
了解云速度分配、确定要迁移的应用程序的优先级、调整最佳实例的规模/选择最佳实例、评估本地成本与云计算成本、缺乏专业技术知识、了解应用程序依赖关系

这促使 DNB 转而选择了定价更清晰且不影响性能、可靠性或支持的云服务提供商。

但是，无论 DNB 处于云技术之旅的哪个阶段，无论他们是在混合环境中运营、在多云环境中运营还是已部分迁移到云端，管控安全隐患始终是一项艰巨的挑战。

实际上，大多数受访企业目前都将安全性视为云基础架构中的最大不足。

Akamai 的定价简单、透明，出站流量费用低廉，每个月都会提供充裕的出站流量额度，并会提供相关工具来最大限度地优化数据中心和云流量分载能力。

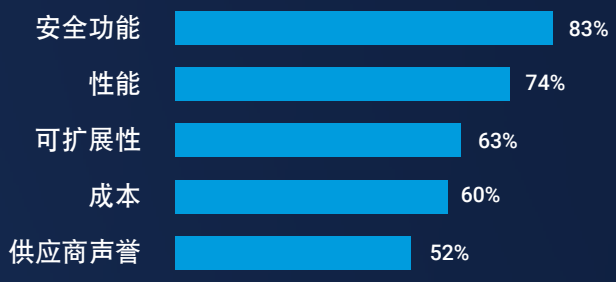
总之，这些对企业而言都意味着更多的机会，可助力他们利用 Akamai 的全球影响力来优化数据密集型和流量密集型应用程序的成本。

选择云服务提供商时，安全功能甚至比性能、声誉、可扩展性和成本更重要。

您认为云基础架构的性能或功能中存在的最大不足是什么？

	安全性	网络延迟	数据存储和检索	计算资源
已完全迁移到云端	65%	65%	67%	47%
正在探索云技术采用	81%	58%	67%	62%
在混合环境中运营	74%	66%	49%	46%
在多云环境中运营	84%	66%	66%	63%
已部分迁移到云端	69%	62%	62%	24%

选择云服务提供商时的考虑因素



技术优先的思维方式——DNB 的致命弱点?

对于 DNB 来说，这便是技术有利有弊之处。

大多数受访企业表示，复杂的 IT 基础架构是增强其网络安全态势时遇到的最大挑战。

数字原生企业采用数字原生设计原则，这些原则高度重视可组合的微服务和用于连接他们的 API。

这些 API 可以加快技术部署速度和上市速度，使 DNB 能够快速迭代和交付功能。

但是，当与各种服务相关的开发者没有动力专注于 DNB 的运营时，这种速度和可组合性便会以复杂性为代价。

安全团队和技术会发现这是一项挑战，因为大多数安全工具不支持混合环境，而且嵌入式云安全模式往往只关注提供商的云。

例如，由于游戏开发需要数年时间，因此游戏提供商热衷于和身为可信赖合作伙伴的云基础架构提供商合作，而不是与供应商合作。

游戏公司及其开发团队需要深入了解云计算的各个方面，包括性能、资源分配、延迟、吞吐量以及可预测的定价和计费透明性。

对于喜欢密切监控与直接开发或升级游戏无关的任何运营费用的游戏提供商来说，随用随付和按需付费的分布式云计算基础架构极具吸引力。

该调查的结果突显出 DNB 面对的是日益复杂的 IT 基础架构，这会影响他们的企业网络安全态势。

增强网络安全态势时面临的最大挑战

	复杂的 IT 基础架构	当地合规要求	缺乏拥有相关技能的人员	预算限制	快速变化的威胁
已完全迁移到云端	43%	7%	13%	12%	25%
正在探索云技术采用	37%	6%	10%	27%	21%
在混合环境中运营	49%	3%	9%	23%	17%
在多云环境中运营	59%	13%	13%	6%	9%
已部分迁移到云端	31%	7%	17%	14%	31%

在风险与回报之间取得平衡

现实证明：在云之间应用一致的安全策略困难重重。

创立时间短的 DNB 可能会对云技术给他们带来的实现速度感到兴奋，但随着企业的发展成熟，DNB 必须在每次技术创新中实现风险与回报的平衡。每项创新技术都会增加一层复杂性。

那么，如何在上市速度和客户采用与安全性、合规性以及治理之间取得平衡，以避免出现违规或滥用?

无论 DNB 处于云技术之旅的哪个阶段，这始终都是增强网络安全时面临的首要挑战。

> *Akamai Connected Cloud 是一个采用开源和多云架构的开放式平台。该架构旨在让开发人员能够轻松利用他们想要的应用程序和软件以及他们所需的服务，以便为全球可扩展、区域优化的低延迟工作负载提供支持*

云技术本身已从仅提供基础架构转变为提供包括基础架构管理在内的全方位服务。

运行云原生基础架构会带来集中风险以及复杂的基础架构挑战。

以下是一些需要考虑的因素，适用于云技术采用之旅的任何阶段：

采用多云策略

各企业应采用多云方法来避免供应商锁定、增强灵活性并优化云服务使用。

由 Forrester Research 对 IT 负责人进行的调查显示，对云服务供应商的首要要求是具备从云到边缘的部署和执行能力。

对特定供应商的集中依赖会减少未来的技术选择，并让供应商能够对企业的技术未来施加重大影响。

利用一个不可知的分布式平台，数字原生企业便能够无缝、快速地访问原始数据，并从分布在多个系统上的数据中获得见解。

定期审查和迭代

定期审查云成本，以分析和优化云支出、确定可节省成本的领域并优化资源使用。

使用监控数据和实施分析来确定需要优化的领域，例如资源分配、成本管理和安全改进。

定期监控和优化能够确保您从云投资中获得最大的业务价值。

实施云治理框架

依赖于特定云服务提供商的应用程序（和业务流程）越多，云服务问题的潜在影响范围就越大，这可能会加剧对业务连续性的担忧。

制定并实施云治理策略，以有效管理云资源、确保合规性并控制成本。

此模式应包含访问控制、安全措施、成本管理及合规要求。明确的治理模式有助于在整个企业内保持一致性和最佳实践。

此外，不同的监管机构对集中风险的处理方法可能有所不同，因此各企业也可能无法满足这些机构就应对集中风险提出的监管要求。

优先考虑高级 API 安全

在连接非云、云和多云架构时，API 是 DNB 的核心。

通过连接内部应用程序、加快与业务合作伙伴的流程以及向使用方提供数据服务，API 使 DNB 在连接性、生产力和敏捷性方面更上一层楼。

为了追求速度和技术驱动型创新，涉及 API 的应用程序和业务流程的启动及部署速度往往比安全团队评估相关态势的速度更快。

配置错误和漏洞，加上缺少 API 安全专业知识，会为创新型 DNB 带来潜在的网络威胁。

实际上，另一项对 631 位网络安全专业人士的行业调查发现，二分之一的开发人员会花费一半的时间来重构和修复 API。

*受 Akamai 保护的流量中有 **31%** 是 API 流量。Akamai 提供了相关工具，以通过集成的用户体验优化功能对您的应用程序和工作负载保持一致控制。*

亚洲地区的 DNB 始终将 API 安全性放在首位，以确保业务的可持续增长。

无论是在澳大利亚拓展市场，还是在印度和东盟国家扩大市场份额，DNB 都优先考虑将高级 API 安全作为首要的网络安全投资领域，随后才会考虑 Web/应用程序安全和反网络钓鱼技术。

将以下网络安全投资领域按最重要（顶部）到最不重要（底部）的顺序进行排序

1. 高级 API 安全
2. Web 应用程序安全
3. 反网络钓鱼技术
4. 分布式拒绝服务 (DDoS) 攻击抵御
5. 与 Zero Trust 相关的技术

API 的安全性出现问题的原因

使用 API 的关键业务流程的快速部署 + 缺乏对 API 的监测能力 = 错误配置或易受攻击的 API

从 Akamai 的流量数据来看，制造业在整个亚太地区及日本遭受的 API 攻击占比最高。

导致这种情况的部分原因在于，这一关键基础设施行业通过 API 建立的连接越来越多，并且供应链中断的可能性也较高。

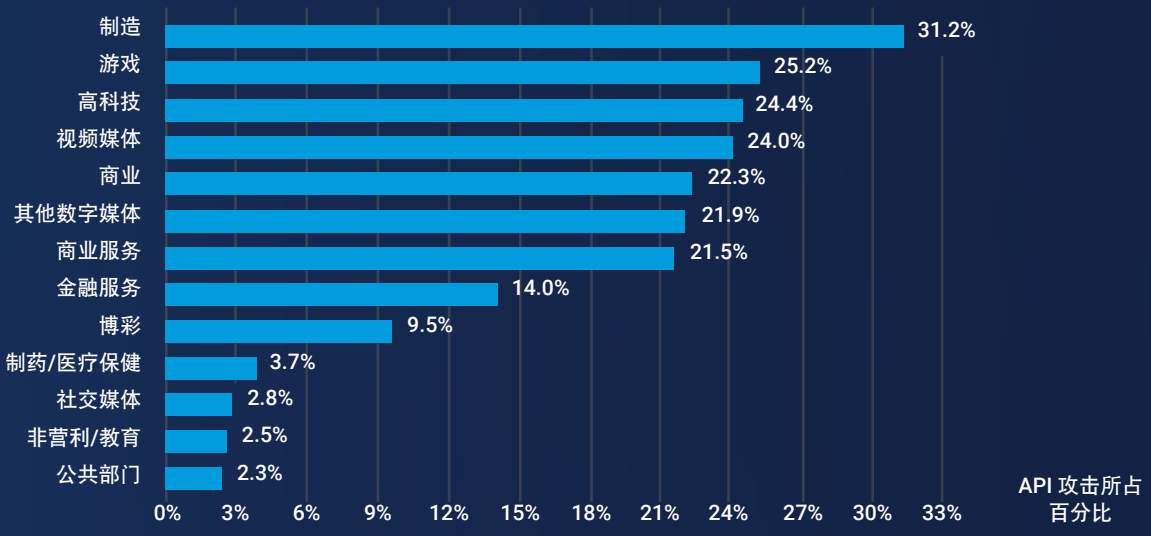
另一方面，游戏、高科技、视频媒体和商业等数字化驱动型行业也成为了 API 攻击者的目标。

数字原生企业遭受攻击最多的原因可能在于，其业务有很大一部分依赖于 API、他们部署到云端的基础架构最多，并且与传统公司和架构相比，他们对网络钓鱼、帐户入侵和勒索软件的吸引力更大。

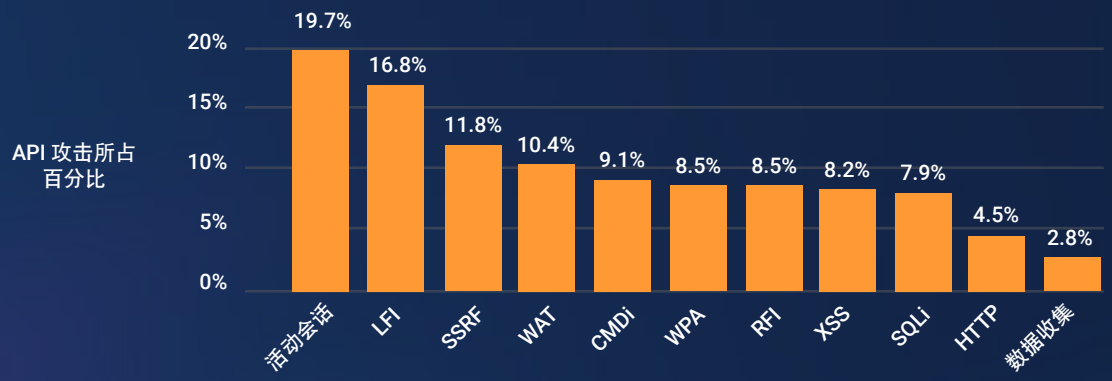
本地文件包含 (LFI) 仍然是头号 API 攻击媒介，但我们通过 2023 年的数据发现了更多攻击媒介，例如命令注入 (CMDi) 和服务器端请求伪造 (SSRF)。这些攻击媒介对易受攻击、配置错误或未记录的 API 构成了重大风险。

爬虫程序请求也是值得关注的一个领域。在同样的 12 个月报告期内，超过 2 万亿次的可疑爬虫程序请求中有 40% 以 API 作为攻击目标。

亚太地区及日本：各垂直行业的 API 攻击占比（2023 年 1 月 1 日 - 2023 年 12 月 31 日）



亚太地区及日本：各攻击媒介的 API 攻击占比（2023 年 1 月 1 日 - 2023 年 12 月 31 日）



API 安全性方面的关键考虑因素

API 漏洞不断在发展变化。了解一些最严重的 API 安全风险可以让您的企业在与风险的较量中领先一步。

发现和监测

如果过时或先前版本的 API 仍在使用中或者未得到妥善记录，那么会让企业面临更大的风险。影子 API 等示例存在并在管理范围之外运行，这可能成为一个漏洞点。

运行时保护

由于执行 API 的目的是主动交换数据，因此传统安全工具难以分辨出 API 发出的合法请求和恶意请求。众所周知，API 逻辑滥用等隐蔽性强的威胁难以检测，因为它们能够与正常的 API 请求融为一体。

API 测试

为提升安全性且不牺牲速度，务必将 API 安全测试融入到开发过程的各个阶段。从成本和补救的角度看，在 API 开发阶段纠正问题比在 API 投入生产并获得积极使用后更容易。

未经身份验证的资源访问

在机器对机器的场景中，身份验证和授权更为复杂。通常，由于 API 实施或配置中存在漏洞，用户或系统或许可以在不提供任何形式身份验证的情况下访问 API 资源。

URL 中的敏感数据

URL 中的数据往往存储在攻击者或许可以访问的位置（例如，存储在日志和缓存中），从而会产生敏感数据泄露和合规问题等重大风险。

宽松的跨源资源策略

API 可能会允许请求来自于必要范围之外更广泛的来源（例如，协议、域和端口）。

从一开始就树立 API 安全性优先的文化

在评估云/安全解决方案提供商时，九成的受访 DNB 将 API 安全性列为一项关键或重要的产品功能。

随着技术创新和第三方连接步伐的加快，DNB 需要获得供应商的支持，以识别可能会遭到网络攻击者利用的潜在薄弱环节。

需要将 API 安全性融入到开发过程中的各个阶段。缺少 API 测试框架和具体的 API 测试攻击可能会导致发布更多易受攻击的 API，从而造成与 API 安全性相关的事件增加。缺乏对 API 业务逻辑滥用的监测能力是另一个导致出现 API 数据泄露和欺诈的因素。

例如，安全团队如何知道 API 在运行过程中遭到滥用？贵企业的 API 在任何时候会遭到哪些攻击？

例如，安全团队可能并不完全了解 API 端点的用途，因此难以知道哪些后端工作负载正在与他们进行交互或者正在交换哪些数据类型。开发团队也可能会高估自己在开发周期后期修复错误的能力。

依托 AI 技术的发现和分析是 API 安全性中的重要趋势，但在开发过程早期 (DevSecOps) 采取安全第一的立场有助于尽早减少 DNB 的漏洞，并帮助建立“通过设计保证安全”的 API 开发理念。

从一开始就找到这些高级 API 安全盲点可帮助建立更稳健的网络安全态势。

评估云或安全解决方案提供商时，以下产品功能的重要性如何？

	关键	重要	有点重要	中立	不太重要
API 安全	45.60%	45.10%	7.40%	1.90%	0.00%
可自定义的云安全策略	31.20%	53.90%	8.40%	6.50%	0.00%
边缘计算功能	29.80%	47.00%	15.80%	6.00%	0.90%
可观察性	28.40%	52.10%	11.20%	7.00%	0.90%
实时分析和报告	45.60%	34.40%	11.20%	7.40%	1.40%
Zero Trust	32.60%	39.10%	14.40%	9.30%	0.90%

常见的 API 安全盲点

未经身份验证的资源访问尝试

该衍生问题比上一节中所述的未经身份验证的资源访问态势告警更加紧迫。在此类问题中，我们发现攻击者未进行适当的身份验证就能够对敏感 API 资源进行明确的访问尝试。即使观察到的尝试未成功，这些情况也表明攻击者在主动尝试寻找并利用 API 漏洞。如果不进行及时干预，此尝试过程有可能最终取得成功。

JSON 属性异常

使用异常 JSON 有效负载（例如，意外数据类型、异常大小或过于复杂）的 API 活动可能表示攻击者在主动尝试利用容易受到攻击的 API。此活动可能表示攻击者在尝试执行各种恶意操作，例如注入攻击、拒绝服务、数据外泄或利用 API 逻辑缺陷。

路径参数模糊测试尝试

路径参数模糊测试是故意在 API 请求中发送意外或格式错误的数据的另一个示例，重点是 RESTful API 用于指定某些资源或操作的 URL 部分。它是攻击者用于进行侦察以发现潜在易受攻击 API 的另一种技术，可以通过数据外泄或服务中断尝试来攻击这些 API。

不可能的时间旅行

在分析 API 活动时，会出现 API 调用的时间戳、地理位置或顺序不合逻辑的情况，这表明攻击者正在尝试通过某种方式来操纵 API。此外，此类行为有可能表示存在多种可能的威胁，例如欺诈活动中包含的数据篡改。

数据抓取

数据抓取是指以不符合 API 的预期用途和服务条款的方式和数量从 API 中自动提取数据。攻击者往往会缓慢收集此类数据以避免被检测到，并以这种方式窃取知识产权、收集敏感客户数据或获得某种好处。当攻击者在 API 内悄悄进行数据收集时，虽然是少量缓慢的数据抓取，但却可能引发大规模的数据泄露攻击。

现代 API 安全方法

现代 API 是连接纽带，能够实现微服务、多云、无缝集成和快速扩展。它们是任何应用程序或工作负载的软肋，必须采用正确的架构并进行正确的开发和部署才能优化业务成果。

但是，尽管现代 API 事务往往具有独特的特征（例如，高频交易），但企业倾向于采用相同的安全措施。

1 实施自动 API 发现

确保您提供和使用的 API 都能够正确得到识别，以防止出现与 API 相关的安全漏洞、未知依赖关系和意外的不一致。与 API 数据源的原生集成将帮助降低复杂性并减少运营开销。

2 管理 API 的态势

评估 API 安全包括检测任何错误配置、执行渗透测试或使用能够主动进行配置问题（例如，在 URL 中暴露敏感数据的 API）扫描的自动评估工具。自动响应可确保在响应工作流程中能够寻求 API 开发团队等相关方的帮助来修复相关问题。

3 API 运行时保护

这包括检测表明存在恶意活动的模式。基于类似攻击的数据集进行训练的异常检测引擎应当能够识别威胁并向相关方发出告警。在检测到异常 API 流量时，可触发响应工作流程以创建补救工单或阻止潜在威胁。

4 主动安全测试

通过动态扫描和模糊处理进行 API 安全测试可以发现在初步评估期间可能未检测到的错误配置技术漏洞。

随着您的 API 安全日趋成熟，安全测试应当更紧密地融入 API 开发周期中，并在发现漏洞后立即加以解决，然后再将 API 投入生产。这意味着安全和开发团队之间需要进行跨职能协调。

5 API 安全生态系统

拥有丰富而强大的技术生态系统，让 API 安全解决方案能够与第三方技术进行原生集成和互操作，这可以降低成本并缩短实施时间。它还能够对数据源进行更广泛的 API 流量监测、通过自动工作流程实现更快的威胁响应以及提升整体 API 安全态势。

澳大利亚/新西兰：从初创到扩大规模

分析人员报告指出，未来几年澳大利亚/新西兰 (ANZ) 的国内需求和劳动力需求疲软。

由于工资增长缓慢和通胀持续，客户已经感受到了经济压力。

可能是为了应对当前的经济形势，来自新西兰的受访 DNB 优先考虑提高效率和企业韧性。

随着云技术现在成为业务必需品，人们的观念也发生了转变。共有 97% 的受访企业已采用云技术或正在探索云技术采用。

新西兰的企业或许会深化云技术采用，在经济增长放缓的情况下进一步提升运营效率。

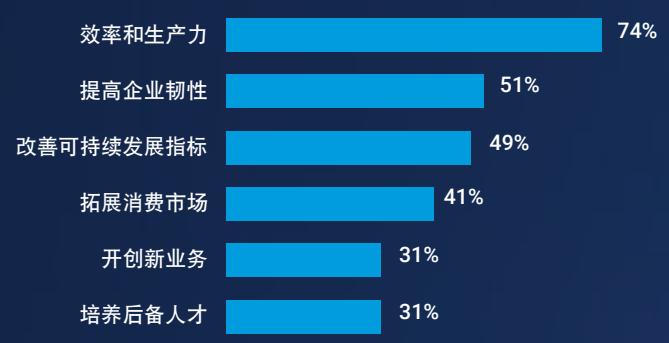
主要预测摘要

日历年	2020 年	2021 年	2022 年	2023 年	2024 年（预测值）	2025 年（预测值）	2026 年（预测值）
实际 GDP[1]（年平均变化百分比）	-1.4	5.6	2.4	0.6	0.5	1.5	2.5
失业率（季节性调整；十二月季度）	4.9	3.2	3.4	4.0	5.1	5.5	5.0
CPI 通胀（年变化百分比；十二月季度）	1.4	5.9	7.2	4.7	2.6	2.0	2.0
官方现金利率（十二月季度末）	0.25	0.75	4.25	5.50	5.50	4.75	4.00

[1] 基于生产

资料来源：Statistics NZ、REINZ、Bloomberg、ANZ Research

未来 12 个月的首要业务重点



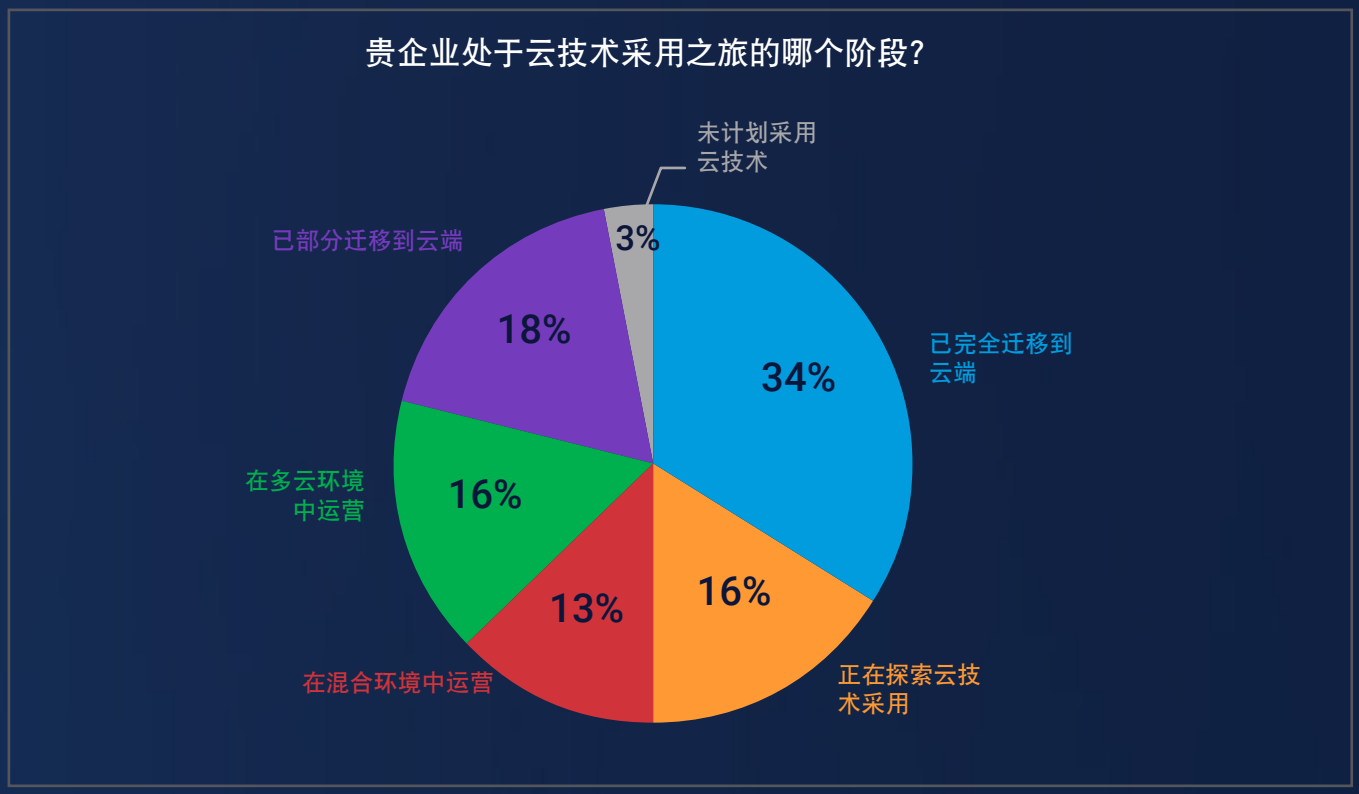
例如，新西兰地区的公有云采用已不再局限于基于离散软件即服务的解决方案，从灾难恢复等基础架构替代方案，发展为推动企业范围内数字化转型和创新的高级应用场景。

在云技术采用相对地发展成熟的过程中，人们的思维方式发生了转变，从将云技术视为业务颠覆者转变为将其视为业务必需品。

在澳大利亚和新西兰，公共部门也是推动云技术采用的主导力量。新西兰于 2012 年颁布了云技术优先的政府政策，而澳大利亚于 2015 年颁布了相应政策。

据估计，2024 年澳大利亚公司在公有云上的开支将达到 154 亿美元，比 2023 年增加 19.7%（来源：Gartner）。

数字化技术采用率的进一步提高意味着，ANZ 企业中可能存在未针对云技术进行架构设计、未进行容器化或未基于微服务的传统应用程序，也就是说它们最终的成本会高于云原生应用程序。



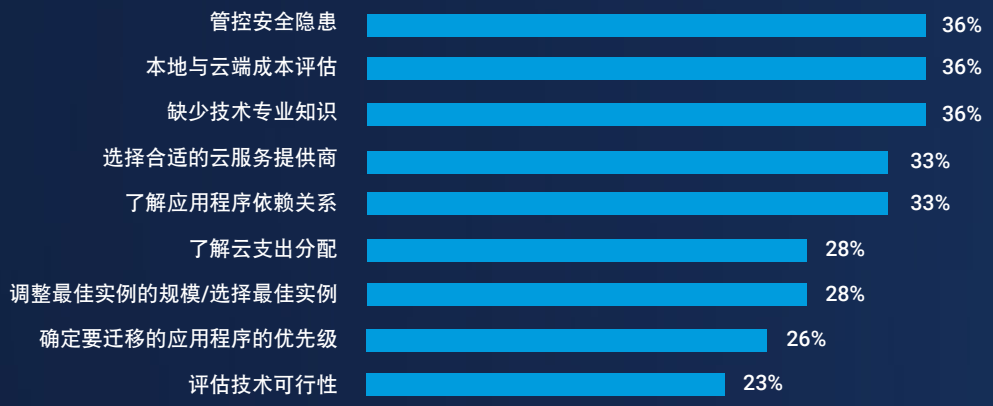
新西兰地区的调查受访企业认为，云成本是云迁移过程中遇到的最大挑战之一，其他挑战包括安全隐患和缺少技术专业知识。

技术采用的规模，加上创新压力和经济增长放缓，重新引发了人们对尽量减少云浪费的关注。

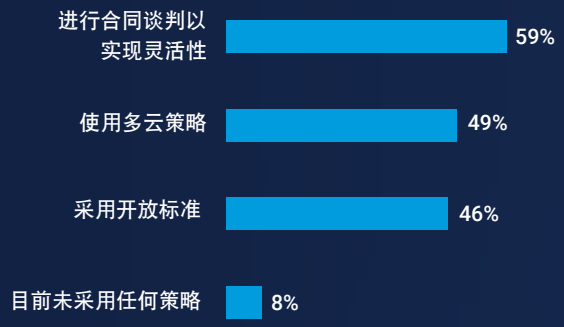
云成本可能会很复杂，因为需要专业知识和时间来预测并解读微服务和多云部署的费用，这些服务和部署会基于各种因素而进行不同的扩展。

FinOps 等云成本管理解决方案将财务责任引入云的可变支出模式中。用户需要对支出决策负责，并深入了解企业的云使用情况和生产力优化机会。

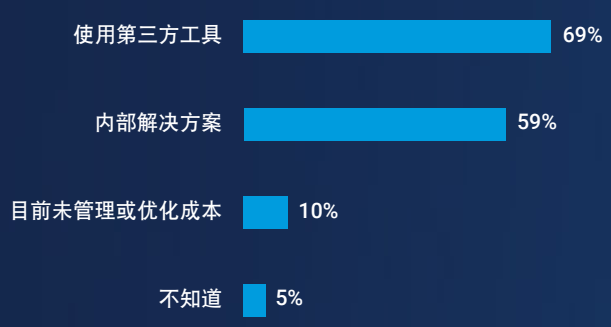
您在云迁移过程中遇到的主要挑战有哪些?



用于避免供应商锁定的策略



用于优化云成本的第三方工具



新西兰地区的 IT 负责人正在利用第三方工具、托管服务和合同谈判，以更高的承诺支出额或承诺增长率来换取折扣。

将云运营管理与财务治理相结合，可以保护企业不受无限制自动扩展的影响，这种扩展可能会在一夜之间将您的年度云预算消耗殆尽。

这表明，随着 DNB 利用第三方工具和托管服务来增强专职工作人员的能力以实现高效、可持续扩展，云技术的采用已相对成熟。

Akamai 的全球网络已与世界各地的 ***1,200*** *个网络融为一体并与所有主要云服务提供商保持优化互连，以确保高可用性、低延迟和无限扩展。*

更丰富的客户体验意味着有更多的敏感数据

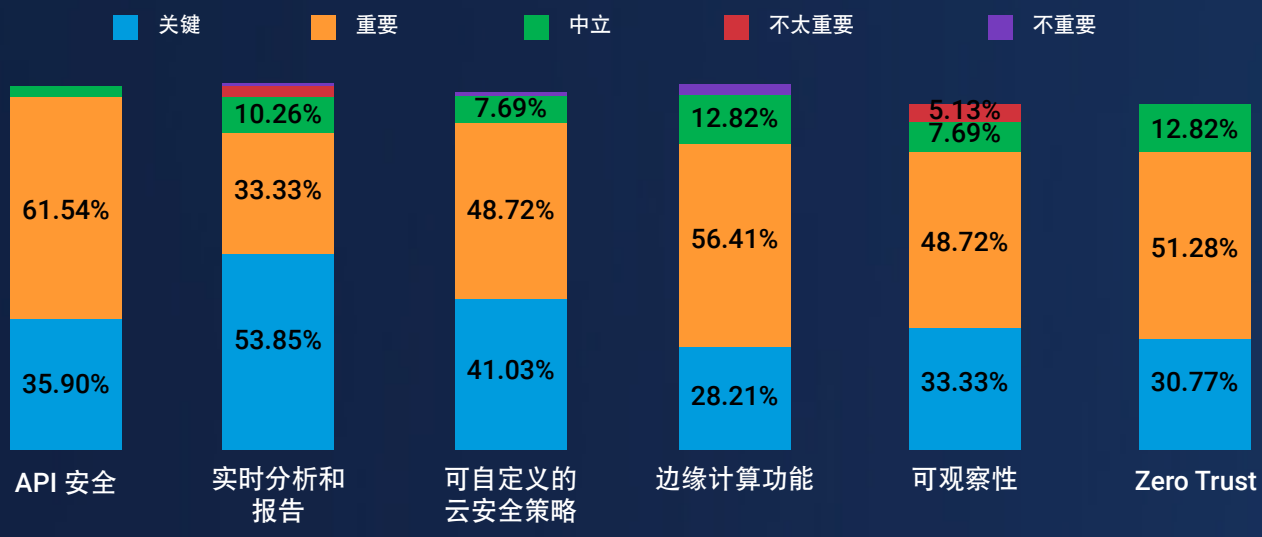
随着客户数字化技术采用的相对成熟，新西兰地区的企业希望能够提取、处理、分析实时数据并采取相应的行动，以提供出色的用户体验。

新西兰地区共有 87% 的受访企业认为实时分析和报告是其评估云/安全解决方案提供商时的一项关键/重要产品功能。

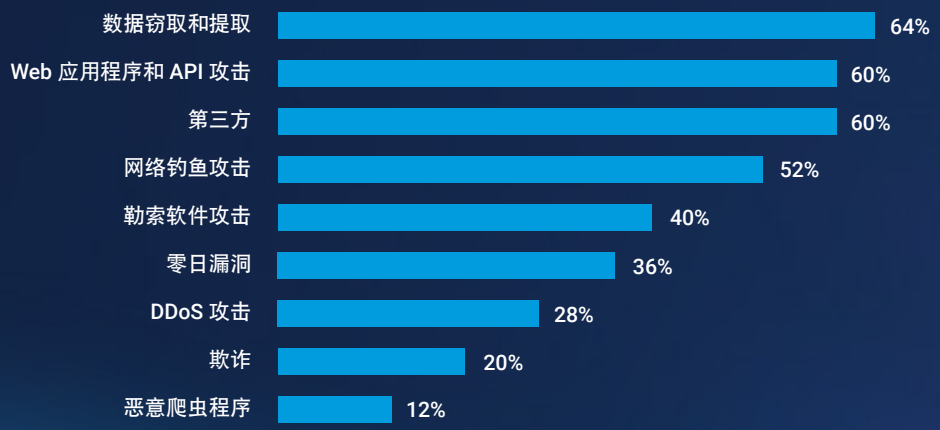
另一方面，新西兰地区的数字原生企业寻求提供更丰富的客户体验，这也可能导致它们面临以丰富的个人和财务数据为目标的网络攻击。

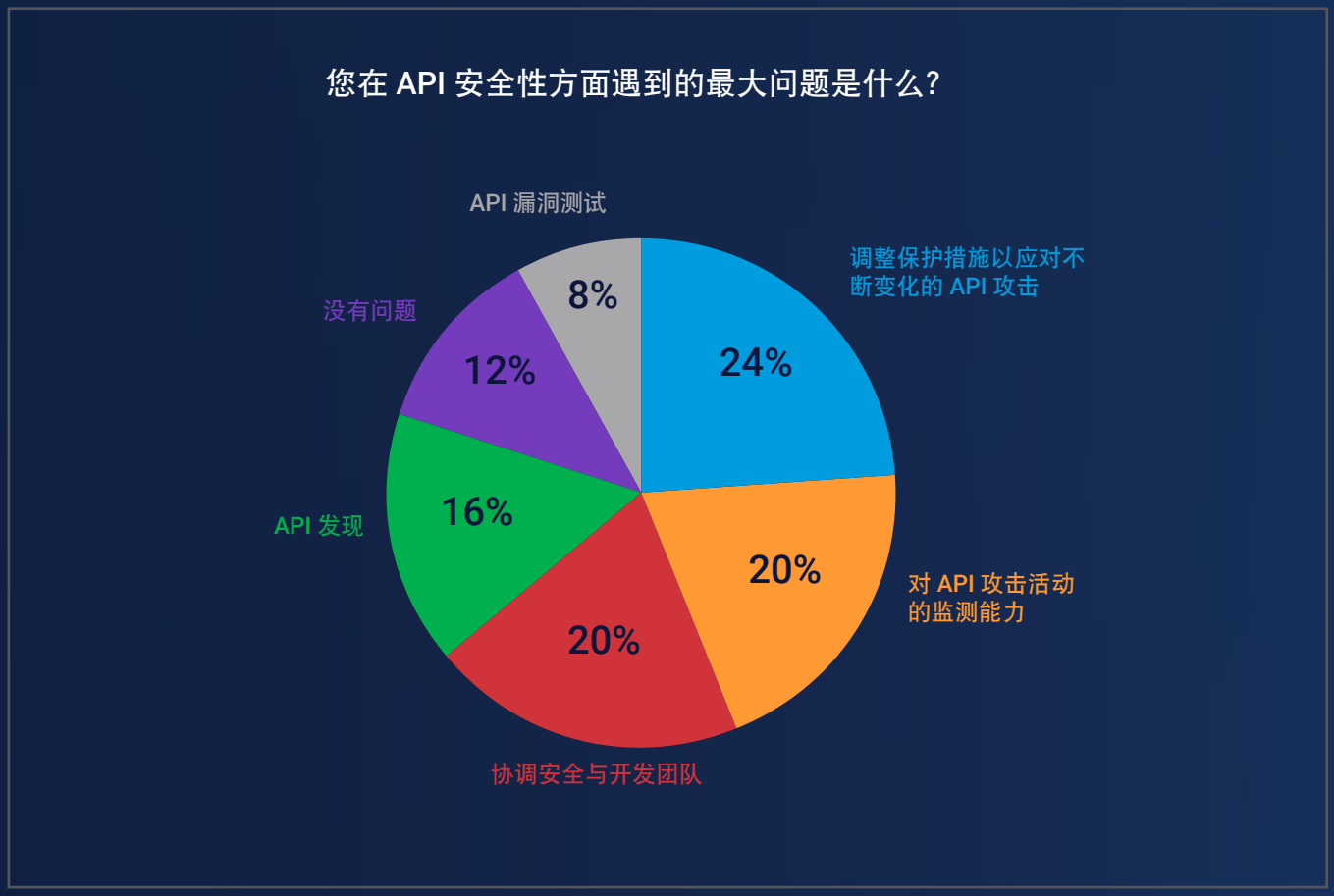
Akamai 的《金融服务业网络安全》报告显示，Web 应用程序和 API 攻击以及数据窃取和提取是澳大利亚 IT 负责人关注的主要网络威胁。

评估云/安全解决方案提供商时，以下产品功能的重要性如何？



澳大利亚 IT 负责人关注的主要网络威胁





还有安全维度的问题，新西兰地区的 IT 负责人认为，他们在 API 安全性方面面临的最大问题是获取对 API 攻击活动的监测能力 (20%) 以及调整保护措施以应对不断变化的 API 攻击 (24%)。

常言道，“您无法保护看不到的东西”。许多公司并不清楚自己真正有多少个 API，也就很难量化风险。

对于很多提升其 API 活动监测能力的企业来说，最大的意外发现之一是在他们不知情的情况下自己的环境中运行着如此之多的影子端点。

因此，在评估云/安全解决方案提供商时，新西兰地区 97% 的受访企业将 API 安全性列为关键/重要的产品功能。

在这种情况下，实时分析和报告可以加快检测和响应速度，并减少发生网络攻击时的损失。

连接 ASEAN：数字经济推动区域增长

东南亚是全球增长最快的互联网市场，每日新增 125,000 名互联网用户（来源：世界经济论坛）。

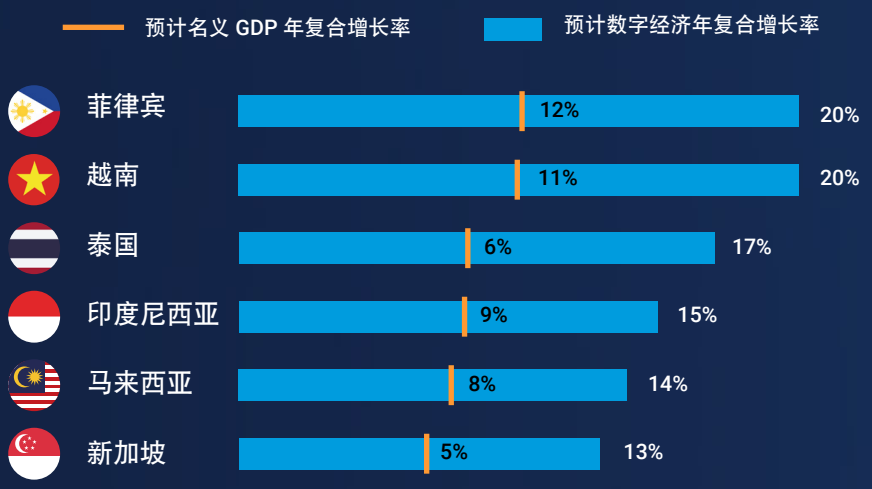
预计到 2030 年，数字原生代和关联的千禧一代及 Z 世代将占东盟消费者的 75%，并占印度尼西亚消费者的 70%（来源：世界经济论坛）。

实际上，所有东盟国家中数字经济总市值的增长率超过了 GDP 增长率（来源：e-conomy SEA 2023）。

虽然东盟国家的消费者正在迅速接受数字生活，但该地区的基础架构仍然需要跟上发展速度。精通数字化的年轻一代对服务正常运行时间和低延迟有着很高的期望。

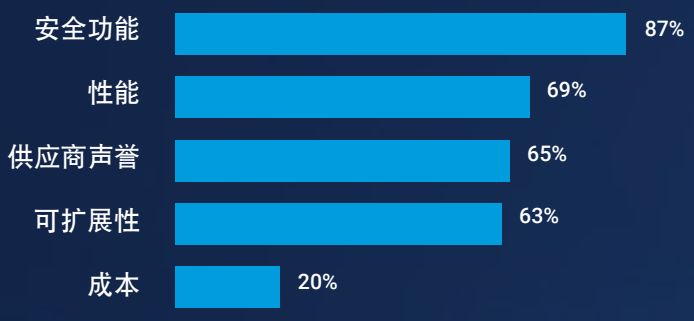
因此，在东盟国家受访企业的供应商选择中，性能和供应商声誉的排名靠前，分别占 69% 和 65%，这也在意料之中。

数字经济 GMV 增长率与 GDP 增长率对比（2023 年 - 2025 年）



（来源：e-conomy SEA 2023、Google、淡马锡和贝恩公司）

影响云供应商选择的因素



另一方面，对于东盟国家的 DNB，网络延迟也是一个老大难问题。

该地区仍然需要确保高速可靠的互联网连接，并在城市和农村地区实现电力普及。在地理位置分散的国家/地区，例如拥有 17,508 座岛屿（非官方消息来源称该数字接近 25,000 座岛屿！）的印度尼西亚，仍然存在连接不均衡的情况。

超过三分之二的受访企业认为网络延迟是其企业云基础架构性能和功能方面的一个不足之处。

该地区的各国政府一直积极投资于互联网连接，以促进持续增长。

印度尼西亚最近完成了 Palapa Ring 项目，为最偏远的地区实现了 4G 互联网连接，并在全国铺设了超过 35,000 公里的陆地和海上光缆。

> *与其他提供商相比，Akamai 在更多地区提供基础架构，提供核心和边缘的云计算资源，并能够为旨在满足区域偏好的低延迟、数据密集型应用程序提供支持和全球扩展。*

对东盟国家来说，API 安全性是一项关键的产品功能

东盟国家的 DNB 非常清楚，API 能够保证其企业的运行，并有助于促进与其他供应商及生态系统合作伙伴的合作。

与新西兰 (69%) 和印度 (91%) 的受访企业相比，东盟国家的受访企业在识别和抵御高级 API 攻击方面更有信心 (99%)。

实际上，几乎所有 (99%) 的东盟国家受访企业都认为 API 安全性很关键/重要。

但是，API 蔓延千真万确，并且很快的增长速度意味着缺乏监测能力，这会迅速成为一个安全和合规问题。

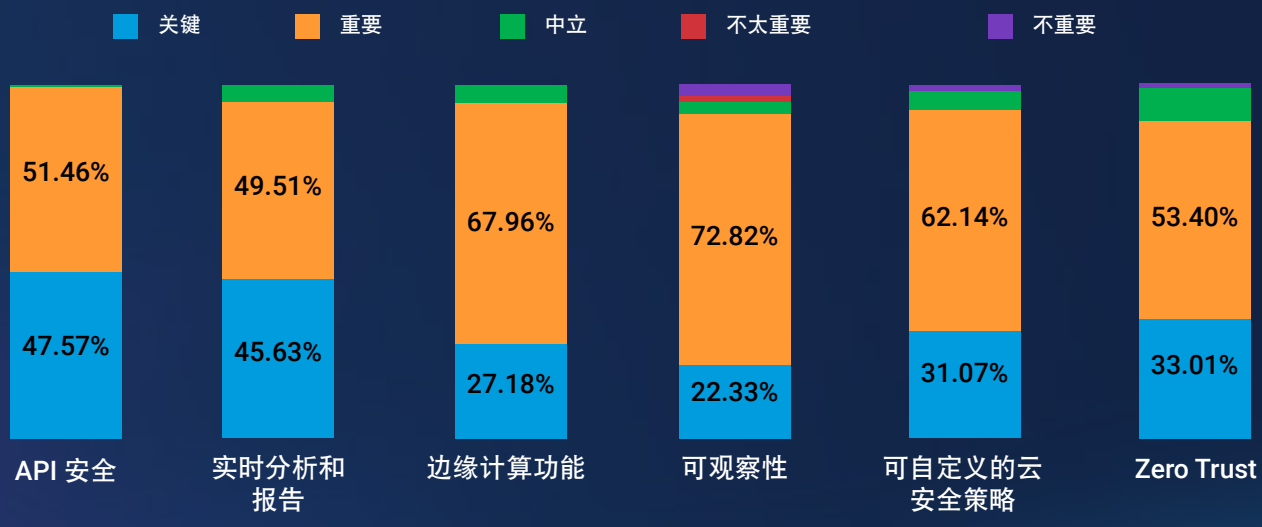
监测能力是 API 安全中一个至关重要的方面。一旦影子 API 或恶意 API 等盲点得以揭示，安全团队就可以开始解决先前未察觉到的漏洞。

因此，95% 的东盟国家受访企业都认为实时分析和报告很关键/重要。如果不进行妥善管理，API 会成为滋生数据泄露、违反合规要求和管理缺失等问题的温床。

您在识别和抵御高级 API 攻击（如 OWASP 十大 API 安全风险中的攻击）方面的信心如何？

地理位置	有信心/非常有信心
东盟地区	99%
新西兰	69%
印度	91%

评估云/安全解决方案提供商时，以下产品功能的重要性如何？



前所未有的数字增长带来网络钓鱼问题

对于东盟国家的 DNB 来说，数字技术采用率高已成为一把双刃剑。

数字技术的采用速度如此之快，以至于客户在网上交换信息时并不一定会将隐私放在首位。网络钓鱼已从基于电子邮件的攻击演变为现如今包含移动设备和社交媒体的攻击。

因此，该地区成为网络钓鱼最严重的地区之一，仅在 2023 年就报告了近 50 万起案件。

东盟国家颁布的数据保护和隐私法在很大程度上取决于各国政府能否跟上快速变化的数字通信趋势。例如，短信中的可点击链接仍然是一种常用的诈骗手段，尽管越来越多的国家/地区正在实施相关政策来拦截这种常见的网络钓鱼方法。

与该地区的同行相比，受访的东盟国家 DNB 更注重投资于反网络钓鱼技术。

网络钓鱼并不会消失。

生成式 AI 的兴起让网络钓鱼企图更具说服力，并为犯罪分子攻击受害者提供了更多选择。毕竟，网络钓鱼针对的是人性，而不是软件漏洞或系统利用问题。

这正是所谓的，进攻是最好的防守。网络钓鱼模拟与可靠的端点保护相结合，可帮助 DNB 在与网络钓鱼的较量中占得先机。

2023 年东南亚地区检测和拦截的金融行业网络钓鱼数量

国家/地区	金融行业网络钓鱼数量
菲律宾	163,279
马来西亚	124,105
印度尼西亚	97,465
越南	36,130
泰国	25,227
新加坡	9,502
总计：	455,708

资料来源：2024 年，卡巴斯基

将以下网络安全投资领域按最重要（顶部）到最不重要（底部）的顺序进行排序

1. 反网络钓鱼技术
2. 高级 API 安全
3. Web 应用程序安全
4. 与 Zero Trust 相关的技术
5. 分布式拒绝服务 (DDoS) 攻击抵御

印度：“I”代表创新

过去十多年来，印度一直是创新和 DNB 的中心，也是云原生架构和实验的主要来源。

对于印度的 DNB，他们始终专注于增长和创新，该地区云基础架构的 AI 集成度最高 (98%)，并且几乎所有 DNB 已采用云技术或者正在探索云技术采用。

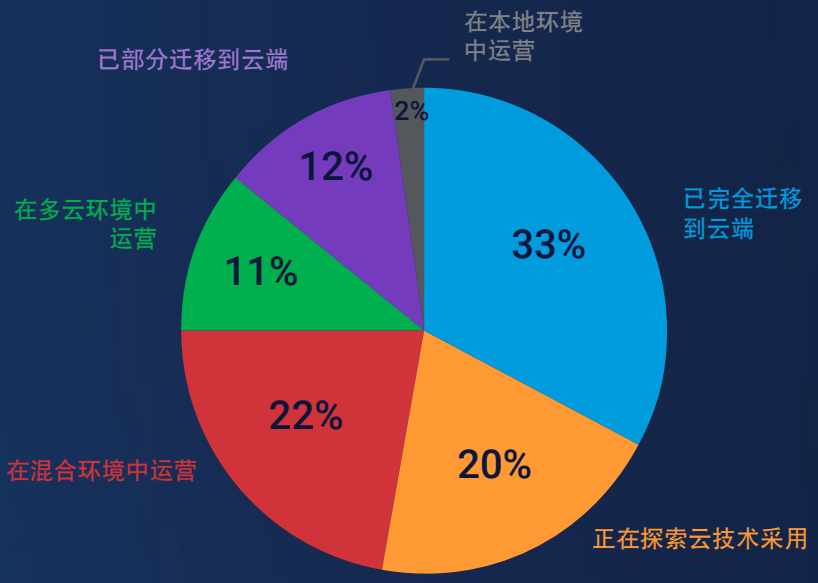
但是，随着印度 DNB 的日趋成熟，他们开始将重点放在安全和成本优化上，并仔细审查供应商选择，以实现可持续增长。

印度早期 DNB 的客户通常自身就是科技公司。

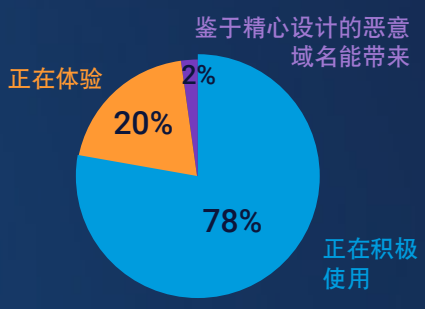
在 API 的支持下，印度的 DNB 已能够为全球企业提供技术支持和专业知识，而无需直接访问客户的数据。印度的 DNB 很早就在专业知识、API 和定制系统方面进行了投资。

由于在技术卓越性方面拥有深厚的传统，印度的数字原生企业比该地区的同行（东盟国家位列第二，新西兰位列第四）更加重视供应商的表现。

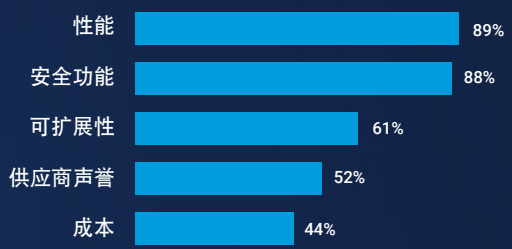
贵企业处于云技术采用之旅的哪个阶段?



云基础架构中当前的 AI 技术集成度



影响云供应商选择的因素



“I”也代表内部专业知识

与该地区的同行相比，印度数字原生企业的另一个突出特点是采用“自己动手”的方式进行云成本管理。

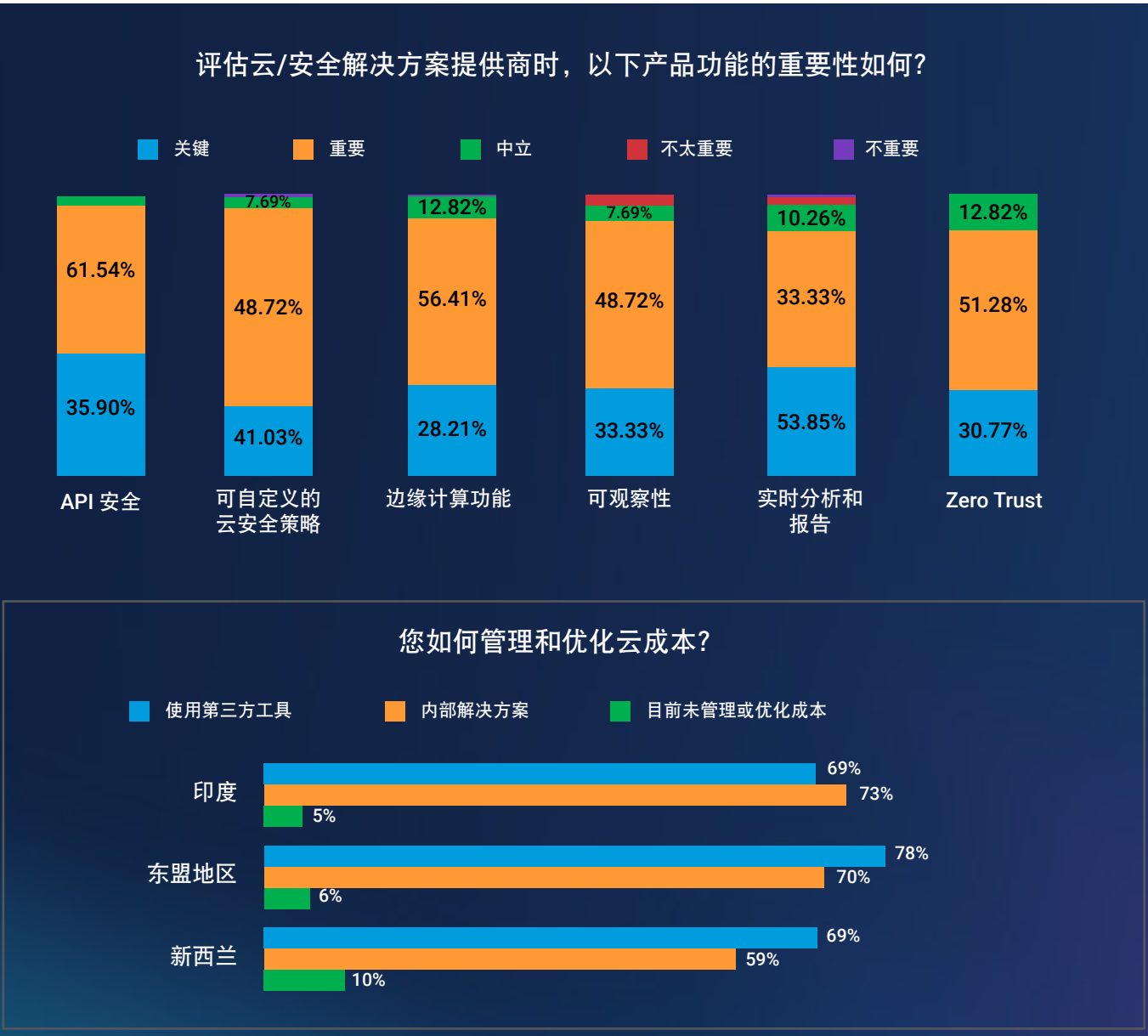
在印度，共有 73% 的受访企业表示使用内部解决方案来管理和优化云成本，而与之相比，东盟国家和新西兰地区的受访企业中相关比例分别为 78% 和 69%，他们更喜欢使用第三方工具。

新西兰地区的受访企业选择第三方工具可能是因为当地 IT 技术人才短缺。

例如，新西兰每年需要 5,000 名网络安全人员，但预计到 2026 年，当地的教育系统只能培养大约 2,000 名具备网络安全专业知识的人员。

相比之下，得益于其作为全球技术服务中心的历史优势，印度拥有丰富的技术人才。

在印度，目前有超过 1,600 个全球能力中心 (GCC) 为世界各地的企业提供技术支持。到 2030 年，该数据将继续增加，届时 GCC 将达到约 2,500 个，员工数量超过 450 万人，并创造 1000 亿美元的收入。



DIY 使印度的 DNB 面临各种漏洞

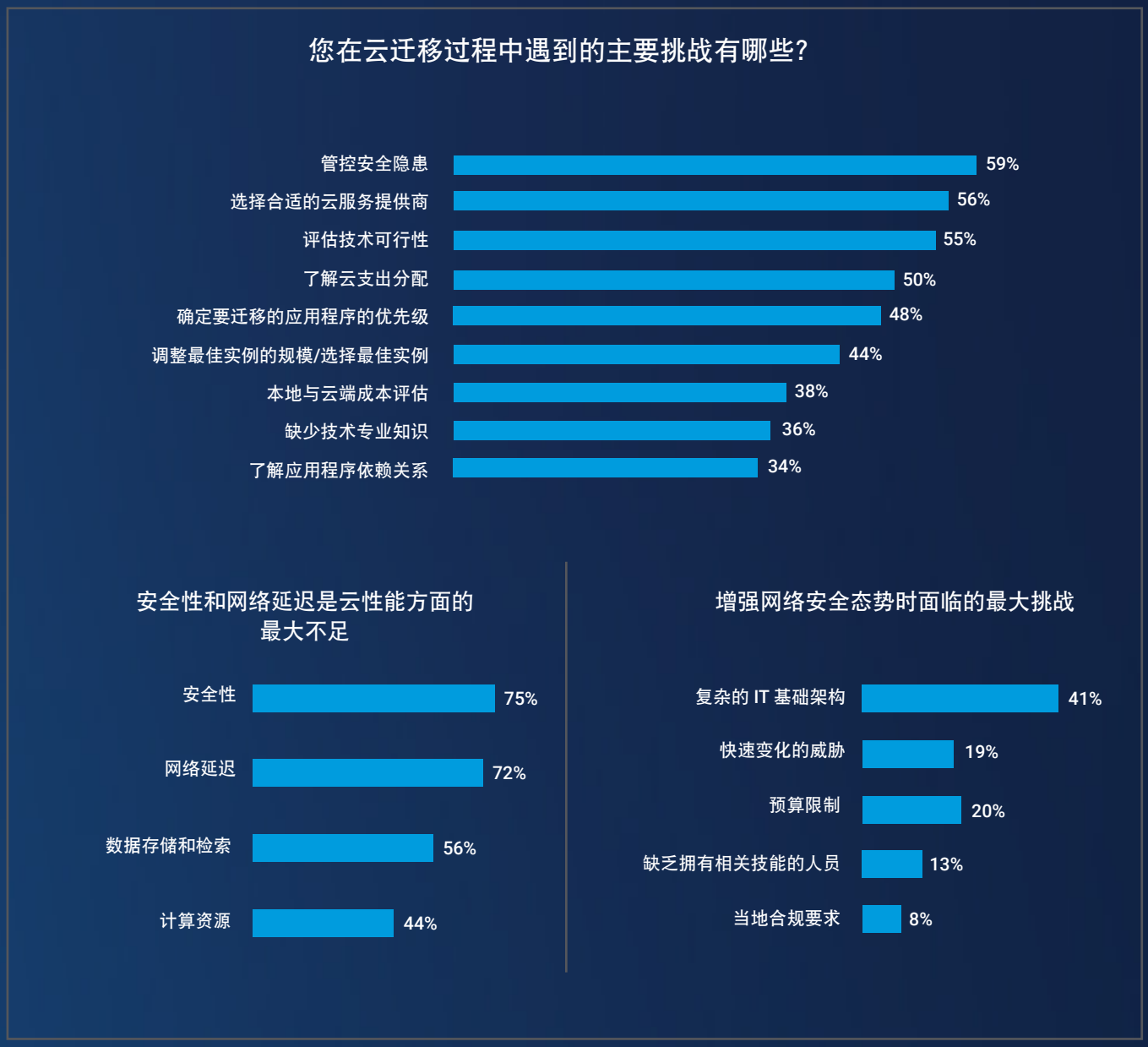
随着企业规模扩大并日趋成熟，印度的数字化企业在管理其技术基础架构时采用的 DIY 方法可能会导致自己面临各种漏洞。

将不同的系统与多个 API 相集成本就增大了潜在的攻击面。对于在云端诞生并完全在线运行服务的企业来说，这一问题更加严重。

五分之三的印度受访企业认为，管控与云基础架构和迁移相关的安全隐患是首要问题。实际上，四分之三的受访企业认为安全性是其企业在云基础架构方面的最大不足。

印度的 DNB 需要从两个方面来了解其企业的漏洞和潜在攻击场景。网络威胁形势正在快速演变，新的攻击方法和工具日益复杂。

印度的 DNB 可能需要与拥有专业技能的第三方合作来摆脱技术自给自足的束缚，并利用新兴技术所能提供的效率。



实际上，一大部分 (41%) 调查受访企业表示，复杂的 IT 基础架构是他们在增强企业网络安全态势时面临的最大挑战。与之相比，36% 的新西兰地区受访企业认为复杂的 IT 基础架构是一项挑战。

尝试在没有全天候专家的帮助下在内部管控网络安全可能不再是一个可行的选项，对于印度等快速增长的市场来说尤其如此，它恰好是该地区的主要网络攻击目标之一。

这将是印度技术基础架构拼图的核心部分。

> *Akamai 的分布式云平台让开发人员能够控制在何处部署和扩展计算资源。开发人员拥有定义在何处采集、处理和管理数据的能力和灵活性。*

强强联手

亚洲数字原生企业的技术负责人在接受 AI、云计算和大数据以追求更丰富、更快捷的客户体验时面临各种挑战，该调查针对这些挑战提供了开创性的见解。

但是，一概而论地描绘所有数字原生企业不切实际。

这项研究区分了亚太地区不同地域和行业的数字原始企业在云/API 成熟度和网络安全态势方面的细微差别。

例如，高度监管行业或地区的企业正寻求在安全和隐私与用户体验之间取得平衡。

对于成败尽在毫秒之间的数字原生企业来说，通过超本地化优化实现个性化体验的先进功能至关重要。

究其根本，云原生架构得益于架构良好的 API 和端点，数字原生企业能够利用这些 API 和端点进行纵向/横向扩展，并提供丰富的个性化体验。

大多数企业缺少有效锁定云所需的原生监测能力和安全控制能力。要确保公有云和多云环境的安全，安全从业人员必须能够看到哪些应用程序、工作负载和流量在环境中移动。

Akamai 正在改变企业处理云架构的方式，强调采用分布更加广泛、分散化、低延迟且全球可扩展的设计——非常适合于需要在更靠近最终用户的位置运行的高性能工作负载。

我们致力于在全球难以进入的市场建立核心计算区域，目前广泛覆盖 131 个国家或地区的 4,100 多个边缘入网点。

如果您想了解为什么世界各地的优秀公司都选择 Akamai 来构建、交付和保护他们的数字化体验，欢迎联系我们。

方法

此调查通过对整个地区的 IT 负责人进行实地调研获得了这些见解。
调查于 2024 年 3 月到 5 月进行。

目的

该报告深入探讨了数字原生企业如何看待即将到来的趋势和威胁。这些发现结果建立在当前实地见解的基础之上，可为企业提供宝贵参考。

对象

以下行业的首席信息官、首席技术官、IT 总监及副总裁：

- 航空公司
- 媒体/广播/出版
- 电子商务/互联网
- 游戏
- 酒店
- 信息技术
- 零售/批发

地点

- 澳大利亚
- 新西兰
- 印度
- 新加坡
- 印度尼西亚
- 泰国
- 马来西亚
- 越南