Akamai TD SYNNEX Public Sector DLT

WHITE PAPER

Transformation Activated: Modernizing Today’s Government Agency

Simplify the Complexity of Hybrid and Multi-cloud Architectures

Accelerating IT Modernization

As government agencies continue to accelerate their IT modernization, there is an increasing need for a smart approach to transforming systems to manage and secure virtual boundaries across agencies, programs, and environments. Ensuring that this expedited shift from on-premises data centers to hybrid environments and multi-cloud architectures has a positive impact on the agency and users requires balancing performance, scalability, and security of workflows.

Modernization efforts help federal civilian agencies and state and local governments reduce the complexity of managing siloed hybrid multi-cloud environments. This allows them to secure and aid productivity across hybrid workforces by easing access and automating routine tasks — freeing workers to focus on higher-level tasks. Additionally, accelerated IT modernization ensures that sensitive data is protected through measures including multi-factor authentication (MFA) and network segmentation.

Reliability and availability help secure access to critical information during unexpected events or emergencies. These factors also increase the resilience and scalability of services and websites. In addition, acceleration enables data-driven decision-making based on accurate insights shared across the department or agency. Lastly, it provides better service for users through improved access to digital services such as online portals, mobile apps, and chatbots.

As agencies modernize their complex IT systems, security challenges arise, ranging from the potential complexity of Zero Trust implementation to securing remote and hybrid workforces. Legacy systems also result in limited visibility, lack of interoperability, and inability to scale for agencies.

To stay ahead of threats while maintaining performance, scalability, and availability, agencies need holistic, layered security.

Akamai’s Smarter Approach

- Layered, holistic security
- Infinitely scalable
- Complete North-South-East-West protections
- Cloud-agnostic
- 100% availability
- Performance and resilience assured

Implementing Modern Security Solutions

What is the foundation of modern security? Secure access.

As remote work becomes more prevalent, ensuring secure access to IT systems and applications while maintaining ease of use and manageability is crucial. Key requirements include robust authentication and access controls, monitoring and managing remote access, and implementing Zero Trust principles. Yet, as agencies move forward with these initiatives, they need to consider a variety of challenges.

Challenges of Legacy IT Systems

Many government agencies and organizations grapple with siloed legacy IT systems that are difficult to integrate with modern cloud-based systems. This complexity can hinder data and application migration to the cloud, leading to increased costs and maintenance.

Additionally, legacy systems create challenges related to visibility. Siloed systems generate numerous blind spots and vulnerabilities. These obstruct the identification of potential security risks and vulnerabilities, which can result in data breaches and other incidents.

Inadequacy of Traditional Security

Conventional security tools and manual processes are ill-equipped to counter fast-moving cyberattacks. Automation, real-time threat detection and response, and threat intelligence are essential components of an effective, proactive security stance.

Growing Attack Surfaces

The more a system expands and the more features it has, the larger target it offers. To address the expanding attack surfaces and evolving threats in modern systems, government agencies need a proactive security approach that includes continuous monitoring and threat intelligence.

Increasing Attack Sophistication

Lateral movement is a common tactic employed in ransomware attacks. Halting lateral movement requires a multi-layered defense approach. This approach can include the segmentation and isolation of critical systems and data.

Government agencies must also be prepared to combat advanced attack techniques, tactics, and procedures (TTP) employed by increasingly sophisticated adversaries. By adopting modern security measures and staying informed about the latest threats, agencies can better protect their IT systems, applications, and sensitive data against potential breaches and security incidents.

The Solution

A smarter approach to modernizing security means addressing the new demands of dynamic environments with distributed boundaries. This involves securing environments without impacting the performance or availability of government services. Agencies can secure their digital transformations by layering security solutions for more comprehensive visibility and control, working to maximize network security and productivity.

It starts with unified visibility to understand the current environment's behavior, enhancing awareness and facilitating proactive action. Secondly, continuous monitoring keeps an eye on network and user activities, identifying any unusual patterns or threats early. Implementing software-defined segmentation to complex environments and detecting and blocking attackers from moving across the network is yet another layer. And agencies should advance Zero Trust by ensuring only authorized users and devices can access the apps they need instead of the entire network with Enhanced Adaptive Access (EAA) controls.

Keys to Holistic Security

- Full visual map of infrastructure
- Software-defined segmentation
- Adaptive access controls
- Continuous monitoring

Visualizing Vulnerabilities: A Key to Improving Government IT Infrastructure

A single visual map of all assets and infrastructure — including legacy and modern operating systems, operational technology, and Internet of Things (IoT) devices with user and process-level granularity on a real-time or historical basis — is essential for government agencies to modernize their IT infrastructure effectively. This unified visibility allows agencies to:

- Understand network behaviors in real time
- Eliminate discrepancies and gaps
- Control the expanding attack surface

Benefits of Segmentation

- Consistent umbrella security protection of all assets
- Identity-aware access controls
- Precise segmentation and workload isolation
- Visual map of apps communication to understand gaps
- Proven, intelligent platform for modern, automated security
- Easier management and scaling as requirements and demand changes

Unified visibility enables agencies to optimize their IT and cloud infrastructure, identify areas of inefficiency, and make necessary adjustments. The outcome? Better resource utilization, reduced costs, and improved system performance.

Furthermore, leveraging automation and machine learning (ML) to troubleshoot issues can enhance overall system performance and reduce downtime, allowing for a better user experience and reliable productivity.

Access to full network maps allows agencies to acquire insights into how networks behave quickly, enabling them to see how applications connect. This information helps them quickly spot gaps in security policies and vulnerabilities before moving to the cloud or extending clouds.

Simplifying cloud management is another crucial aspect of modernizing IT infrastructure to improve security, compliance, detection, and response. By monitoring all systems through one view — possible with Akamai's global, cloud-agnostic platform — instead of managing multiple systems through separate consoles that require data normalization, agencies can achieve easier management and better efficiency, accuracy, and staff morale.

Improved compliance, auditing, and reporting are possible through simplified environment and security management. As a result, agencies can devote less time and expense to audit preparation, lowering the risk of penalties and eliminating audit fatigue.

Continuous monitoring of network segments and users helps detect issues in real-time, proactively respond to threats at scale, and optimize continuously. Given the massive and growing number of threats, unified visibility exposes the most critical ones, reducing the chance of threats becoming full-blown breaches.

Software-defined Segmentation Enables Smart Modernization

Smart modernization combines advanced technologies with business goals to enhance security, improve operational efficiency, and reduce costs. Technologies that constitute smart modernization — such as artificial intelligence (AI), ML, IoT, and cloud computing — have the potential to introduce risk. Segmentation addresses this by putting up barriers that prevent attackers from moving laterally in case of a successful breach.

To execute a smart approach to modernization with software-defined segmentation, agencies can:

- **Use microsegmentation** to acquire granular control over security policies and network behaviors, resulting in more flexible and scalable network architectures. These are decoupled from physical infrastructure and built for modern, dynamic environments.
- **Implement Zero Trust security** with Enterprise Application Access, which focuses on controlling access using MFA and role-based access controls while eliminating network access. This means users get the resources they need and nothing else.
- **Use cloud-native security** whenever possible, as it is specifically designed for cloud environments and provides better protection. Examples include cloud access security brokers (CASBs), next-generation firewalls (NGFWs), and automated security scanning.
- Deploy tools that use **machine learning** to identify anomalies and potential threats, establishing intelligent and dynamic security policies that can adapt to changing conditions.

Adaptive Access Controls for Dynamic Workloads

Adaptive access controls in Enterprise Application Access provide secure access for modern environments, ensuring the right people have secure access to the right applications at the right time versus the entire network. Adaptive access controls support smart modernization by:

- Enforcing granular access controls based on roles, user behavior, device posture, and context, minimizing the potential and impact of unauthorized access
- Automating provisioning to reduce the burden on IT staff and apply access controls consistently across the environment
- Providing continuous monitoring of access requests, user behavior, and device activity, resulting in the ability to adjust and apply controls as needed and gather insights into potential threats
- Integrating adaptive access controls to manage access across all environments (cloud, multi-cloud, hybrid, on-premises), reducing security risk
- Improving the user experience through one centrally managed portal, delivering seamless access that adapts to user needs and behaviors, ultimately enhancing operational efficiency

The Akamai Difference

Akamai provides intelligent, layered solutions that modernize and segment agency environments, enabling government agencies to benefit from a secure and efficient digital transformation. With Akamai, your agency can leverage:

1. **Massive scalability** and 100% availability service level agreements (SLAs), ensuring that critical services are always available to constituents, promoting trust and reliability
2. **Secure digital transformation** with North-South-East-West holistic protections, creating comprehensive security measures that safeguard your agency's digital infrastructure from all angles
3. **Holistic microsegmentation** that benefits from granular, intelligent segmentation with infinite tagging that isolates workloads, no matter where they reside, and is paired with continuous monitoring, automated detection, and incident response to block threats
4. **Fast, real-time visualization** of network activity that empowers IT teams to quickly identify and respond to security threats, reducing the time it takes to detect and mitigate cyberattacks
5. **Scalable, fast, secure access** for the right users and applications to the right data and assets to efficiently control access to a large number of users, devices, and applications while ensuring the security and confidentiality of sensitive data
6. **Enforce laser-focused Zero Trust** principles within your distributed technology environments to secure access to sensitive data and assets across systems and networks, decouple policy enforcement from underlying infrastructure, and provide greater flexibility and control for IT teams

Lead the way in the ever-evolving world of agency digital transformation. Learn more about how Akamai helps federal civilian and state and local government agencies accelerate modernization while ensuring security and efficiency. Contact us today to discover the Akamai difference and let our experts guide you through a seamless and secure modernization process.

Your Proven Platform and Partner

- 100% visibility and control across agency environments
- Providing the right users with precise access to the right apps, content, and data
- Simplified environment and security management
- Keeping pace with the speed of digital transformation

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

Akamai TD SYNNEX Public Sector | DLT