AKAMAI FOR THE PUBLIC SECTOR

Zero Trust Strategies for Government Agencies and Organizations

Implementing your zero trust strategy

Government agencies today face unprecedented security challenges as exemplified by the SolarWinds and Colonial Pipeline attacks. In response, Presidential Executive Order 14028 and Memorandum M-22-09 have laid out directives to implement a Zero Trust strategy.

Meeting these strategic directives should be viewed as a journey, not a destination. With 20 years' proven experience in public sector security, Akamai is here to help you get started on your Zero Trust journey. `

Akamai's zero trust advantage

The Zero Trust goals presented in the presidential order and memorandum align with the Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust Maturity Model, which has five pillars:

- Identity
- Devices
- Networks
- Applications & Workloads
- Data

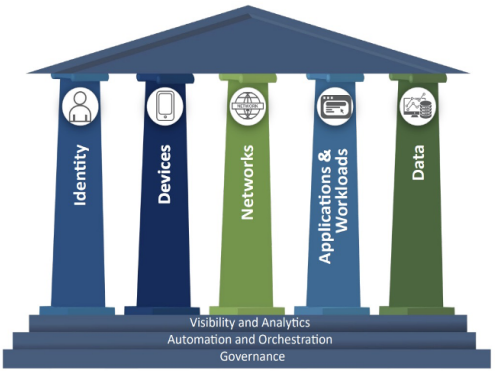
As your trusted government security advisor, Akamai offers the products, people, and partners to help you achieve your Zero Trust goals.

Benefits:

- Secure your users
- Secure your network
- Secure your access

"Once we implemented Akamai Guardicore Segmentation, we could identify traffic patterns that were not only unnecessary but also were previously unknown."

Edwin Blom
Chief Information Security Officer
FCC Group



Zero Trust Security Model Pillars

Source: "Zero Trust Maturity Model" by the Cybersecurity and Infrastructure Security Agency, Cybersecurity Division, April 2023

Identity

Akamai Multi-Factor Authentication (MFA) is our 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 our industry-leading microsegmentation solution, designed to limit the spread of ransomware and other malware. By continuously monitoring and enforcing policies on devices, it 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 IoT devices.

Akamai Enterprise Application Access (EAA) is our Zero Trust Network Access (ZTNA) solution, ensuring that only authenticated users and devices can access applications. By verifying the identity and posture of devices, EAA complements the capabilities of Guardicore. If a device is found to be non-compliant or poses a security risk, EAA can restrict its access to sensitive applications.

Networks

Akamai App & API Protector brings together web application firewall, bot mitigation, API security, and Layer 7 DDoS protection into a single solution. It quickly identifies vulnerabilities and mitigates threats across your entire web and API estates.

Akamai Secure Internet Access Enterprise is our cloud-based secure DNS service that ensures your 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. By segmenting the network at a micro level, it ensures that potential threats are isolated and cannot move laterally within the network.

Applications & Workloads

Akamai EAA provides Zero Trust access for your employees, third-party contractors, partners, and mobile users — regardless of their location. EAA eliminates the operational cost and risk involved in maintaining and patching VPNs or other appliance-based solutions.

Akamai Guardicore Segmentation provides visibility and understanding into workloads, applications and processes, as well as the enforcement of secure access policies. Together, Guardicore and EAA provide a comprehensive solution for application and workload security

Data

Akamai Secure Internet Access 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.

Proven partners

In addition, you can trust our proven partner relationships to help you meet your Zero Trust directives. Our public sector security team can help you find the right partners and customized solutions to protect your environment.

You can rely on Akamai

Akamai's people, products and partners will help you meet your Zero Trust directives. We will assist you to build and customize uncompromised, end-to-end security for your agency or organization. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences — helping billions of people live, work, and play every day.

To learn more, visit Getting Started with Your Zero Trust Strategy or contact your Akamai public sector security sales team.