Akamai

白皮书

Zero Trust Network Access 发展蓝图

谁应该阅读本指南?

网络架构师、安全工程师、首席技术官、首席信息安全官以及其他 IT 和安全决策者都将从本指南中受益。

对于负责界定、配置、部署、实施和管理 Zero Trust Network Access (ZTNA) 项目的人员来说，本指南全面回顾了不同系统的潜在优势以及它们之间的差异。本指南介绍了：

- 传统应用程序访问方法的局限性和安全漏洞，以及需要 ZTNA 的原因
- ZTNA 的组成部分以及它的工作原理
- Akamai Enterprise Application Access 及 Akamai MFA 如何快速、轻松地实现 ZTNA

随着商业世界的日新月异以及网络威胁的不断涌现，广大公司都在重新审视自己的网络防御措施。很多公司已认识到，传统网络架构依赖于一个集中位置，所有相关方都可以从该位置访问应用程序，这让他们很容易受到攻击。这种城堡加护城河式的安全防御方法在保护边界的同时，假设城堡内的所有人都是安全无害的，但是在现今移动连接和云技术盛行的环境中，这会使公司面临遭受网络攻击的风险。一些高瞻远瞩的公司正在转为采用 Zero Trust 架构来保护重要的资产。任何 Zero Trust 项目的核心原则都是保护网络。本白皮书将详细介绍传统的集散式网络安全方法为何无法继续提供充分保护，以及转为使用 ZTNA 如何能够更好地保护关键资产，还有如何将 ZTNA 作为构建全面 Zero Trust 架构的关键因素。

企业变革的步伐速度惊人

企业运营和使用技术的方式不断发展演变，可以说是一日千里。在计算技术发展的推动下，原先在本地数据中心托管业务应用程序的模式快速转变为将应用程序托管至多个公有云、私有云或混合云（本地和公有云/私有云）的模式。

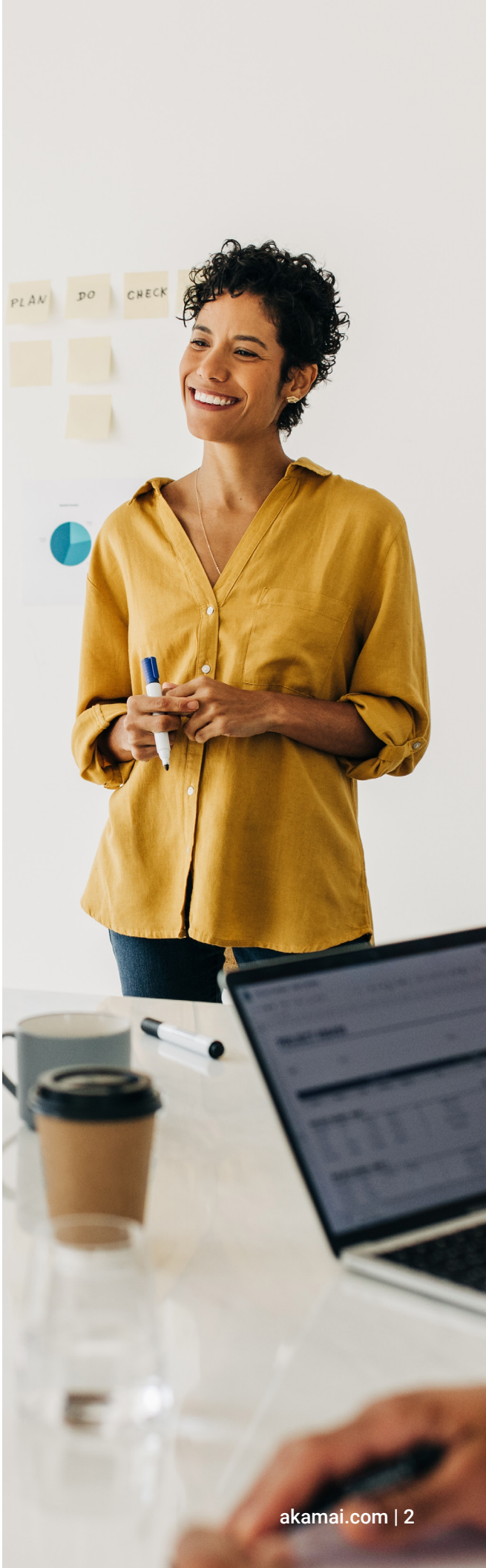
此外，业务模式的演变促使各个实体之间加强协作，同时为合作伙伴和供应商提供应用程序和资源访问的需求也在相应增加。

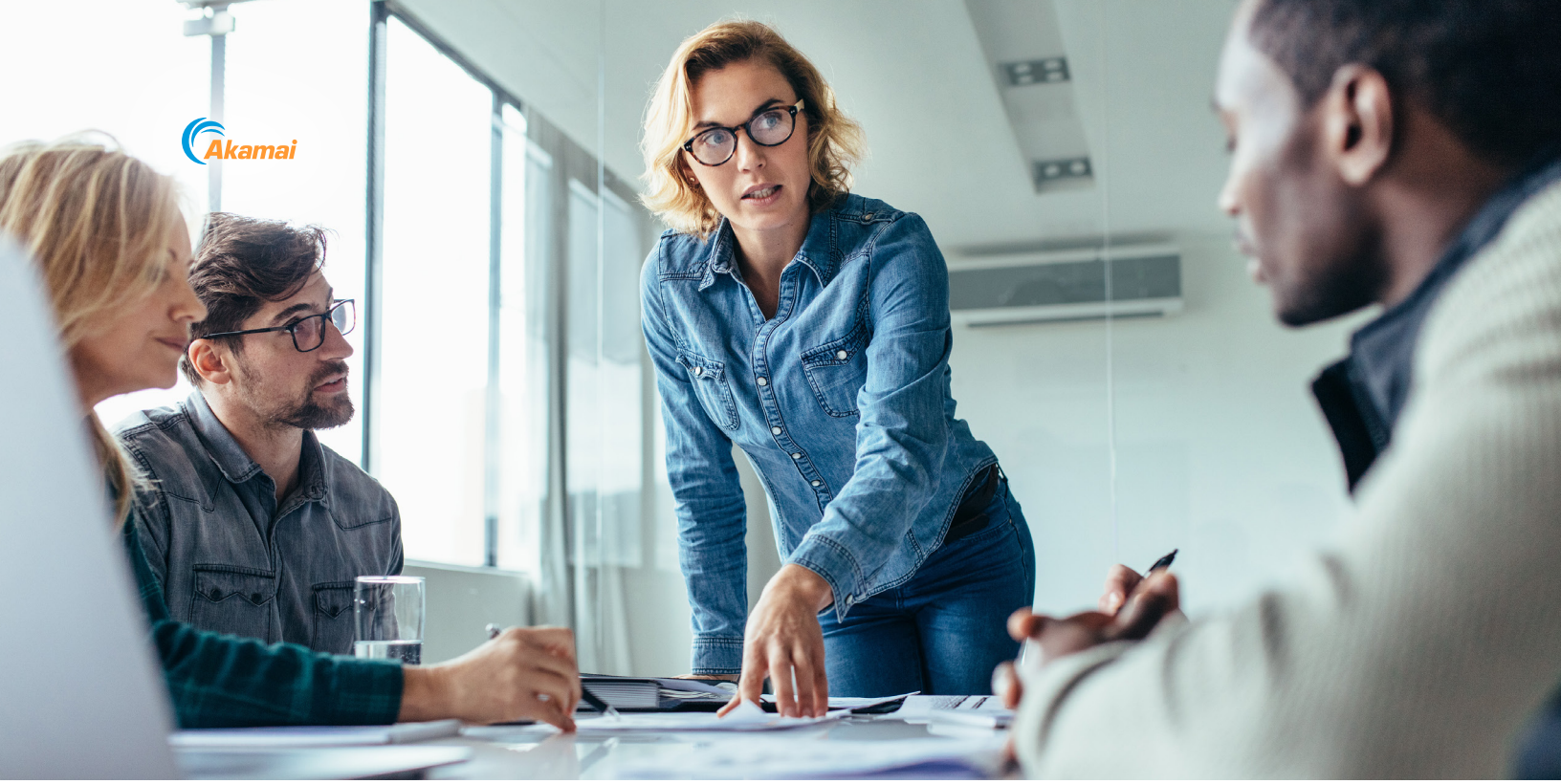
最后，由于企业继续采用远程或混合工作方式，用户现在要能够从任何地方通过托管和非托管设备访问业务应用程序和资源。

在这些变化的推动之下，传统方法在管理应用程序访问方面已经力不从心。因此，企业现在必须采用一种全新的方法，既能实现安全访问，又无需考虑托管应用程序的位置或用户所在的位置。

传统的应用程序访问

20 多年来，企业一直依赖防火墙来建立强大的安全边界并对边界内的用户信任有加。这就好比是将网络看作有护城河的城堡：厚厚的围墙和坚固的大门组成了保护城堡（在这里指网络）的边界，只有拥有正确凭据的用户才被允许进入。一旦进入网络，用户便能够根据自己的身份访问特定应用程序，这可以通过 Microsoft Active Directory 等身份提供程序 (IdP) 解决方案来实现。





但是，由于网络是扁平的，用户实际上可以对整个网络进行 IP 访问，这意味着他们可以发现其他服务器和应用程序。例如，如果 IdP 的配置正确，用户也许能够发现托管薪资应用程序的服务器，但当他们尝试登录该应用程序时，他们的访问会被拒绝。

为了解决这个不受限制的横向移动问题，企业通过虚拟局域网 (VLAN) 将应用程序划分到防火墙内的独立分段中，并对个人用户或群组强制实施目前已不再使用的基于 IP 范围的规则。这个过程十分脆弱，并且极易出错。不妨设想这样一个场景：某人正在执行维护工作，他将计算机移到新的机架中，或者需要为它们分配新的 IP 范围。突然之间，有用户遭到锁定并且支持电话接踵而至。或者，可能某次软件升级需要更改某个应用程序的架构，而用户被重定向到工作流程中的另一台计算机。一些用户或群组可能无法访问这台计算机，因为防火墙规则未更新。

该架构非常复杂，在进行任何更改期间都要求应用程序所有者、网络管理员和安全群组之间保持密切沟通才能确保不会发生停机。

我们都知道在协调失败时通常会发生什么样的结果。管理员想要遵循最佳实践，但如果时间紧迫，他们会添加糟糕的“IP ANY/ANY ALLOW”规则作为快速修复措施，以允许受影响的用户访问所有内容，直到能够对底层问题进行诊断并修复为止。然而，管理员往往没有时间撤销这些更改，而随着时间推移，这些快速修复措施会削弱公司的安全态势。

VPN 带来了更多的复杂性、性能和安全挑战

对于远程用户来说，虚拟专用网络 (VPN) 通常让他们能够访问托管在边界内的本地应用程序，然后这些应用程序提供对公司网络的直接隧道访问。

为管理用户对应用程序的访问，企业通常会添加专用的应用程序交付控制器，或者使用其 VPN 解决方案内置的访问控制措施。这样做的目的是使应用程序访问权限保持一致，而不管用户身在何处。如果用户在边界内时访问 CRM 应用程序被拒绝，那么即使他们通过 VPN 建立连接，相关访问也应当被拒绝。尽管目标是这样，然而在两种应用场景与快速修复措施之间同步应用程序权限非常复杂，这可能导致用户获得意外的应用程序访问权限。

承包商、合作伙伴和供应商的应用程序访问

此外，许多公司通常会使用 VPN 来允许承包商、合作伙伴公司或供应商进行远程应用程序访问。例如，某个公司可能允许供应商从外部访问公司的财务系统，以便其提交发票。允许第三方通过 VPN 访问应用程序会使得该公司不再拥有端到端安全性，从而带来更多安全风险。如果拥有 VPN 访问权限的第三方设备遭到入侵，攻击者便获得了对该公司网络的访问权限。

VPN 和性能

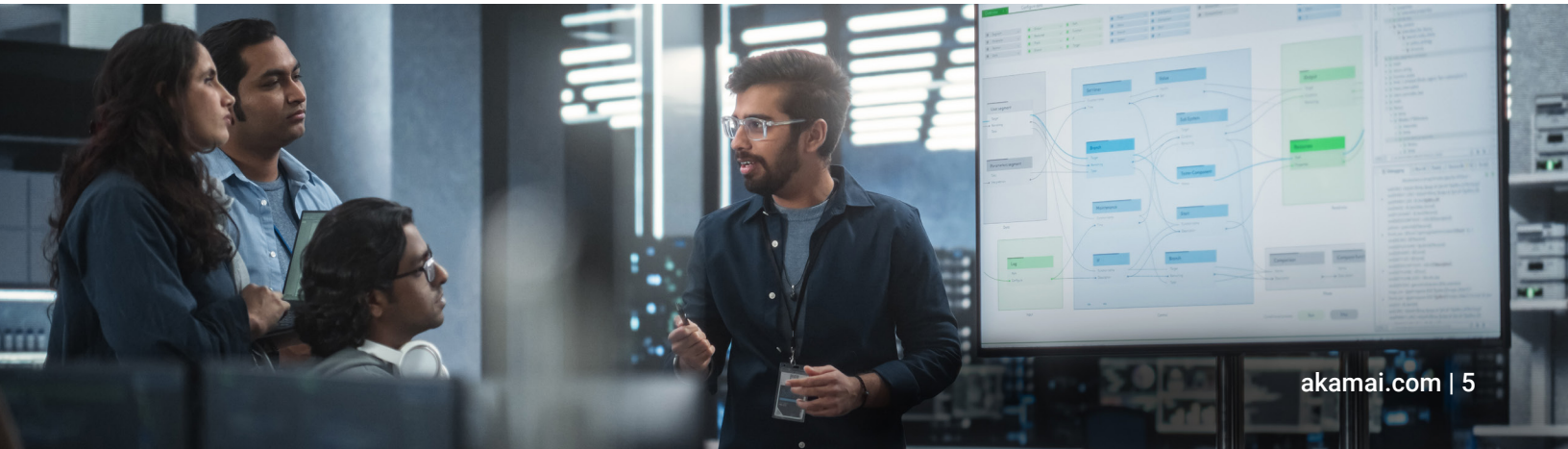
在性能方面，也会遇到相同的权衡问题。使用非常简单的 VPN 时，所有流量都会被定向回数据中心基础架构。由于存在会导致流量翻倍的发夹问题，这会造成对互联网资产以及软件即服务 (SaaS) 应用程序的访问变得极其缓慢。

为了克服这个性能阻碍，管理员通常会部署分离的隧道，并再次标记出哪些 IP 范围应通过 VPN 传输，哪些应直接进入互联网。当您只有一个内部边界时，此方法可能简单有效。但是，当您添加多个数据中心和虚拟私有云提供商时，它的复杂性会大大增加。管理员必须确定他们是否要在每个数据中心内安装 VPN 聚合器，以及将如何有效管理多点拆分隧道。

这并不是说 VPN 没有价值。实际上恰恰相反。比如，在多数据中心基础架构的站点到站点访问中，VPN 就极为有用。但是，对于访问应用程序的用户来说，网络级访问并不是应当使用的正确模式，因为网络级访问会强制在简单性与安全性/性能之间进行非自然的折衷。

对于攻击者来说，基于网络的应用程序访问是个好消息

到目前为止，我们都在专注于介绍将网络级访问权限授予所有员工所带来的风险和挑战。但是，此方法也会给企业带来另一项风险：利用被盗用户凭据或安全漏洞的网络犯罪分子还有可能不受限制地访问整个网络。例如，如果攻击者使用被泄露的员工凭据获得了 VPN 访问权限，那么他们可以在网络中进行横向移动，以查找、访问和攻击高价值目标。



这些方法有可能导致发生灾难性入侵

从理论上来说，使用这些方法可以安全地管理应用程序访问并尽可能减小阻碍。您可能已在使用其中一些解决方案的组合。问题在于，要想很好地实施这些方法、对其进行维护并在其生命周期内提供适当的安全性和性能，相关操作往往过于复杂而无法始终保持正确。在许多情况下，公司会说服自己，由于员工可以访问他们的应用程序，因此一切肯定都处于理想状态。当其中一项快速修复措施导致发生灾难性入侵或严重的性能下降，以致于出现服务中断或员工工作效率大打折扣时，他们便会被打个措手不及。

使用 Zero Trust 方法执行应用程序访问

考虑到边界安全防范中的固有缺陷，以及这些方法在管理应用程序访问时带来的特定挑战，新兴的 Zero Trust 网络安全模式无疑给企业提供了更理想的替代方案。该模式由 Forrester Research 于 2010 年首次提出，它是许多公司在进行 IT 基础架构、安全策略和业务流程转型时使用的一个框架。

它背后的原理十分简单，但又无比强大：信任与位置无关。您不能仅仅因为某个东西位于您的防火墙之内便信任它。反之，无论是发生在何处的任何操作，只有获得明确许可的操作才能得到信任。最终，只有*应该*发生的操作才*能够*发生。消除对不必要操作的所有隐式信任，因为它们会带来风险，而不是价值。

这需要强身份验证和授权，并且在信任建立前，系统不得传输数据。此外，还应采用分析、筛选和日志记录来验证行为并持续监控入侵信号。

在过去十年中，这种根本性转变抵御了我们观察到的大量安全隐患。攻击者无法再利用边界中的漏洞，进而通过成功入侵网络来收集您的敏感数据和应用程序。现在，没有用来保护访问的护城河了。有的只是应用程序和用户，两者必须先相互验证身份并验证授权，然

后才能实现访问。

Zero Trust Network Access

ZTNA 是一个基于这些原则构建的架构，它会根据强身份验证、授权和上下文来授予对应用程序和资源的安全访问权限。ZTNA 架构仅提供对用户完成工作所需的应用程序的访问权限，而不会提供对整个网络的访问权限。有了 ZTNA 方法，用户位置不再重要；也没有了边界内外的概念。无论应用程序托管在何处（本地、公有云还是私有云上）都无关紧要，因为经过身份验证的用户只能访问他们有权使用的应用程序。

例如，销售部门的某位员工只能访问与其销售职位相关的应用程序，而无法访问人力资源或财务应用程序。

Akamai ZTNA 的工作原理

利用 Akamai Enterprise Application Access 和 Akamai MFA，您可以迁移到 ZTNA 架构，这会是您迈向 Zero Trust 之旅中重要且关键的一步。

Enterprise Application Access 是一种云端身份感知代理 (IAP)。这是一项灵活且适应性强的服务，可根据威胁情报、设备态势和用户身份信息等实时信号制定精细的决策。Akamai MFA 是一项多重身份验证服务，提供强力身份验证，以确保发出访问请求的用户与其声明的身份相符。

开始使用时，您可以在防火墙内运行一个名为 Enterprise Application Access 连接器的小型虚拟机，但连接到的是您的应用程序。它不需要（也不*应当*）位于您的 DMZ 中。它的地址应位于私有 IP 空间上，不可直接从互联网访问。实际上，它看上去应当和您放在防火墙后的其他应用程序一样。

为了支持多云环境，必须将连接器部署在您的本地数据中心内或者部署在私有云或公有云中。

Enterprise Application Access 连接器会立即与 Akamai Connected Cloud 上的 IAP 建立出站加密连接。与 IAP 建立连接后，该连接器会下载其配置并准备好为连接提供服务。连接器与 IAP 之间的连接是出站连接，这允许您关闭所有入站防火墙连接，从而使应用程序在公共互

联网上几乎处于隐身状态。

IAP 会执行在用户连接到应用程序之前需要完成的所有预处理，包括身份验证、授权和设备安全及态势检查。当用户尝试访问应用程序时，他们通过 DNS CNAME 被定向至 Akamai，然后连接到 IAP。假设您的最终用户及其设备通过了所有检查，他们随后会被路由以执行身份验证、多重身份验证和单点登录，然后系统会执行设备标识功能。

在用户和计算机获得授权后，来自最终用户的连接会与来自 Enterprise Application Access 连接器的出站连接整合到一起。来自用户会话的流量会流过这个整合的 IAP，然后该 IAP 会连接到所请求的应用程序或服务。此时，一条完整的数据路径建立完毕，然后系统会根据身份、设备和用户上下文持续动态地执行所有访问决策。

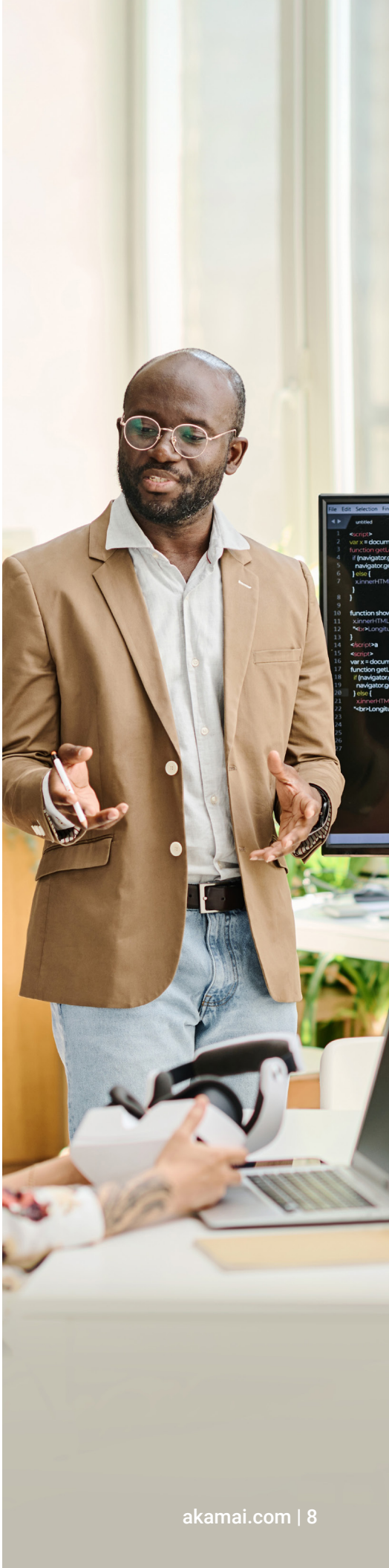
这种访问方法会带来明显的优势。对性能和安全非常敏感的活动将在更靠近最终用户的边缘开展，而 Akamai 在 134 个国家或地区拥有超过 4,200 个边缘位置。

此外，进入应用程序的敏感进入路径使用了反向应用程序隧道，这有效去除了边界的 IP 可见性，并降低了流量攻击的风险。

Enterprise Application Access 可以直接与公司的身份基础架构进行集成，即使其身份基础架构使用多个目录和身份服务提供商也是如此。因此，可以快速部署 ZTNA 服务，而无需对现有的身份基础架构或架构进行更改。

对于不支持现代身份验证协议的传统应用程序，Enterprise Application Access 拥有 IdP 桥接功能，该功能可以对基于 SAML 的 IdP 进行身份验证，并可以将身份验证令牌转换为传统应用程序支持的身份验证协议。

提供应用程序级访问是 Enterprise Application Access 等基于 IAP 的方法



如此有吸引力的原因。借助应用程序级访问，性能和安全性与复杂性*不再相关*。

您只需将所有相互之间具有本地关联（例如，均托管在同一数据中心或同一虚拟私有云中）的应用程序放置到专用网络 IP 空间或受限 VLAN 中，然后在该微边界中放置访问代理即可。仅此而已——大功告成。

应用程序所有者在访问代理上设置自己的安全策略（有关谁可以访问、访问内容以及访问原因的策略），而更引人注目的是，用户可以身处任何位置。内部和外部没有区别，因为不存在包含最终用户的网络边界。在咖啡店中工作的员工和在办公室中工作的员工并无二致。唯一重要的是，用户是否具有授权或者计算机是否安全。

借助应用程序级访问，您可以兼顾出色的性能和轻松的部署及使用。用户直接通过互联网访问应用程序即可，无论这些应用程序托管在何处或出现在何处，互联网都能将数据包路由到其目的地，而不必经过不在其路径上的聚合器或中介。

实际上，借助应用程序级访问，内部网络通常可以融入到简单的访客 Wi-Fi 中。需要牢记的是，要让 Zero Trust 真正发挥作用，就不能将内部用户和外部用户区别对待。默认情况下，不信任任何人。

ZTNA 所需的最终状态

对于所有用户来说，无论他们是内部用户还是外部用户，都必须通过身份感知访问代理来访问所有的应用程序——不管其托管在何处。这些代理不仅应当执行标准身份验证，还应当使用防网络钓鱼的多重身份验证，例如 Akamai MFA。此外，还应当具备强大的设备态势功能，以获取设备条件来允许访问特定应用程序。

我们坚信，ZTNA 不会止步于身份验证和授权。为了支持 Zero Trust 原则，应当在激活会话期间持续监控在初始身份验证和授权阶段检查的所有参数。检测到任何更改时都应当触发一项相关操作，例如重新对用户进行身份验证、移除对应用程序的访问权限或限制对应用程序的访问。

应当位于访问代理之上的一个关键安全系统是 Web 应用程序和 API 保护 (WAAP)，它将确保最终用户不会（有意或无意）向您的内部应用程序发起应用程序级攻击。您可以对非 API 站点使用其他高级系统（例如，人类/爬虫程序检测），以帮助确保恶意软件不会在有效端点背后实施伪装。Akamai 可以在 IAP 中布置 WAAP、爬虫程序检测、行为分析和缓存。这旨在提供出色的性能，并且能够让潜在的攻击者尽可能远离您的物理位置、应用程序和数据。

随着您的应用程序上线并且可通过访问代理进行访问，防范分布式拒绝服务 (DDoS) 攻击变得更加重要。您应当与可吸收针对您的微边界和访问代理发起的攻击的提供商进行合作，从而实现在高负载下持续运行。

最后，为了确保您的应用程序拥有出色的性能，同时确保用户不仅可以接受这种访问方式上的转变，还可以对它表示拥护，应当在您的访问代理前设置可以提供性能优势的网络。具体而言，内容交付网络和互联网路由覆盖应当成为您资源的一部分，以便不仅提供访问，还要让它具备比之前的方法更出色的性能。

威胁防护

Akamai Enterprise Application Access 等解决方案可以保护您的应用程序免受恶意攻击者的侵害。但是，对于因为遭到入侵（例如，通过感染恶意软件的设备或通过网络钓鱼链接和登录页遭到窃取的凭据）而无意中成为此类攻击者的用户来说，该如何保护他们？在此情况下，防范和检测对于 Web 流量至关重要。

一种方法是部署基于云的 DNS 防火墙解决方案，例如 Akamai Secure Internet Access。该产品可以检查用户发出的每个 DNS 请求并应用实时威胁情报，从而正常解析良性请求，但主动拦截对恶意域的任何请求。这会降低员工设备遭到恶意软件或勒索软件攻击的风险，也可以降低员工成为网络钓鱼攻击受害者的风险。

总结

在如今的云和移动环境中，传统的集散式网络架构以及它们使用的城堡和护城河式安全边界已经无法有效提供性能和安全保障。这是所有公司必须开始解决的问题，否则他们将容易受到攻击。未能过渡到更安全的企业安全架构是当今企业遭受入侵的头号原因，并且入侵次数只会越来越多。简而言之，边界不能为您保证安全，因为边界本身不再存在。

后续行动

如何开始向 Zero Trust Network Access 架构过渡？

Akamai 的云安全服务可以组合构建一个全面的 ZTNA 架构，这不仅可以在多云环境中实现安全的应用程序访问，还可以利用云来几乎完全消除对于内部公司网络的需求。

通过使用高级分布式 IAP 解决方案、防网络钓鱼的多重身份验证以及 Akamai Connected Cloud 的强大功能，您最终可以非常轻松地迁移到一个没有边界的环境中。在此过程中，您将分阶段过渡应用程序，这几乎完全消除了您的迁移风险，并且 Akamai 在成熟可靠的性能和安全解决方案方面拥有的丰富经验将为您提供助力。

随着您向着 Zero Trust 继续迁移，您可以放心，Akamai 将在每个步骤为您提供助力，帮助您将网络转变为先进的架构，从而不仅可以为您的应用程序和数据提供访问，还可以提供易于管理的访问方式，与此同时维持高水平的安全性和性能。

详细了解如何借助 Akamai Zero Trust 产品组合满足业务需求。

Akamai 支持并保护网络生活。全球各大优秀公司纷纷选择 Akamai 来打造并提供安全的数字化体验，为数十亿人每天的生活、工作和娱乐提供助力。Akamai Connected Cloud 是一种大规模分布式边缘和云平台，可使应用程序和体验更靠近用户，帮助用户远离威胁。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号。发布时间：2024 年 2 月。

扫码关注 · 获取最新CDN前沿资讯