Akamai

WHITE PAPER

Achieving Zero Trust Maturity with Akamai

Supporting CISA's cross-cutting capabilities for federal agencies and departments

Introduction

Zero Trust security has become the gold standard for protecting sensitive government data, critical infrastructure, and national security systems. Federal agencies and departments can no longer rely on traditional perimeter-based security models to combat modern threats. As cybercriminals grow more sophisticated, using advanced tactics such as credential theft, ransomware, and insider attacks, federal organizations are increasingly shifting their security posture toward a Zero Trust framework. However, this shift has been fragmented and more needs to be done to secure federal systems.

The Cybersecurity and Infrastructure Security Agency's (CISA's) Zero Trust Maturity Model can help federal agencies and departments implement security principles that eliminate implicit trust and enforce strict verification mechanisms. The model is built on five foundational pillars: Identity, Devices, Networks, Applications and Workloads, and Data. In addition, three cross-cutting capabilities — Visibility and Analytics, Automation and Orchestration, and Governance — ensure a holistic and consistent approach to cybersecurity.

To meet these goals, microsegmentation should be considered a core tenet of Zero Trust security, serving as a fundamental component of internal (i.e., east-west) network defense. By segmenting workloads and restricting lateral movement, federal organizations can contain potential breaches and enforce Zero Trust policies. Additionally, comprehensive application programming interface (API) security solutions should be implemented to safeguard external (i.e., north-south) communications, ensuring only authorized entities access government applications.

This white paper explores the essential steps in achieving Zero Trust maturity, highlighting how Akamai's advanced security solutions, including Akamai Guardicore Segmentation, Akamai API Security, and Akamai Enterprise Application Access, empower federal agencies and departments to meet CISA's guidelines and enhance their cybersecurity posture.

The shift from perimeter-based security to Zero Trust

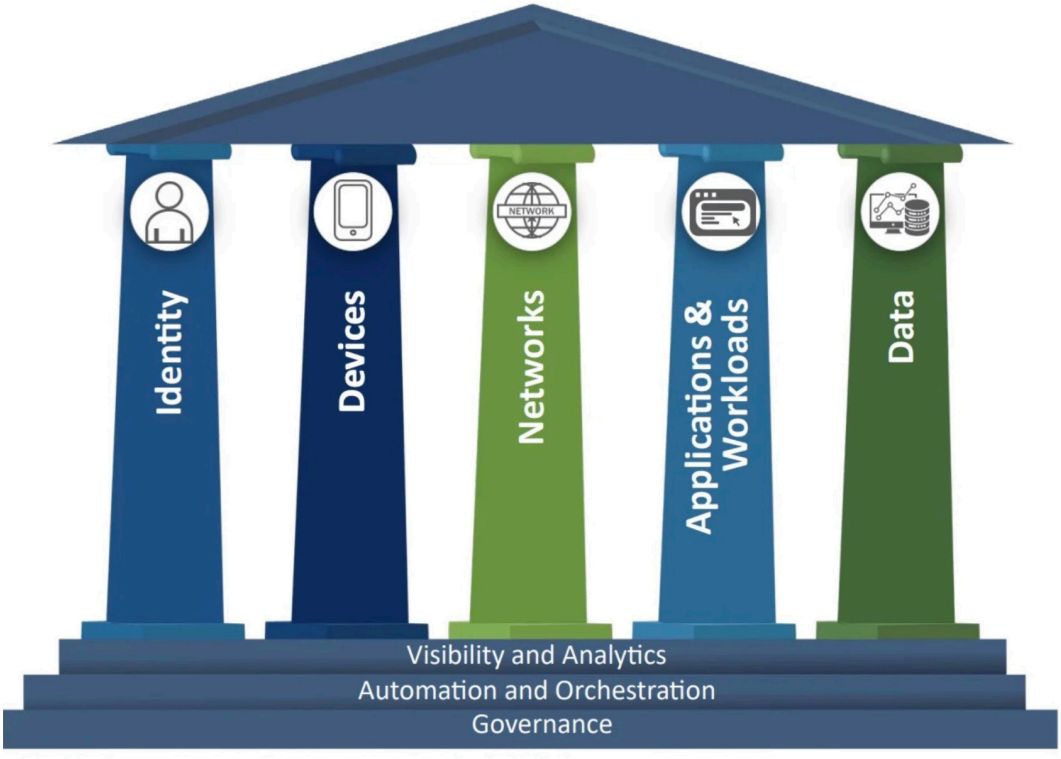
Traditional cybersecurity relied on perimeter-based defenses, assuming that once an entity was inside the network, it could be trusted. However, this model has repeatedly failed in the face of modern cyberthreats. Attackers exploit weak credentials and misconfigured security settings and use lateral movement techniques to bypass traditional defenses and gain access to sensitive information.

Zero Trust eliminates implicit trust by requiring continuous verification of users, devices, applications, and network traffic. Every access request is authenticated, authorized, and continuously monitored based on real-time risk assessments. This approach dramatically reduces the attack surface and prevents unauthorized access, even if an adversary breaches part of the network.

CISA's Zero Trust Maturity Model

CISA's Zero Trust Maturity Model provides a roadmap for federal agencies and departments to progressively strengthen their security framework (Figure). The model is built upon five key pillars:

- **Identity:** Enforcing strong authentication, authorization, and access controls to ensure only legitimate users can interact with sensitive resources
- **Devices:** Monitoring, securing, and validating endpoint devices to ensure they comply with security policies before accessing government networks
- **Networks:** Implementing microsegmentation and advanced access control policies to prevent unauthorized lateral movement
- **Applications and Workloads:** Protecting applications and workloads with strict identity-based access policies, runtime security, and API security controls
- **Data:** Ensuring that sensitive government data remains encrypted, monitored, and protected against unauthorized access and exfiltration



CISA's Zero Trust Maturity Model Pillars (Source: CISA)

In addition to these pillars, the model integrates three critical cross-cutting capabilities that apply across all Zero Trust components:

- **Visibility and Analytics:** Continuous monitoring, logging, and anomaly detection to identify and mitigate threats in real time
- **Automation and Orchestration:** AI-driven security automation to enforce policies, respond to threats, and streamline access control
- **Governance:** Centralized policy enforcement to maintain compliance with federal mandates, such as the Federal Information Security Modernization Act (FISMA) and the National Institute of Standards and Technology (NIST) Special Publication 800-207

The importance of microsegmentation and API security

In traditional network security models, networks are usually divided into broad segments using network-based firewalls. While this approach provides a certain level of security, it lacks the granularity required to fully protect modern, distributed environments. In federal environments, network-based segmentation typically results in overprovisioning; that is, users and applications have access to more resources than they really need. This creates unintended opportunities for lateral movement. As attackers compromise one part of the network, they can move across to more sensitive areas with little resistance.

The concept of microsegmentation addresses this challenge by introducing fine-grained control over east-west traffic within the network. In a microsegmented environment, each application, workload, or service is isolated from others, and access is restricted based on specific policies. This ensures that users, devices, and applications can only communicate with the resources they are explicitly authorized to access. By implementing identity-based, application-aware segmentation, microsegmentation limits the potential damage from cyberattacks, reduces the attack surface, and enforces the principle of Zero Trust.

When it comes to north-south network traffic, federal networks increasingly rely on APIs to facilitate communication among systems. As a result, protecting API endpoints becomes a top priority. API attacks — including injection attacks, credential stuffing, and unauthorized data access — have increased sharply in recent years. Federal agencies and departments need comprehensive API security solutions that provide full lifecycle protection for APIs, enabling security personnel to discover, monitor, and secure their API traffic in real time. API discovery is especially important — it is not uncommon to have APIs that no one knows about.

Akamai Zero Trust solutions at a glance

Identity

Akamai MFA is a keyless FIDO2 identity solution that protects employee accounts from phishing and other machine-in-the-middle attacks. It ensures that only strongly identity-based authenticated employees can access the accounts they own. Other access is denied, and employee account takeover is prevented.

Devices

Akamai Guardicore Segmentation is an industry-leading microsegmentation solution, designed to limit the east-west spread of ransomware and other malware. By continuously monitoring and enforcing policies on devices, Akamai Guardicore Segmentation can verify device configurations, software installations, and potential vulnerabilities, ensuring that only compliant devices can access the network. In addition, the solution supports an agentless approach to secure Internet of Things devices.

Akamai Enterprise Application Access is a comprehensive Zero Trust Network Access solution that ensures that only authenticated users and devices can access applications. By verifying the identity and posture of devices, Enterprise Application Access complements the capabilities of Akamai Guardicore Segmentation. If a device is found to be noncompliant or poses a security risk, Enterprise Application Access can restrict its access to sensitive applications.

Networks

Akamai API Security provides federal security professionals with comprehensive visibility into the entire API estate through continuous discovery and real-time analysis of north-south traffic. The solution detects unknown APIs, identifies vulnerabilities, and analyzes API behavior so security teams can detect attacks and remediate risk in this fast-growing attack surface.

Akamai App & API Protector brings together web application firewall, bot mitigation, API security, and Layer 7 distributed denial-of-service (DDoS) protection into a single solution. It quickly identifies vulnerabilities and mitigates threats across the entire network and API estates.

Akamai Secure Internet Access Enterprise is a cloud-based secure domain name service (DNS) that ensures that users and devices can securely connect to the internet wherever they happen to be — without the intricacy and management overheads associated with other security solutions.

Akamai Guardicore Segmentation provides granular control over network traffic, ensuring that only legitimate traffic is allowed.

Akamai Zero Trust solutions at a glance

Applications and Workloads

Akamai Enterprise Application Access provides Zero Trust access for employees, third-party contractors, partners, and mobile users — regardless of their location.

Akamai Guardicore Segmentation provides visibility into and understanding of applications and workloads.

Data

Akamai Secure Internet Access Enterprise provides secure access to data with features like content filtering, advanced threat protection, and data loss prevention. It supports data inventory management by preventing unauthorized access and data leaks.

Akamai Guardicore Segmentation: The key to east-west protection

Akamai Guardicore Segmentation is a leading microsegmentation solution designed to help organizations — especially federal agencies and departments — implement granular security controls across on-premises and cloud environments.

Granular segmentation of workloads and applications

Unlike traditional segmentation, which controls access at the network level, Akamai Guardicore Segmentation applies security policies at the application and workload level. This ensures that access is tightly restricted. For example, in a federal agency, a human resources (HR) application can be limited to communicating only with its designated HR database, preventing attackers from moving laterally if a breach occurs.

Identity-based microsegmentation

Akamai Guardicore Segmentation enforces segmentation based on user and device identity rather than just IP addresses. This ensures that access is granted dynamically based on role, trust level, and real-time verification. For instance, contractors and third-party partners can be restricted to only the systems they need, reducing unauthorized access risks.

Dynamic policy enforcement

Akamai Guardicore Segmentation continuously adjusts security policies based on real-time factors, such as user behavior, device health, and network activity. If suspicious activity is detected — such as an abnormal volume of data transfers — Akamai Guardicore Segmentation can automatically restrict access, block traffic, or alert security teams. This proactive approach ensures security policies evolve to counter emerging threats.

By integrating Akamai Guardicore Segmentation's microsegmentation, organizations can strengthen their Zero Trust architecture, minimize risk, and maintain strict access control over their networks.

CASE STUDY

Akamai Guardicore Segmentation in a federal environment

One federal agency recently implemented Akamai's microsegmentation solution to protect its internal systems from lateral movement attacks. Before adopting Akamai Guardicore Segmentation, the agency relied on traditional network-based segmentation, which provided limited granularity and allowed for broad access among different network segments. This created a significant risk of lateral movement if any part of the network were compromised.

With Akamai Guardicore Segmentation, the agency was able to:

- Implement granular segmentation: By segmenting workloads at the application level, the agency reduced the risk of lateral movement and ensured that each application could communicate only with the resources it needed.
- Improve visibility: The solution's visualization tools provided the agency with deep insight into its internal traffic, allowing security teams to identify and mitigate potential threats in real time.
- Enhance security: By integrating Akamai Guardicore Segmentation with its existing identity management and access control systems, the agency was able to enforce Zero Trust across the network, ensuring that access was continuously monitored and dynamically adjusted based on real-time risk assessments.

This example demonstrates the power of Akamai Guardicore Segmentation to improve network security, reduce the risk of lateral movement, and ensure that permissions are kept to the minimum necessary at all times.

API security: Protecting north-south traffic

Akamai offers several solutions to ensure API security. Akamai's API security platform ensures comprehensive visibility into API interactions and automatically detects and mitigates north-south threats in real time. With advanced behavioral analytics, federal agencies and departments can:

- **Identify shadow APIs** that could be exploited by attackers
- **Monitor API traffic patterns** to detect unauthorized access attempts
- **Implement API rate limiting** to prevent abuse and denial-of-service attacks
- **Identify forgotten, neglected, or unknown APIs** to uncover potential attack paths
- **Inventory all APIs** regardless of configuration or type, including RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, and gRPC

Akamai Secure Internet Access Enterprise is a cloud-based DNS firewall that is designed to help security teams ensure that all users and devices — both on-network and off — can securely connect to the internet. It proactively blocks malicious DNS requests including malware, ransomware, phishing, and low-throughput DNS data exfiltration. Secure Internet Access Enterprise reduces security complexity with no appliances to deploy, manage, and upgrade. The solution is simple and intuitive to use.

Akamai App & API Protector discovers and mitigates API threats for apps and APIs running through Akamai Cloud and can block any traffic that contains potential threats uncovered by Akamai API Security. When deployed together, Akamai's API protections offer comprehensive and continuous visibility into APIs, and allow security personnel to discover, audit, detect, and respond to API security concerns across the full application estate.

Enabling cross-cutting capabilities with Zero Trust

One of the main challenges with Zero Trust architectures is the risk of creating technology silos. Each silo often operates independently, leading to fragmented security controls, policy enforcements, and threat detection. Therefore, the importance of integration across all security layers is paramount.

For federal agencies and departments that manage highly sensitive data and complex infrastructures, this fragmented approach can introduce significant security risks. Attackers can exploit the lack of visibility between silos (or pillars) or capitalize on inconsistent policy enforcement across different systems. To mitigate these risks, federal organizations must adopt a unified, cross-pillar security model that integrates visibility, governance, and automation across all pillars, ensuring consistent policy enforcement and reducing gaps that adversaries can exploit.

To achieve a unified security model, cross-pillar integration must focus on the three cross-cutting areas of CISA's Zero Trust Maturity Model: Visibility and Analytics, Automation and Orchestration, and Governance. These elements are essential for enabling a Zero Trust architecture, in which access and permissions are dynamically adjusted across all pillars based on real-time risk assessments.

Visibility and Analytics

Visibility is critical for detecting threats, understanding user behavior, and enforcing dynamic security policies across all pillars. Without full visibility into how identities, devices, applications, and data interact, security teams are left in the dark, making it difficult to detect anomalous behavior or unauthorized access attempts. Akamai solutions provide comprehensive, cross-pillar visibility.

- Akamai Guardicore Segmentation monitors network traffic among segmented workloads, providing visibility into east-west traffic and detecting any attempts at lateral movement within the network.
- Enterprise Application Access provides insight into application access patterns, tracking how users interact with sensitive applications and ensuring that access is dynamically adjusted based on contextual data.

By integrating these capabilities, federal agencies can correlate data across all pillars, enabling a unified view of security events. When a user requests access to an application, Akamai's solutions can check not only the user's identity but also the security of the device, the network they are using, and the real-time behavior of the application. This allows security teams to detect potential threats faster, minimize the risk of privilege escalation, and ensure that permissions are dynamically adjusted in response to real-time risk assessments.

Automation and Orchestration

Responding to incidents and enforcing policies across multiple systems can be a slow, manual process. With Zero Trust, security policies need to be enforced dynamically across all pillars, which requires a high level of automation and orchestration. This ensures that as risk levels change, permissions are immediately adjusted to the minimum necessary level, reducing the chance of human error or delayed response. Akamai's solutions offer automated workflows that span identity, network, and application security.

- Akamai Guardicore Segmentation offers automated microsegmentation, dynamically adjusting network segmentation policies based on real-time traffic patterns and detected anomalies. This ensures that any suspicious activity within the network is quickly isolated, preventing lateral movement.
- Enterprise Application Access automates the process of securing application access, ensuring that users can only access applications through a secure proxy and that permissions are continuously updated based on changing risk factors.

By automating these processes, federal agencies and departments can ensure that security policies are enforced consistently and rapidly, reducing the window of opportunity for attackers.

Governance

Governance is the foundation of any security strategy, ensuring that policies are consistently enforced and compliance requirements are met. In a cross-pillar model, governance must ensure that all security controls are aligned with the principles of Zero Trust. With Akamai's solutions, agencies can implement governance policies that span all pillars.

- Identity governance: Ensuring that identity-based access controls are enforced consistently across devices, applications, and networks, and that access permissions are periodically reviewed and updated based on real-time risk assessments
- Network governance: Enforcing network segmentation and traffic monitoring policies across environments, including on-premises, cloud, and hybrid infrastructures; Akamai Guardicore Segmentation allows agencies to define network segmentation policies and ensure that they are applied consistently across the entire infrastructure
- Data governance: Protecting sensitive data by ensuring that access is restricted based on least privilege and that all data transfers are continuously monitored for unauthorized access or suspicious activity

Akamai's technologies are designed to work together seamlessly to provide federal agencies with a fully integrated, cross-pillar security architecture that supports Zero Trust.

CASE STUDY

Cross-pillar integration in a federal agency

A large federal agency faced significant challenges with fragmented security policies across its identity, network, and application layers. Different systems managed identity verification, application access, and network segmentation, leading to inconsistent enforcement of security policies and gaps in visibility.

By adopting Akamai's integrated solutions, the agency was able to:

- **Unify identity and application security:** Akamai's Identity, Credential, and Access Management (ICAM) solution, Enterprise Application Access was integrated to ensure that application access was always authenticated based on real-time identity data. This allowed the agency to dynamically adjust application permissions based on user behavior and device health.
- **Enforce dynamic network segmentation:** Akamai Guardicore Segmentation was deployed to segment network traffic based on identity and application access, preventing lateral movement among sensitive systems and ensuring that permissions were continuously updated based on real-time risk assessments.
- **Enhance visibility and automation:** The agency used Akamai's integrated analytics and automation tools to gain full visibility into its security posture and automate policy enforcement across all pillars.

As a result, the agency reduced its attack surface, improved incident response times, and achieved full compliance with federal security regulations. This case demonstrates the power of cross-pillar integration to transform a fragmented security architecture into a cohesive, dynamic security model that supports Zero Trust.

Conclusion

Zero Trust security is no longer optional. It is a necessity for protecting federal agencies from sophisticated cyberthreats. By implementing microsegmentation, API security, and strong identity controls, federal agencies and departments can drastically reduce risk while maintaining compliance with federal cybersecurity mandates.

Akamai provides a comprehensive suite of Zero Trust solutions, including Akamai Guardicore Segmentation, Akamai API Security, and Akamai Secure Internet Access Enterprise, enabling agencies to adopt a proactive, adaptive security posture. By engaging Akamai's expertise, federal organizations can accelerate their Zero Trust journey and ensure their long-term security resilience.

Now is the time for federal agencies to act. By integrating Akamai's security solutions, agencies can achieve Zero Trust maturity, mitigate cyber risks, and safeguard the nation's most critical digital assets.

Contact Akamai today to learn more about our comprehensive security solutions.