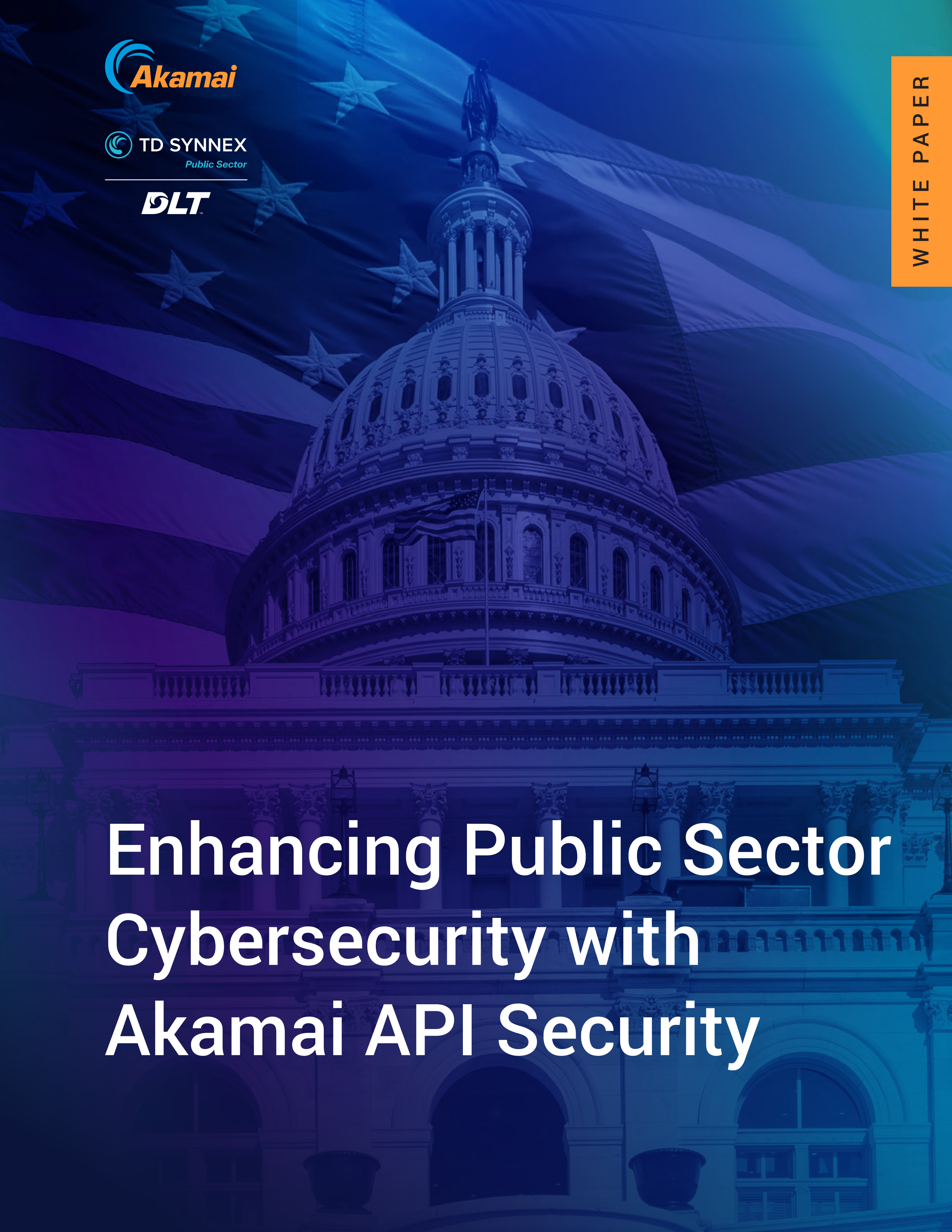


Akamai

TD SYNNEX
Public Sector

DLT

WHITE PAPER

Enhancing Public Sector Cybersecurity with Akamai API Security

Application programming interfaces (APIs) are the backbone of digital transformation in the public sector, enabling seamless service delivery, data sharing, and improved citizen experiences. However, this growing reliance on APIs also expands the attack surface, making API security a critical priority for government agencies.

Akamai's API security solution, integrated within its broader web and application security solutions, helps federal agencies identify, protect, and monitor API traffic in real time. With built-in threat intelligence, automated runtime anomaly detection, and integration with Identity, Credential, and Access Management (ICAM) frameworks, Akamai ensures that APIs remain secure while maintaining high performance and scalability.

Securing the expanded attack surface in a distributed environment

Federal agencies increasingly operate within multi-cloud and hybrid environments, combining private cloud (on-premises) and public cloud infrastructures. While this enhances connectivity and efficiency, it also introduces new security challenges, including:

- **An increased attack surface** — APIs are exposed across cloud environments, data centers, and edge nodes, making them potential entry points for adversaries. Furthermore, these APIs are often the preferred cyberattack vector as they often have direct access to back-end databases that contain sensitive data.
- **Distributed denial-of-service (DDoS) and automated attacks** — Hackers exploit API vulnerabilities to launch large-scale DDoS attacks, credential stuffing, and injection attacks.
- **Visibility challenges** — Many agencies struggle to track shadow APIs (those developed as rapid solutions outside of the standard approval processes) and zombie APIs (outdated interfaces that remain active because of incomplete decommissioning and staff turnover) that increase risks.

Akamai's API security capabilities address these challenges with:

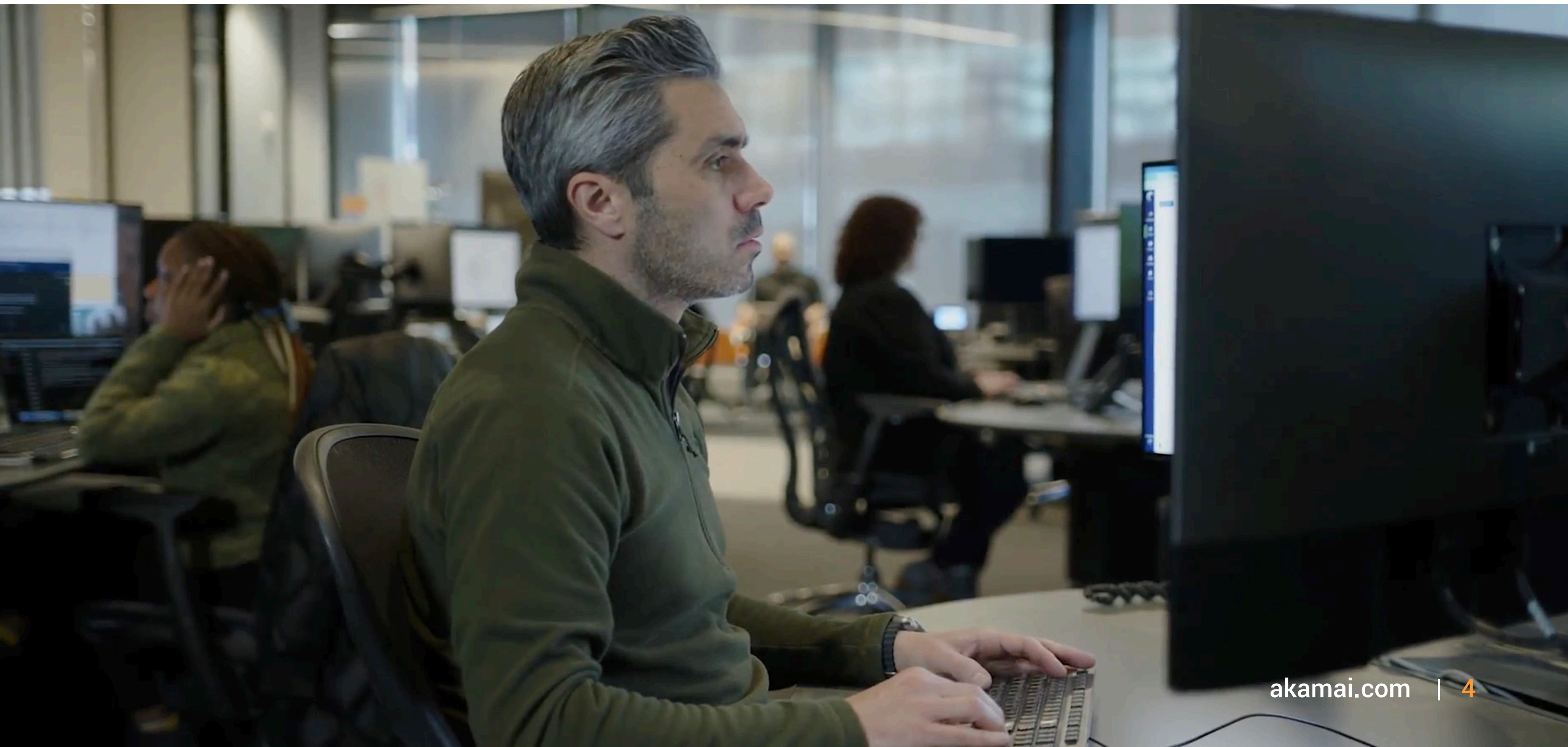
- **Real-time API discovery** — Identifies and comprehensively maps APIs, including shadow APIs, ensuring complete visibility across your entire digital ecosystem
- **Machine learning (ML)** – powered threat detection — Analyzes API traffic patterns to detect anomalies and block sophisticated attacks proactively, often before they can impact operations
- **Scalable API protection** — Secures API endpoints against injection attacks, credential abuse, and DDoS threats without impacting performance, even during peak traffic periods

Strengthening identity and access controls with ICAM integration

ICAM is a **cornerstone of federal cybersecurity authentication strategy**, ensuring that only authorized users and systems can access sensitive APIs. Akamai integrates with existing **Department of Defense–compliant ICAM solutions** to enforce Zero Trust principles through:

- **Granular role-based access control (RBAC)** — Define and enforce precise permissions to access API environments based on user roles, responsibilities, and security clearance levels. The use of ICAM ensures that only users with proper authentication and authorization have access.
- **Behavior-based anomaly detection** — Monitor API interactions continuously to detect suspicious activity that might indicate compromised credentials or insider threats.
- **Regulatory compliance alignment** — Help agencies meet federal Zero Trust mandates such as OMB M-22-09 and NIST SP 800-207, simplifying compliance reporting.

By combining API security with ICAM, agencies **mitigate insider threats, enforce least-privilege access, and prevent unauthorized access to APIs** while maintaining operational efficiency.



A unified approach to API security and application performance

Akamai's **comprehensive security and performance solutions** ensure that federal agencies can securely accelerate digital services without trade-offs. This includes:

- **Advanced threat protection** — ML-driven insights block sophisticated API attacks while providing security teams with actionable intelligence to improve defenses continuously.
- **Application acceleration** — Edge caching and optimization improve response times and reliability, ensuring citizen services remain responsive even during high-demand periods.
- **DDoS mitigation at scale** — This feature absorbs and neutralizes large-scale attacks to maintain availability by using Akamai's massive, distributed platform to protect critical infrastructure.
- **API lifecycle management** — Agencies can implement secure API development practices from design through deployment and ongoing monitoring. Our Active Testing module allows seamless integration into the software development lifecycle, which provides automation of API security testing for application development.

Enterprise Threat Monitor
Distributed Denial of Service (DDoS) Monitor - Past 7 Days

Real-world federal applications

Federal agencies use Akamai to:

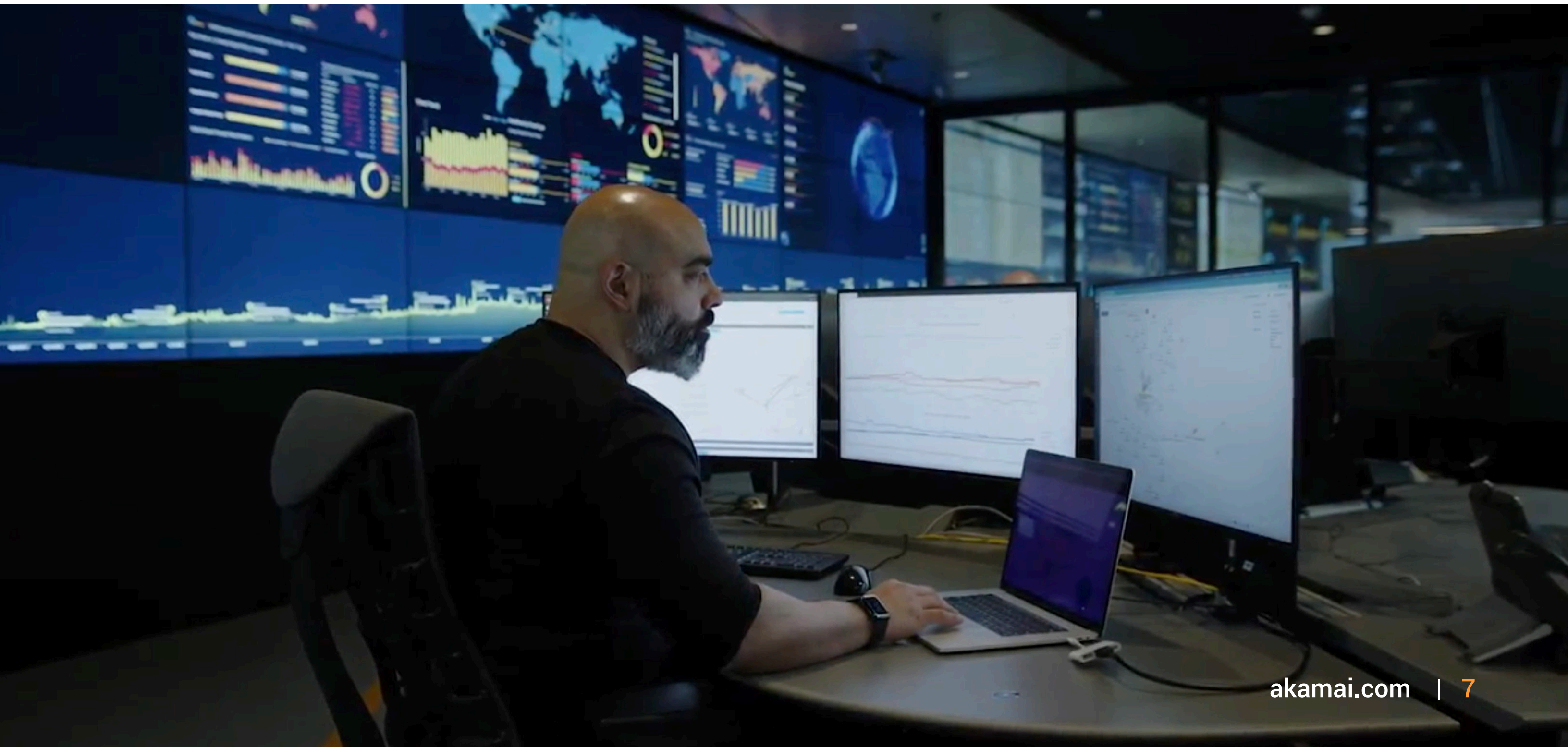
- **Protect critical citizen services** — Secure the APIs that power healthcare, benefits, and tax systems to help ensure that citizens can access essential services without interruption.
- **Safeguard mission-critical defense and intelligence systems** — Protect sensitive military and intelligence APIs from cyberthreats while enabling secure data exchange across classified and unclassified environments.
- **Enable smart government initiatives** — Securely connect Internet of Things (IoT) devices and sensors that power smart city infrastructure and environmental monitoring systems.
- **Enhance inter-agency and cross-agency collaboration** — Ensure secure data exchange across government applications by breaking down silos while maintaining strict security controls.

Akamai has successfully **secured national defense networks** by mitigating API attack surfaces and preventing data breaches across **thousands of endpoints** while supporting the mission needs of defense agencies worldwide.

The Akamai advantage for federal agencies

What sets Akamai apart for government API security needs?

- **Unmatched scale** — Akamai's platform processes trillions of internet interactions daily, providing unprecedented visibility into emerging threats.
- **FedRAMP compliance** — Our solutions are designed to meet rigorous federal security standards and simplify procurement processes.
- **Proven government experience** — Akamai's decades of experience in supporting federal agencies allows us to understand the unique security challenges that face government IT teams.
- **Zero Trust architecture** — Our solutions align perfectly with federal Zero Trust mandates and help agencies meet compliance requirements while enhancing security.



Secure your agency’s digital future today

API security isn’t just about protecting endpoints — it’s about securing your agency’s digital transformation. As federal agencies increasingly rely on APIs to deliver services, share data, and improve citizen experiences, securing these critical connections becomes paramount.

Akamai provides the comprehensive protection modern government agencies need by combining advanced threat intelligence, continuous monitoring, and seamless integration with existing security frameworks.

Take action now

Don’t wait for a breach to prioritize API security. Contact Akamai’s public sector team today to:

- Schedule a personalized assessment of your agency’s API security posture.
- See a live demonstration of our API security capabilities in action.
- Discuss implementation strategies tailored to your specific security requirements.

Contact us to begin enhancing your agency’s API security posture today.

Learn more

Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision. Learn more about Akamai’s cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X and LinkedIn. Published 05/25.