Akamai

企业需要 Zero Trust 安全解决方案的 4 大理由

目录

前言

攻击手段的日益复杂，勒索软件团伙的数量激增以及技术发展带来的新型漏洞，促使越来越多的企业开始转为采用 Zero Trust 安全模式。从本质上讲，这种方法消除了对用户、应用程序和设备的隐性信任，而隐性信任恰恰是以往安全方法的核心原则。实际上，在遇到以下四种重要情况时，企业将会从 Zero Trust 安全模式中受益匪浅：公司遭到勒索软件攻击时，向远程工作方式转型时，需要保护云环境的安全时，以及应对即将到来的安全审核时。

上述四种情况是近期出现的一些新趋势产生的结果，包括勒索软件攻击数量攀升、向混合工作团队的转型、向云计算的迁移以及安全审核需求的增加。在这些趋势的影响下，企业需要一种基于身份验证的安全方法，可以突破地点的制约，并且能够主动采取措施来应对安全漏洞。而 Zero Trust 方法恰好可以满足企业需求，此方法要求对用户进行严格身份验证才能访问数据，并且在遭遇攻击后能够主动采取抵御措施。

实施 Zero Trust 策略看似会让本已负担过重的安全团队雪上加霜，但其实并非如此。通过分阶段方法并专注于速效方案，您可以降低传统安全解决方案的某些复杂性和风险，进而增强您的安全态势。

您不必完全淘汰和更换现有的技术即可开始使用。首先，您可以从当下最为紧迫的业务需求着手，选择与之相匹配的 Zero Trust 投资。我们建议您选择值得信赖的 Zero Trust 供应商，而不是那些一夜之间就将旧版解决方案重新包装成 Zero Trust 的供应商。另外，也强烈建议您选择能够将 Zero Trust 安全的多个要素（Zero Trust Network Access、DNS 防火墙、微分段等）整合到一个平台下的供应商。无论您出于何种原因采用 Zero Trust，它都能够帮助您实现业务敏捷性、成本优化和工具整合，进而改善整体运营。

企业转向 Zero Trust 的 4 大理由

勒索软件攻击数量逐渐攀升

员工转向混合工作模式

云计算资源采用日益广泛

合规性要求日趋严格

01

勒索软件攻击数量逐渐攀升

提升勒索软件防护能力

在过去几年中，勒索软件攻击干扰了全球各地的企业，遍及医院、银行，乃至管道和其他关键基础设施。实际上，**Cybersecurity Ventures** 预计，到 2031 年，勒索软件每年将给受害者造成大约 2,650 亿美元的损失。该公司还预测，随着勒索软件犯罪分子逐步改进其恶意软件攻击负载和相关勒索活动，他们将每两秒就发动一起针对消费者或企业的新攻击。

如果不采用 Zero Trust 策略，勒索软件团伙则可能会利用以下弱点：

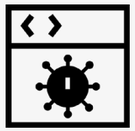
- 对用户、应用程序和网络的隐性信任让成功入侵网络的攻击者能够横向移动并传播恶意软件
- 过度授权的访问策略可能导致能够用来注入勒索软件的感染
- 仅以密码作为信任凭据的系统可能为凭据盗窃提供机会

Zero Trust 如何助您一臂之力

企业通过实施 Zero Trust 架构、访问控制策略和使用微分段能够最大限度地限制此类攻击可能造成的破坏。攻击者不仅一开始更难入侵系统，而且扩张能力也将受到限制。

Akamai 如何打破勒索软件杀伤链

勒索软件攻击通常涉及初始感染、横向移动以及数据外泄和加密。借助 Zero Trust，企业能够在每个步骤发生的同时进行应对，甚至在发生前就加以防范。



初始感染

Akamai Guardicore 平台可防止攻击传播到初始入侵点以外，同时 Akamai MFA 可保护用户凭据免遭盗窃和滥用。

横向移动

Akamai Guardicore 平台可减少传播路径并帮助防止横向移动。Akamai Guardicore Access 可限制攻击者的移动能力，使其难以感染企图利用的应用程序。Akamai Hunt 可检测和抵御您网络中隐匿的高级威胁。

数据外泄和加密

Akamai Guardicore 平台可限制对关键应用程序的访问，阻止攻击者访问所入侵网络中的敏感数据。Akamai Secure Internet Access Enterprise 可阻止向钓鱼网站及命令和控制网站发送请求。最后，Akamai Hunt 可监测异常行为，防止攻击者对可用于勒索的高价值数据进行加密。

02

员工转向混合工作模式

保护新型混合工作团队的安全

对于依赖防火墙、VPN 等过时安全工具的企业而言，要想确保新冠疫情期间不断发展壮大并且数量越来越多的新型混合工作团队的安全将更具挑战性。远程访问 VPN 在大约 30 年前首次出现，那时一切都不一样：网络处于发展初期，应用程序还在数据中心运行，从远程位置连接的用户数量要少得多。继续使用 VPN 对用户进行身份验证并授予其全网访问权限将扩大攻击面，同时为传统 VPN 带来的很多零日漏洞敞开大门。任何用户只要拥有必要的凭据，便可以登录公司 VPN，随后可以在整个网络中横向移动，访问 VPN 保护的资源。

Zero Trust 如何助您一臂之力

Zero Trust 基于最低权限访问原则，假定任何用户或应用程序都不应获得固有的信任。Zero Trust Network Access (ZTNA) 采取与 VPN 截然不同的方法来确保远程员工的访问安全可靠。与将整个网络置于风险之下的传统安全策略不同，Zero Trust 会将用户直接与其需要的应用程序和数据相关联，从而避免恶意用户在获得过度授予的敏感数据和资源访问权限后进行横向移动。如果出现入侵，有效的 Zero Trust 微分段解决方案能够实现内部网络分段，确保入侵不再扩散并破坏网络的其他部分。**Gartner** 预计，到 2025 年，至少 70% 的新增远程访问部署都将由 ZTNA 而非 VPN 提供服务，而在 2021 年底，这一比例还不到 10%。

Akamai 如何助力混合和远程办公

Akamai 全面的 Zero Trust 平台能够满足您的混合工作团队的需求。优势如下：

降低风险

Akamai 将适当的用户直接与相应的应用程序相关联，从而缩小攻击面并限制横向移动。

改善用户体验

远程用户访问资源不受应用程序、设备或位置限制，不再需要建立和中断与 VPN 的连接。

提升敏捷性

Akamai 的解决方案以服务的形式提供，企业无需部署硬件，需求增长时无需担心规模扩展，因而可降低成本和复杂性。

03

云计算资源采用日益广泛

轻松实现云迁移

企业将应用程序迁移到云端，以获得更高的灵活性和敏捷性，并实现基础架构现代化。然而，这些云环境会造成攻击面扩大并带来新的安全要求。不同的云端和本地环境的整合可能会破坏应用程序并带来安全风险。对于使用 VPN 和防火墙等传统网络架构的企业，在尝试将应用程序迁移到云端时，他们常常面临更大的横向移动威胁风险、较差的可扩展性和高昂的成本。即便在迁移完成后，还需确保资产安全，并且必须根据角色权限对用户进行身份验证。较之本地环境，云基础架构用户通常对资源、服务和管理权限拥有更大的访问权，这也带来了额外的风险，可能造成中断。

Zero Trust 如何助您一臂之力

Zero Trust 策略有助于迁移到云端。Zero Trust 将消除许多基于云的应用程序（尤其是第三方应用程序）固有的隐性信任，这种信任可能会导致漏洞。Zero Trust 解决方案可确保企业能够更轻松地部署基于云的应用程序并获得更强有力的保护。为云端部署 Zero Trust 能够带来的优势如下：

- ☑ 更出色的监测能力，可更好地监测资产和风险
- ☑ 更小的攻击面，通过 Zero Trust 分段及仅提供对云资源的最低访问权限可缩小攻击面
- ☑ 经现代化改造的网络基础架构，可带来速度和敏捷性方面的提升
- ☑ 更低的运营成本和复杂性

Akamai 如何改善云迁移

Akamai 的 Zero Trust 解决方案能够帮助您自动迁移资产及其各自的策略。这无需停机且不会扰乱业务。Akamai 可提供：

更出色的监测能力

您可以更好地了解应用程序依赖关系，从而制定有效的云分段策略，以缩小攻击面并最大限度降低风险。

Zero Trust Network Access

用户只有通过强身份验证，才能连接到其有权访问的应用程序。

威胁搜寻

Akamai 专门的威胁搜寻团队始终致力于搜寻云环境中的匿名攻击行为，告知客户其网络存在的任何风险。

04

合规性要求日趋严格

轻松满足合规性要求并降低风险

安全负责人明白，满足合规性要求并不意味着企业真正安全，但安全审核仍旧是高管团队的头等要事。他们知道，一旦未能通过审核，就会造成重大业务中断，影响利润。对于安全团队而言，合规性评估是最消耗时间和资源的任务之一。此外，随着企业向无边界数字环境的转变及远程办公的盛行，这项任务变得愈发困难。企业通常需要隔离环境、为管制资产建立安全围栏，以满足《支付卡行业数据安全标准》(PCI DSS)、《健康保险流通与责任法案》(HIPAA)、环球银行金融电信协会 (SWIFT) 等合规性标准。

各企业还需要应对远程用户、公司本地用户、合作伙伴、供应商等，这使得企业环境的边界几乎无法确定。访问控制是审核成功与否的主要决定因素之一。安全团队在准备审核时，必须回答以下问题：

- **如何限制对敏感信息的访问，以使其仅向授权用户开放？**
- **如何确定审核环境的范围？**
- **如何简化审核过程并减少混乱？**

Zero Trust 如何助您一臂之力

幸运的是，Zero Trust 方法可有助于回答以上所有问题以及更多问题。显式验证能力以及支持最低访问权限的能力是 Zero Trust 的两大关键能力，能够大幅度简化合规工作流程。各企业可以将受监管资产与数据中心或云的其他流量隔离，并根据身份而非位置允许访问。增强的监测能力可以显示出其受监管环境的进出流量，并帮助确定范围中的内容。这能够大幅降低审核的复杂性和成本，简化审核员的工作。

Akamai 如何助力满足合规性要求

Akamai 全面的 Zero Trust 产品组合可帮助您为 PCI DSS、HIPAA、国际标准化组织 (ISO)、《萨班斯-奥克斯利法案》(SOX) 或任何其他框架下的每一场审核做好准备。Akamai Enterprise Application Access 可控制第三方对敏感个人信息的访问，从而满足《通用数据保护条例》(GDPR) 的要求。Akamai Guardicore Segmentation 提升了对受 PCI DSS 管制的资产的理解，通过隔离票据交换功能满足 HIPAA 的规定，通过限制网络访问、隔离关键系统满足 SWIFT 法规的要求。Akamai MFA 保护 HIPAA 患者信息，使其免受获得医疗系统密码的攻击者的攻击，并且它可以通过防止凭据泄露加强 SWIFT 合规性。

一家全球银行在两周内实现 SWIFT 合规性

外部监管机构要求 Akamai 的一家全球银行客户为其所有关键应用程序建立安全围栏，以满足 SWIFT 的要求，保障金融机构间资金转账安全。一般而言，一个诸如此类的应用程序需要在不同地点部署 100 多个服务器，包括裸机服务器和虚拟服务器。通常情况下，与该客户同等规模的银行计划和实施上述过程需要花费 8 到 12 个月，因为这需要为跨多个位置的分段创建一个虚拟局域网 (VLAN)。明确 SWIFT 应用程序的依赖关系以及确保规则集正确且不会产生破坏，会进一步增加项目所需的时间。同时，上述项目还需要购买新的防火墙设备。由于 SWIFT 应用程序对银行业务至关重要，该银行无法承受停机造成的后果。总而言之，分段项目预计需要很多人投入大量精力。但是，在 Akamai 的帮助下，全过程仅由一位安全工程师花费大约两周时间便大功告成，不需要任何网络更改，银行也避免了任何应用程序变化或停机。

简化并加快实现合规

全球银行

- 需要为 SWIFT 应用程序建立安全围栏
- 包含裸机、VMware 和 OpenStack 服务器的复杂环境

传统分段

- 难以在复杂的基础架构下定义分段
- 无法监测应用程序和依赖关系
- 需要停机
  时间：8–12 个月
  人员：至少 5 人

Akamai Guardicore Segmentation

- 几小时内便可完成 SWIFT 应用程序映射
- 自动建议和优化分段策略
- 无需购买或部署新的硬件和防火墙
- 不需要停机
  时间：2 周
  人数：1 位架构师

详细了解如何借助 Akamai Zero Trust 产品组合满足业务需求

了解更多

Akamai Security 可为推动业务发展的应用程序提供全方位安全防护，而且不影响性能或客户体验。诚邀您与我们合作，利用我们规模庞大的全球平台以及出色的威胁监测能力，防范、检测和抵御网络威胁，帮助您建立品牌信任度并实现您的愿景。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 9 月。