Akamai | TechnologyAdvice

Zero Trust 架构从三个方面为金融机构保驾护航

金融机构仍然是网络攻击者的主要目标，2023 年第二季度发生的 Web 应用程序和 API 攻击与去年同期相比增加了 65%。愈演愈烈的网络威胁不仅会消耗企业的宝贵资源，还使企业无法专注于重要的核心业务功能。

传统防火墙和端点解决方案会隐式信任经过密码和用户名初步审查的端点、设备和用户，只偶尔通过多重身份验证 (MFA) 强化审查。除了基本的端点恶意软件监控之外，通常未对网络内运行的应用程序、API 和系统服务执行进一步的安全审查。为了应对日益加剧的勒索软件威胁、严格的法规要求和云迁移的挑战，许多金融机构现在开始采用 Zero Trust 架构。

Zero Trust 架构可以消除隐式信任，并根据相应的请求和权限，持续验证所有应用程序、用户和设备的访问权限。即使攻击者能够侵入设备或窃取凭据来访问网络，其访问也会受到严格限制，攻击造成的损害也会显著降低。

Zero Trust 框架具体如何为金融机构保驾护航？

满足不断变化的法规要求

金融机构必须投入大量资源来证明自身对各项法规的遵从性，例如确立已久的《支付卡行业数据安全标准》(PCI DSS) 或即将出台的《数字运营弹性法案》(DORA)，该法案预计将于 2025 年 1 月全面实施。由于要求不明确、相互冲突和不断变化，审计工作的复杂性、成本和时间频繁增加，但金融机构不得不在这方面投入资金，因为审计不过关还可能导致收入损失、监管制裁、罚款或处罚，以及声誉损失和潜在的法律责任。

合规报告需要对涉及监管数据的系统进行清晰、准确地记录，并要求证明这些系统受到充分保护。然而，在大型金融机构中，IT 环境太庞杂、太琐碎，不易于跟踪资产和访问情况。

传统防火墙和端点保护工具主要跟踪和保护传统用户及资产。依赖这种传统方法进行网络分段会给运营扩展带来挑战，妨碍策略的创建和执行，并限制敏捷性。

为了利用符合未来战略的技术来克服遗留环境的挑战，金融机构需要对东西向流量实施精细的监测并且能在多云和容器环境中实施分段策略。随着企业愈加需要管理多个区域和多种 IT 基础架构类型（包括容器技术），金融机构需要采取最简单直接并且具备策略灵活性、DevOps 集成和自动化能力的微分段方法。

金融机构如果不能定期识别、跟踪和保护所有资源，就无法确保对监管数据的访问始终处于完全控制和保护之下。如果对数据、用户、应用程序或设备的监控不重视或不充分，会使网络攻击的风险显著增加，并可能导致合规审计不过关。

Zero Trust 架构默认拒绝访问，所有连接必须被授予明确的上下文——只有已授权设备上的已授权用户才能对所请求的数据进行权限内的访问。Zero Trust 默认使用最小访问权限，会中断被遗忘或未知的遗留连接。Akamai 的解决方案可快速识别恶意设备、遗留用户（人员、API 或应用程序）和被遗忘的数据源，这些数据源可能大量存在于旧的分支机构或被收购企业的遗留技术环境中。

无论用户位于何处，Akamai 的 Zero Trust 架构都适用，但可将位置上下文纳入访问决策过程中。安全团队可获得统一控制和报告能力，这是快速分析和全面管理本地网络、数据中心或云中资源访问所必须具备的能力。

在保护关键应用程序和东西向流量方面，金融机构面临的监管压力日益加大，为此，这些机构正致力于提高对运营环境的监测和了解。通过采用 Zero Trust 原则，金融机构现在可以对不合规的资产进行无缝识别和分段，让应用程序团队能够自主管理分段策略。这确保了高效的工作流并简化了报告流程。

全面监测东西向流量并掌握背景信息丰富的流量数据有助于轻松映射和隔离业务关键型应用程序，而无需更改基础架构或应用程序。这种能力使金融机构能够限制第三方访问并增强整体安全性。

拥有监测能力可简化向云端安全迁移的过程；同时，将分段集成到 DevOps 周期中可确保即时更新策略而无需大量修改基础架构，这和以往的 VLAN 实践不同。此外，Akamai 还能帮助企业实现并简化多种基础架构合规策略的统一创建、执行和报告。这是通过更强的监测能力、应用程序依赖关系映射、自动化分段策略、DevOps 策略自动化和无缝变更管理集成来实现的。

防止勒索软件传播

从分支办事处到全球性金融机构，勒索软件攻击引起了广泛关注并成为全球性挑战。根据 Cybersecurity Ventures 发布的《2022 年勒索软件市场报告》，“预计到 2031 年，勒索软件将每两秒攻击一家企业、一位消费者或一台设备。”

由于金融服务机构经常通过并购发展壮大，因此他们往往对自身的整个技术生态系统缺乏了解，从而为攻击者留下了可乘之机。勒索软件攻击者利用后门或网络钓鱼攻击来窃取凭据或在端点上投放可逃避端点保护措施的未知恶意软件。

过度宽松的用户访问策略和以密码为中心的身份验证方法使攻击者能够绕过防火墙、逃避端点检测，不受限制地访问对流量、用户和连接的设备隐式信任的网络。勒索软件攻击者通常是有组织的团伙（例如 CL0P），他们利用已成功入侵的资产，在网络中横向移动，继续发现并利用其他易受攻击的资产。通过利用零日漏洞（例如 MOVEit SQL 注入漏洞），攻击者可以获得访问权限并使用自动化脚本对系统进行加密、窃取数据和投放勒索请求，快速扩大攻击范围。

Akamai 的 Zero Trust 解决方案使金融机构能够识别和隔离关键系统，并限制进出这些系统的网络访问。这种方法可以最大限度降低勒索软件攻击的可能性和影响，并减少修复漏洞所耗费的时间。首先，我们跟踪并监控恶意域和 IP 地址，根据情况进行分区隔离控制，防止发生多次攻击。

随后，凭借对网络流量的近实时的监测能力，我们能够观察并控制进程级和服务级的流量。这种深度洞察力使安全运营中心和网络运营中心的团队能够准确识别当前的具体威胁并采取针对性措施。

接下来，即使攻击者得逞，Akamai Guardicore Segmentation 内置的微分段技术也能够将攻击限制在最小范围。每个访问请求都将不断进行凭据和权限验证，而且受 Akamai Enterprise Application Access 保护的应用程序会拒绝所有连接。

此外，用户未请求的应用程序、服务器和其他资源将自动隐藏起来不被发现，以防止攻击者进行横向移动或扩大访问范围。最后，Akamai Hunt 的异常检测功能会标记异常行为，向安全团队发出告警以帮助他们识别攻击，避免数据遭到窃取或加密。

提升数字化转型效率

为了实现敏捷性、可扩展性和现代化，许多金融机构将应用程序迁移到云端。但是，这样的迁移带来了许多新的挑战。

首先，金融机构无法迁移未检测到的、未知的资源和连接。其次，云迁移不仅扩大了攻击面，多云和本地混合云集成通常会破坏应用程序，并在既有的安全层中形成漏洞。再者，软件可部署的基础架构（容器、虚拟机等）自动部署的速度太快，无法使用原有解决方案进行有效的保护或监控。

Zero Trust 解决方案确保金融机构能更轻松地部署基于云的应用程序，同时获得更强有力的保护并降低运营开销。Akamai 的 Zero Trust 解决方案可跟踪所有数据流，快速识别潜在的攻击面并执行策略，而不会造成业务中断。

完成识别后，安全和运营团队可利用 Akamai 的集中控制措施对应用程序进行分段和保护，并监控数据流。Akamai 解决方案可提供精细控制措施，同时降低运营成本和复杂性。对于金融机构内的安全和运营团队来说，实施通用策略可确保快速灵活地完成基础架构现代化。这是因为 Zero Trust 最小权限分段策略可提供可靠的安全防护，能够抵御不断变化的威胁。

忽视 Zero Trust 会给金融机构带来无法承受的损失

针对金融机构原有技术的攻击可能会导致重大数据泄露，造成数额巨大的损失，并毁掉客户和合作伙伴的信任。网络攻击越来越复杂，速度也日益加快，金融机构如果无法全面监测其技术生态系统，可能会给网络犯罪分子留下可乘之机。

Akamai 解决方案能够更好地监测网络，运用智能策略限制用户访问，持续搜寻威胁并标记任何异常情况，以进行安全审查。点击链接进一步了解金融机构如何利用 Akamai Zero Trust 产品组合满足自身需求。

进一步了解 Akamai 如何为您的数字金融业务保驾护航

了解更多

TechnologyAdvice | Akamai

无论您在何处构建内容，以及将它们分发到何处，Akamai 都能在您创建的一切内容和体验中融入安全屏障，从而保护您的客户体验、员工、系统和数据。我们的平台具备监测全球威胁的能力，这让我们得以帮您调整并增强安全状况，从而实现 Zero Trust、阻止勒索软件、保护应用程序和 API 或抵御 DDoS 攻击，让您信心十足地不断创新、发展和转型。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。

扫码关注，获取最新CDN前沿资讯