白皮书

# Akamai 助力构建 Zero Trust 成熟度模型

## 支持为联邦机构和部门实现 CISA 的跨领域功能

# 前言

Zero Trust 安全已成为保护敏感政府数据、关键基础设施和国家安全系统的黄金标准。面对现代威胁，联邦机构和部门不能再依赖基于边界的传统安全模型。网络犯罪分子变得越来越狡猾，他们利用了凭据盗窃、勒索软件和内部攻击等诸多高级手段。为应对此情况，联邦机构正加速将其安全策略向 Zero Trust 框架调整。但这只是一种零散的转变，还需要采取更多措施来保护联邦系统。

美国网络安全和基础架构安全局 (CISA) 的 Zero Trust 成熟度模型可以帮助联邦机构和部门实施安全原则，以消除隐含信任并执行严格的验证机制。该模型构建于五大基础支柱之上：身份、设备、网络、应用程序和工作负载、数据。此外，还有三种跨领域功能：监测与分析、自动化与编排以及治理，可以确保实施全面且一致的网络安全防护。

要想实现这些目标，就需要将微分段视为 Zero Trust 安全的核心原则，使其成为内部（即东西向）网络防御的基本组成部分。通过对工作负载分段以及限制横向移动，联邦机构可以遏制潜在的违规行为并实施 Zero Trust 政策。此外，还应实施全面的应用程序编程接口 (API) 安全解决方案以保护外部（即南北）通信，确保只有授权实体才能访问政府应用程序。

本白皮书探讨了实现 Zero Trust 成熟度的重要步骤，重点介绍了 Akamai 的高级安全解决方案（包括 Akamai Guardicore Segmentation、Akamai API Security 和 Akamai Enterprise Application Access）如何帮助联邦机构和部门遵循 CISA 指导并增强其网络安全态势。

# 从基于边界的安全防护转向 Zero Trust

传统的网络安全依赖基于边界的防御，它会假设只要能进入网络的实体都可以被信任。但面对现代网络威胁，这一模式已经屡屡失效。为获取敏感信息的访问权限，攻击者会利用保护不力的凭据和配置错误的安全设置，并使用横向移动技术绕过传统防御机制。

而 Zero Trust 则要求对用户、设备、应用程序和网络流量进行持续验证，从而消除隐含信任。每次访问请求都会经过身份验证和授权，并根据实时风险评估进行持续监控。即使攻击者侵入了部分网络，这种方法也可以显著减小攻击面，并防止未经授权的访问。

# CISA 的 Zero Trust 成熟度模型

CISA 的 Zero Trust 成熟度模型为联邦机构和部门逐步增强其安全框架提供了路线图（见图）。该模型构建于五大关键支柱之上：

- **身份：**实施强有力的身份验证、授权和访问控制，确保只有合法用户才能与敏感资源互动
- **设备：**监控、保护和验证端点设备，确保它们必须符合安全策略才能访问政府网络
- **网络：**实施微分段和高级访问控制策略，防止未经授权的横向移动
- **应用程序和工作负载：**实施基于身份的严格访问策略、运行时安全性和 API 安全控制，从而保护应用程序和工作负载
- **数据：**确保敏感的政府数据得到加密、监控和保护，防止未经授权的访问并避免被泄露


CISA 的 Zero Trust 成熟度模型支柱（来源：CISA）

除了这几大支柱外，该模型还集成了适用于所有 Zero Trust 组件的三大关键跨领域功能：

- **监测与分析：**持续监控、记录和异常检测，以实时识别和抵御威胁
- **自动化与编排：**AI 驱动的安全防护自动化，以实施策略、响应威胁并简化访问控制
- **治理：**集中的策略执行以确保遵守联邦法规，例如《联邦信息安全现代化法案》(FISMA) 和美国国家标准与技术研究所 (NIST) 特殊出版物 800-207

# 微分段与 API 安全防护的重要性

在传统的网络安全模型中，通常是使用基于网络的防火墙将网络划分为宽泛的分段。虽然这种方法可以提供一定程度的安全防护，但它缺乏彻底保护现代分布式环境所需的精细度。在联邦环境中，基于网络的分段通常会导致过度调配；也就是说，用户和应用程序可以访问的资源要多于其实际需求。这会在无意之中为横向移动创造条件。攻击者只要破坏网络的一个部分，就能毫无障碍地移动到更敏感的区域。

微分段概念引入了对网络内东西向流量的精细控制，从而解决了这一挑战。在微分段环境中，每个应用程序、工作负载或服务都与其他部分隔离开来，并且根据特定策略来限制访问。这可以确保用户、设备和应用程序只能与其获得明确访问授权的资源进行通信。通过实施基于身份的应用程序感知分段，微分段可以限制网络攻击的潜在损害、减小攻击面，并强化 Zero Trust 原则。

在南北向网络流量方面，联邦网络越来越依赖 API 来推动系统之间的通信。这样，API 端点保护就成为了首要之务。近年来，包括注入攻击、撞库攻击和未经授权数据访问在内的 API 攻击愈演愈烈。联邦机构和部门需要全面的 API 安全解决方案，它们应该为 API 提供全生命周期保护，从而使安全人员能够实时发现、监控和保护其 API 流量。API 发现尤为重要——企业存在未被发现的 API 这种情况很常见。

## Akamai Zero Trust 解决方案概览

### 身份

**Akamai MFA** 是一种免密钥 FIDO2 身份验证解决方案，可以保护员工帐户免受网络钓鱼和其他中间机器攻击。它能确保只有经过强有力身份验证的员工才能访问自己负责的帐户。其他访问都会被拒绝，并且可以预防员工帐户接管。

### 设备

**Akamai Guardicore Segmentation** 是一款出色的微分段解决方案，旨在限制勒索软件和其他恶意软件的传播。通过在设备上持续监控和执行策略，Akamai Guardicore Segmentation 可以验证设备配置、软件安装和潜在漏洞，从而确保只有符合要求的设备才能访问网络。此外，该解决方案还支持采用无代理方法来保护物联网设备。

**Akamai Enterprise Application Access** 是一款全面的 Zero Trust 网络访问解决方案，可以确保只有经过身份验证的用户和设备才能访问应用程序。Enterprise Application Access 可以验证设备的身份和安全态势，从而对 Akamai Guardicore Segmentation 的功能形成了补充。如果发现设备不符合要求或存在安全风险，Enterprise Application Access 可以限制其访问敏感应用程序。

### 网络

**Akamai API Security** 可实现对南北向流量的持续发现和实时分析，使联邦安全专家拥有了对整个 API 资产的全面监测能力。 该解决方案可以检测未知 API、识别漏洞并分析 API 行为，使安全团队能够在这个快速增长的攻击面中检测攻击并消除风险。

**Akamai App & API Protector** 将 Web 应用程序防火墙、爬虫程序抵御、API 安全性和第 7 层分布式拒绝服务 (DDoS) 防护整合到一个解决方案中。它能够快速识别漏洞，抵御整个网络和 API 资产所面临的各种威胁。

**Akamai Secure Internet Access Enterprise** 是一款基于云的安全域名服务 (DNS) 防火墙，它能确保用户和设备在任何位置都能安全地连接到互联网，而且不存在其他安全解决方案固有的复杂性和管理开销。

**Akamai Guardicore Segmentation** 提供了对网络流量的精细控制，从而确保只允许存在合法流量。

## Akamai Zero Trust 解决方案概览

### 应用程序和工作负载

无论员工、第三方承包商、合作伙伴和移动用户身在何处，**Akamai Enterprise Application Access** 都能为其提供 Zero Trust 访问。

**Akamai Guardicore Segmentation** 可帮助监测并了解应用程序和工作负载。

### 数据

**Akamai Secure Internet Access Enterprise** 提供了内容过滤、高级威胁防护和数据丢失预防等功能，从而实现安全的数据访问。它支持数据清单管理，可预防未经授权访问和数据泄露。

# Akamai Guardicore Segmentation：东西向流量防护的关键因素

Akamai Guardicore Segmentation 是一款出色的微分段解决方案，旨在帮助各大实体（特别是联邦机构和部门）在本地和云环境中实施精细的安全控制

## 工作负载和应用程序的精细分段

与在网络级别控制访问的传统分段不同，Akamai Guardicore Segmentation 是在应用程序和工作负载级别实施安全策略。这样可以确保访问受到严格限制。例如，在一家联邦机构中，可以将人力资源 (HR) 应用程序限制为仅与其指定的 HR 数据库进行通信，从而在遭受攻击时阻止攻击者横向移动。

## 基于身份的微分段

在实施分段时，Akamai Guardicore Segmentation 基于的是用户和设备身份，而不只是基于 IP 地址。这样可以确保根据角色、信任程度和实时验证来动态授予访问权限。例如，可以将承包商和第三方合作伙伴限制为仅能访问自己需要的系统，从而降低未经授权访问的风险。

## 动态实施策略

Akamai Guardicore Segmentation 可以根据实时因素（如用户行为、设备健康状况和网络活动）不断调整安全策略。如果检测到可疑活动，例如数据传输量异常，Akamai Guardicore Segmentation 可以自动限制访问、阻止流量或提醒安全团队。这种主动型方法可确保安全策略不断发展，以应对新出现的威胁。

通过集成 Akamai Guardicore Segmentation 的微分段，企业可以加强其 Zero Trust 架构、最大限度地降低风险，并对其网络保持严格的访问控制。

案例研究

## 联邦环境中的 Akamai Guardicore Segmentation

为保护内部系统免遭横向移动攻击，一家联邦机构最近实施了 Akamai 的微分段解决方案。在采用 Akamai Guardicore Segmentation 之前，该机构依赖基于网络的传统分段技术，这种技术提供的精细度有限，并且允许在不同网络分段之间进行广泛访问。当网络的任何部分受到攻击时，这将产生巨大的横向移动风险。

利用 Akamai Guardicore Segmentation，该机构能够：

- 实施精细的分段：通过在应用程序级别进行工作负载分段，该机构降低了横向移动的风险，并能确保每个应用程序只能与自己需要的资源进行通信。
- 提升监测能力: 该解决方案的可视化工具为该机构提供了对其内部流量的深入洞察，使安全团队能够实时识别并抵御潜在威胁。
- 增强安全性：通过将 Akamai Guardicore Segmentation 与其现有身份管理和访问控制系统集成，该机构得以在整个网络中实施 Zero Trust，同时确保根据实时风险评估对访问进行持续监控和动态调整。

这一示例展现了 Akamai Guardicore Segmentation 在提高网络安全性、降低横向移动风险，以及确保始终将权限保持在最低限度方面的强大功能。

# API 安全防护：保护南北向流量

Akamai 提供了多种可确保 API 安全的解决方案。Akamai 的 API 安全平台可以确保全面监测 API 交互，并实时自动检测和抵御针对南北向流量的威胁。凭借高级行为分析，联邦机构和部门能够：

- **识别影子 API**，防止其被攻击者利用
- **监控 API 流量模式**，以检测未经授权的访问企图
- **实施 API 速率限制**，防止滥用和拒绝服务攻击
- **识别已忘记、被忽略或未知的 API**，以发现潜在攻击路径
- **列出所有 API**，且不受配置或类型限制（包括 RESTful、GraphQL、SOAP、XML-RPC、JSON-RPC 和 gRPC）

Akamai Secure Internet Access Enterprise 是一款基于云的 DNS 防火墙，可以帮助安全团队确保所有线上和线下用户及设备安全连接到互联网。它可以主动阻止恶意 DNS 请求，包括恶意软件、勒索软件、网络钓鱼和低吞吐量 DNS 数据泄露。Secure Internet Access Enterprise 无需部署、管理和升级任何应用程序，从而降低了安全工作的复杂性。该解决方案简单直观，非常容易使用。

Akamai App & API Protector 可以发现并抵御通过 Akamai Cloud 运行的应用程序和 API 所面临的 API 威胁，并可以阻止包含 Akamai API Security 发现的存在潜在威胁的任何流量。在联合部署的情况下，Akamai 的 API 防护措施可对 API 提供全面、持续的监测，让安全人员能够发现、审计、检测和应对全部应用程序资产中的 API 安全问题。

# 利用 Zero Trust 实现跨领域功能

Zero Trust 架构面临着一些重大挑战，其中之一就是形成技术孤岛的风险。每个孤岛通常都是独立运行，导致安全控制、策略执行和威胁检测各自为政。因此，跨所有安全层的集成就变得至为重要。

对于管理高度敏感数据和复杂基础架构的联邦机构和部门来说，这种零散的方法可能会带来重大的安全风险。攻击者可以利用孤岛（或支柱）之间缺乏监测能力的漏洞，或者利用不同系统之间不一致的策略执行。为了降低这些风险，联邦机构必须采用统一的跨支柱安全模型，将所有支柱的监测、治理和自动化集成在一起，从而确保一致的政策执行，并减少对手可以利用的漏洞。

要想实现统一的安全模型，跨支柱集成就必须侧重于 CISA Zero Trust 成熟度模型的三个交叉领域：监测与分析、自动化与编排、治理。这些元素是实现 Zero Trust 架构的基础，在该架构中，访问和权限将根据实时风险评估在所有支柱之间动态调整。

## 监测与分析

在检测威胁、了解用户行为以及在所有支柱上实施动态安全策略方面，监测能力至关重要。如果不能完全监测身份、设备、应用程序和数据的交互方式，安全团队就会如同蒙在鼓里，很难检测到异常行为或未经授权的访问企图。Akamai 解决方案提供了全面的跨支柱监测能力。

- Akamai Guardicore Segmentation 可以监控已分段工作负载之间的网络流量，同时提供东西向流量监测能力，并检测网络内的任何横向移动企图。
- Enterprise Application Access 可以提供关于应用程序访问模式的洞察、跟踪用户如何与敏感应用程序交互，并确保根据上下文数据动态调整访问权限。

通过集成这些功能，联邦机构可以跨所有支柱关联数据，从而帮助以统一方式了解安全事件。当用户请求访问某个应用程序时，Akamai 的解决方案不仅可以检查用户的身份，还可以检查设备的安全性、它们正在使用的网络以及应用程序的实时行为。这样，安全团队就能更快地检测潜在威胁、最大限度地降低权限升级的风险，并确保根据实时风险评估来动态调整权限。

## 自动化与编排

跨多个系统的事件响应和策略执行可能是一个缓慢的过程，还可能需要手动完成。而在使用 Zero Trust 后，安全策略就必须在所有支柱上动态执行，这需要高水平的自动化与编排。这样可以确保随着风险水平的变化，权限会立即调整到最低必要水平，从而减少人为错误或延迟响应的可能性。Akamai 解决方案提供了跨身份、网络和应用程序安全的自动化工作流。

- Akamai Guardicore Segmentation 提供了自动化的微分段，并可根据实时流量模式和检测到的异常情况来动态调整网络分段策略。这样可以确保网络内的任何可疑活动都能被迅速隔离，从而阻止横向移动。
- Enterprise Application Access 实现了应用程序访问保护流程的自动化，可确保用户只能通过安全代理访问应用程序，并且权限会根据不断变化的风险因素不断更新。

通过实现这些流程的自动化，联邦机构和部门可以确保安全策略得到一致且快速的执行，从而减少攻击者的机会窗口。

## 治理

治理是任何安全策略的基石，可以确保策略得到一致的执行并满足合规要求。在跨支柱模型中，治理必须确保所有安全控制措施都符合 Zero Trust 原则。凭借 Akamai 解决方案，各大机构可以成功实施跨所有支柱的治理策略。

- 身份治理：确保采用一致的方式，跨设备、应用程序和网络实施基于身份的访问控制，同时根据实时风险评估定期审查和更新访问权限
- 网络治理：通过跨环境（包括本地、云和混合基础架构）执行网络分段和流量监控策略，Akamai Guardicore Segmentation 允许机构定义网络分段策略，并确保这些策略在整个基础架构中得到一致的实施
- 数据治理：确保按最低权限限制访问，并持续监控所有数据传输以防止未经授权的访问或可疑活动，从而保护敏感数据

Akamai 的技术旨在实现无缝协作，为联邦机构提供支持 Zero Trust 的完全集成、跨支柱安全架构。

案例研究

## 联邦机构内的跨支柱集成

一家大型联邦机构面临着重大挑战，其身份、网络和应用程序层采用的是零散的安全策略。身份验证、应用程序访问和网络分段由不同的系统进行管理，导致安全策略执行不一致、监测能力存在不足。

通过采用 Akamai 的集成解决方案，该机构能够：

- **统一实施身份和应用程序安全防护：**集成了 Akamai 的身份、凭据和访问管理 (ICAM) 解决方案 Enterprise Application Access，以确保应用程序访问权限始终根据实时身份数据得到验证。这样，该机构就能根据用户行为和设备健康状况来动态调整应用程序权限。
- **实施动态网络分段：**部署了 Akamai Guardicore Segmentation，以根据身份和应用程序访问权限对网络流量进行分段，从而防止敏感系统之间的横向移动，并确保根据实时风险评估不断更新权限。
- **增强监测能力和自动化：**该机构使用了 Akamai 的集成分析和自动化工具，以全面了解其安全态势，并实现跨所有支柱的策略执行自动化。

凭借此举措，该机构减少了攻击面、缩短了事件响应时间，并且实现了联邦安全法规的全面合规。此案例展示了跨支柱集成的重大作用，它可以将零散的安全架构转变为支持 Zero Trust 且具有凝聚力的动态安全模型。

# 结论

Zero Trust 安全防护已不再是可有可无。在保护联邦机构免遭复杂网络攻击的过程中，它已变得必不可少。通过实施微分段、API 安全防护和强大的身份控制，联邦机构和部门不但确保了遵守联邦网络安全法规，同时还大幅降低了风险。

Akamai 提供了一套全面的 Zero Trust 解决方案，包括 Akamai Guardicore Segmentation、Akamai API Security 和 Akamai Secure Internet Access Enterprise，使机构能够采取主动、自适应的安全防护措施。通过利用 Akamai 的专业知识，联邦机构可以加快其 Zero Trust 实施过程，并确保建立长期稳固的安全韧性。

现在，联邦机构是时候采取行动了。通过集成 Akamai 的安全解决方案，各大机构可以提升 Zero Trust 成熟度、抵御网络风险，并保护至关重要的国家数字资产。

立即联系 Akamai，详细了解我们全面的安全解决方案。

Akamai 安全部门致力于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：2025 年 4 月。

扫码关注，获取最新云计算、云安全与CDN前沿资讯