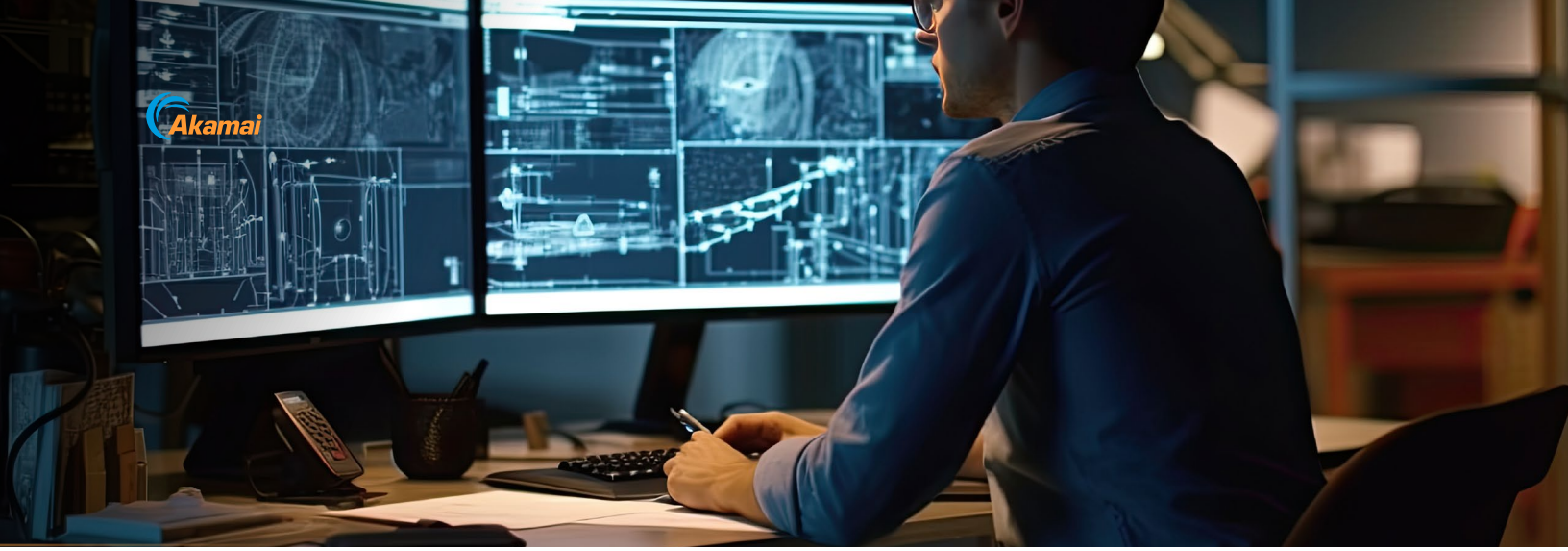
Akamai

WHITE PAPER

Delivering Seamless, Secure Services Across Agency Environments

Advance Zero Trust Architectures and Secure Digital Experiences



The Crucial Role of User Experience

In an era of rapid digitization and an ever-expanding digital landscape, government agencies face the dual challenge of streamlining and improving the efficiency of their digital services while also building out Zero Trust architectures. Yet these simultaneous goals often compete.

The scope and frequency of cyberattacks on agency networks have escalated dramatically. Threat actors have become increasingly sophisticated, employing a range of techniques to compromise critical infrastructure, harvest personally identifiable information (PII), and disrupt essential services. From the high-profile SolarWinds breach in 2020 to recent malware attacks on critical infrastructures like water and power allegedly sponsored by state actors, the threats are relentless and continue to evolve.

As agencies strengthen security postures, modern tools and processes can help streamline the management of complex multi-cloud environments while ensuring 24/7 availability and resiliency of critical resources and services. By focusing on automation, agencies can maximize their efficiency, freeing up IT departments to concentrate on vital tasks. This reinforces the commitment to maintaining secure and streamlined digital environments.

To augment security efforts, compliance mandates continue to expand and become more stringent. Requirements and funding for security and governance are growing across federal and state and local agencies, underlined by Executive Order 14028 and evolving Zero Trust guidelines including the CISA Zero Trust Maturity Model. Notably, the State and Local Government Cybersecurity Act is an example of the increased pressure on and associated funding for agencies of all sizes to enhance cybersecurity measures.

Enhancing CISA Zero Trust Maturity Model scores means that agencies require improved visibility into their systems. This entails greater automation and integration of both processes and symptoms to effectively enforce decisions across identity, networks, applications, and data. The principles of rigorous, continual, intelligent denial of trust, and seamless, secure authentication offer a new way to isolate and protect sensitive workloads and data while maintaining 24/7 availability.

Implementing Zero Trust architectures is a powerful step toward robust security. By finding the right balance between security and the use of trusted, open platforms that work together, agencies can create a more secure network.

This process encourages a complete approach, bringing together people, tools, and technologies to shield the digital ecosystem. It aligns with up-to-date rules and guidelines, such as those provided by the Office of Management and Budget (OMB) and the Cybersecurity and Infrastructure Security Agency (CISA), and meets the needs of the State and Local Government Cybersecurity Act.

Protect and Defend Agency Assets

The following steps can be taken by agencies to safeguard their assets:

1. Provide Access that Supports Zero Trust Architectures

Akamai is at the forefront of the transition to Zero Trust architecture, offering comprehensive solutions that empower agencies to assertively defend their assets.

Zero Trust architecture implementation includes securing user identity, device management, network monitoring, application security, and data control across hybrid systems. A cornerstone of this architecture is the establishment of strict, least-privilege access controls. Akamai's solutions are designed to manage these controls effectively, facilitating secure, productive workflows.

Agencies continue to make great strides toward implementing stronger identity authentication, including automating management and analysis of user access policies. Using CISA's Zero Trust Maturity Model as a guide, the end goal is to enable continuous, phishing-resistant multi-factor authentication (MFA) validation of identities for "just in time" and "just enough" access. That least-privilege access needs to be supported by fully automated and integrated identity stores, activity logs, continuous analysis, and dynamic rules that simplify the orchestration of all identities across the agency environment.

Adopting a Zero Trust automated approach is critical to keep pace with evolving environments as agencies work toward more mature application protections. Following CISA's guidance, teams must account for automating application access decisions and supporting those decisions with real-time risk analytics and integrated threat protection. This enables continuous, dynamic monitoring of all applications for enterprise-wide visibility, allowing proactive gap mitigation and enhancing the governance and security of application CD/CD pipelines.

Akamai's Enterprise Application Access capabilities advance Zero Trust policies by providing a unified service that grants access to only the necessary applications for remote employees, contractors, and partners. Using adaptive identity- and context-aware access controls, EAA improves visibility and decision-making. Offering rapid deployment, it integrates access management, application security, and Single Sign-On (SSO) in one easy-to-use portal, reducing the risks of over-privileged permissions.

Best practices to defend agency assets

- Use zero-day protection such as advanced threat intelligence, proactive monitoring, and behavior-based detection techniques
- Gain a comprehensive understanding of whole IT infrastructure to understand app dependencies and flows, including network assets, processes, users, and traffic flows
- Layer secure, precise access controls with fine-tuned microsegmentation
- Enforce compliance quickly and uniformly with automated policy enforcement and global logging coverage
- Safeguard productivity with Akamai's 100% service-level agreement (SLA)

Protect and defend	Unify visibility and control	Simplify and scale performance	Improve experiences
• Provide secure access to only the applications that users need from any location, bypassing the need for network access • Adaptive access controls use real-time intelligence to automatically protect applications	• Unify management of integrated access controls (data path protection, access management, application security, MFA, and SSO) across applications and locations • Improve visibility and understanding of users, unify auditing, and reporting	• Centrally managed, cloud-delivered service with easy deployment of secure access across distributed users, applications, and locations	• Intelligent access controls that don't block collaboration; web-based SSO for a seamless experience from anywhere • Deploy MFA on smartphones with user-friendly push notifications • Self-service user enrollment

2. Protect Agency Assets

The proliferation of applications and APIs is continuously evolving, making them difficult to secure. As such, they are often leveraged as an attack vector by malicious actors. This is where Akamai's App and API Protection capabilities come into play.

Akamai strengthens an agency's security posture by deploying a holistic web application and API protection solution. This solution adaptively updates protections based on real-time threat intelligence and proactively delivers insights on targeted vulnerabilities. This includes bot visibility and mitigation, DDoS protection, SIEM connectors, web optimization, API acceleration, and more.

By offering self-tuning recommendations, Akamai alleviates the burden of time-intensive manual maintenance, ensuring that agencies can proactively manage their security posture. The result is unified visibility, enabling deep insights for determining traffic patterns and analyzing attacks using customized dashboards.

Protect and defend	Unify visibility and control	Simplify and scale performance
• Adaptive security engine that integrates threat intelligence across Akamai's platform to detect up to 2X more attacks • Extend Zero Trust policies to the edge with automatic discovery and protection of all APIs	• One centrally managed solution with integrated capabilities for holistic protection of all websites, applications, and APIs • Continuous visibility and insights to identify and stop the most sophisticated attacks at the edge with automatic updates from global threat intelligence	• Automatic updates and self-tuning for 5X reduction in false positives, freeing teams to focus on real attacks • Automated onboarding streamlines management

3. Strengthen Zero Trust Implementations with Microsegmentation

Microsegmentation plays a vital role in deploying Zero Trust architectures across complex distributed environments. Agencies continue to move from perimeter-based and macrosegmentation implementations to deploying software-defined microsegmentation capabilities that better protect dynamic, hybrid environments. CISA highlights tactics to improve visibility into communications and situational awareness across the agency enterprise as part of this movement. Building out fully distributed ingress/egress micro-perimeters and microsegmentation based on application profiles and automating the management of dynamic environments enables security policies to evolve with mission needs. Akamai offers robust capabilities for implementing microsegmentation, aiding in reducing the attack surface, meeting compliance requirements, and isolating sensitive data.

Akamai's software-defined segmentation solution allows for precise control and policy enforcement over communication between applications across agency networks. By offering real-time detection and a comprehensive visual map of app dependencies, traffic flows, and policy recommendations, Akamai ensures a streamlined initial deployment. This enables agencies to continually monitor policies, automatically quarantine suspicious entities, and establish a more proactive approach to network security.

Protect and defend	Unify visibility and control	Simplify and scale performance
• Precise software-defined segmentation across clouds • Detect and quarantine breaches quickly to prevent lateral movement of attackers	• Map the entire infrastructure to visualize activity, spot gaps, and dependencies to inform segmentation policies, verify policies are working, and provide evidence of compliance	• More intuitive deployment with automated labeling to implement faster; change policies without impacting networks, applications, or downtime

Akamai Microsegmentation Use Cases

- **Zero Trust segmentation:** Map deep dependencies and enforce policies with least-privilege design and user authorization
- **Threat detection, hunting, and response:** Real-time capabilities that use multiple detection methods made for the cloud with integrated response and detailed forensics
- **IoT Security:** Reduce attack surface and enforce Zero Trust policies on devices that can't run host-based security software
- **Critical application ringfencing:** Visualize applications in detail to understand how they work and communicate and support isolation strategies
- **Third-party access control:** View applications by function and control third-party user access
- **Discovery and network analysis:** Inventory access, discover internet-accessible applications and analyze network traffic using metadata
- **Container security:** Empower DevOps to gain critical capabilities without sacrificing agency security

4. Modernize Agency Networks with Secure Access

Secure remote connections have become a necessity in the modernization of agency networks. With Akamai's Secure Internet Access (SIA) capabilities, agencies will ensure users and devices can securely connect to the internet from any location.

Federal and state and local government agencies can thus support productivity, collaboration, and service delivery while maintaining robust security measures. Users located in field offices or remote sites and those who are mobile can experience secure and efficient internet access.

SIA uses global threat intelligence from Akamai to proactively identify, block, and mitigate targeted threats, such as malware, ransomware, phishing, DNS data exfiltration, and other zero-day attacks. It empowers agencies to enforce geolocation-based restrictions and content-specific computing for an enhanced level of security, ensuring that data is protected no matter where remote access was established.

Akamai, therefore, plays an integral role in fortifying and modernizing agency networks, ensuring a seamless and secure transition to the digital future.

Protect and defend	Unify visibility and control	Simplify and scale performance
• Ensure user and device-secure internet connections • Real-time global threat intelligence powers multiple layers of protection to block targeted threats proactively, such as malware, ransomware, phishing, and DNS exfiltration	• Centrally create, deploy, and enforce both unified security policies and acceptable use policies (AUP) in minutes for all users	• Cloud-based solution is quick to configure, deploy, and scale without worrying about hardware or disruption to users • Manage security from anywhere and push changes out globally in minutes to ensure all locations are protected

The Akamai Advantage: A Comprehensive Approach

Navigating the complexities of the digital world and the cybersecurity landscape requires a comprehensive, forward-thinking approach. This is the Akamai advantage: a unique blend of power, protection, and modernization that helps agency missions evolve and thrive in an interconnected environment. This solution lies in the strategic amalgamation of innovation, holistic security, and relentless commitment to service, tailored specifically to empower government agencies.

Unrivaled Infrastructure and Global Presence

- 6 billion hits per minute
- 100 million attacks defended at the edge daily
- 330,000+ servers
- Billions of daily transactions
- 4,200+ locations
- 1,900+ experts
- 1,400+ networks
- 135+ countries

Real-time Insights and Proactive Security Measures

Akamai solutions enable agencies to anticipate potential threats and mitigate them before they escalate into serious security concerns. Our suite of layered tools allows for proactive identification and attack blocking while maintaining compliance with regulatory mandates.

Leveraging these capabilities, defense teams can safeguard applications and data as they move across the digital landscape, remaining secure and accessible in any environment. With centrally managed platforms, continuous visibility, and automatic updates from global threat intelligence, Akamai solutions encourage a holistic approach to cybersecurity — bringing together people, tools, and technologies to shield the digital ecosystem.

As a trusted government partner, we are committed to empowering agencies to better serve their constituents through reliable, robust, and modern digital services.

Contact Akamai to modernize your mission with layered solutions that protect critical assets.

Scan the code above or visit akamai.com/publicsector to learn more.

Akamai

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's Connected Cloud platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 10/23.