Akamai

WHITE PAPER

Enabling Secure, Mission-Critical Operations at the Edge

Deliver scalable and secure experiences anywhere in the global theater

Advancing the Future of Warfare: Decision Superiority

With the changing nature of global, dynamic multi-domain warfare operations, the Department of Defense (DoD) continues to modernize to maintain an adversarial edge. Decision superiority — the ability to make more informed decisions quicker than the adversary — is crucial to achieving this. This capability is enabled by secure and frictionless warfighter and partner experiences, delivered to any location in the global theater, including the Continental United States (CONUS), Outside the Continental United States (OCONUS), on land, at sea, in air, on-base, or a Defense Industrial Base (DIB) partner location.

Decision superiority necessitates consistent, real-time, and resilient access to applications, content, and data at the edge. This entails building a connected battlefield and extending robust Zero Trust cybersecurity postures of enterprise environments out to the tactical edge, wherever it may be. From information on the battlefield to critical DIB partners, experiences are delivered to any point.

All of this aligns with the 2022 National Defense Strategy (NDS) priorities, which call for defending the homeland against multi-domain threats, particularly in the Indo-Pacific region and Europe.

The Challenges of DoD Modernization

To modernize, the DoD must navigate and overcome a multitude of challenges along the way. Among the most pressing issues is the difficulty of ensuring frictionless information access when and wherever needed without adversarial disruption. Several key factors contribute to this problem:

- **Lack of infrastructure:** Limited or absent infrastructure may prevent the extension of performance, resilience, and security to the edge, reducing the effectiveness of real-time access to essential information.
- **Complexity of hyperscale environments:** The intricate nature of these environments often makes cost savings elusive.
- **Interoperability and latency:** These problems block multi-domain warfighter access at scale, limiting the ability of forces to operate cohesively across different platforms and locations.

Effectively managing tactical edge computing demands a mature and robust infrastructure. It must be resilient and secure, and operate in real-time to ensure frictionless warfighter and partner experiences. This ensures essential information is accessible whenever and wherever it's needed, free from interruptions or security breaches. These foundational requirements contribute to data transfer speed, reliability, and overall system resilience. Extending security and compliance to apps and information at the edge often intersects with specific concerns, including:

- **Low visibility:** With different providers, networks, and continually expanding endpoints, maintaining a clear overview becomes increasingly difficult.
- **Resource limitations:** There are too many tools and too few experts to keep pace with evolving threats, leading to potential gaps in security coverage.
- **Compliance challenges:** Maintaining compliance and driving consistent Zero Trust approaches can be daunting, given the dynamic nature of modern cyber threats and the multifaceted environments in which they operate.

Additionally, maintaining a domain advantage requires the ability to share information to any point at the speed of conflict. This entails rapidly moving data from various silos and clouds to the hands of those who need it most: warfighters at the tactical edge. The mission's focus on "all domain information advantage" underscores this critical need, highlighting how essential it is to provide a seamless flow of information where it can be most impactful.

The proliferation of web applications and APIs has exponentially increased the potential points of attack, presenting challenges. Increasing attacks on the DoD supply chain have exposed vulnerabilities that could endanger national security, necessitating immediate action to shore up DIB security. DIB partners' cyber gaps and non-compliance with security mandates add to the risk, potentially allowing adversaries to exploit weaknesses in the system. The complexity of managing these risks is compounded by the fact that many DIB partners utilize an array of web apps and APIs that need to be effectively managed and secured. Challenges specific to DIB partners can include:

- **Advanced targeted threats:** These continually plague supply chain vulnerabilities, leading to potential breaches and data loss.
- **Cybersecurity maturity among smaller partners:** Small DIB partners often lack the maturity or budgets required to meet stringent cybersecurity requirements, potentially leaving them exposed to risks.
- **Analytics needs among larger companies:** Many larger companies are actively searching for better cyber analytics across apps and APIs at the edge to enhance their security postures and respond to emerging threats more effectively.

The evolution of Zero Trust mandates signifies a shift in the security paradigm that calls for a comprehensive re-examination of security protocols at every level. This includes robust visibility into existing infrastructure and understanding where security gaps lie, so they can be addressed promptly.

Collaborative efforts between governmental bodies, the DIB, and cybersecurity experts must be aligned to secure agency mission environments and develop a holistic approach. The overarching aim is not only to respond to threats but to create a robust, adaptive security posture that can preemptively mitigate risks and protect the nation's vital defense apparatus.

Solutions for Mission-Critical Support

Against this backdrop, Akamai's suite of layered solutions provides a comprehensive approach to advancing security.

Akamai Global Edge Platform

The Akamai Global Edge Platform brings the power of Akamai to extend the enterprise security, performance, and availability of hyperscale environments out to the edge, wherever that edge may be. A highly secure, proven, and powerful global platform, it delivers data, content, and apps to the edge swiftly — regardless of location or cloud service provider. Its array of robust features goes beyond traditional solutions by offering capabilities tailored to the unique needs of military and defense operations.

A continual investment toward unifying control and visibility, Akamai's Global Edge Platform ensures a holistic approach by integrating cloud-agnostic edge solutions. This harmonization is key in delivering resilient and responsive services across multiple clouds and platforms, particularly at the tactical edge.

Key Capabilities for Modern Missions

Frictionless experiences

- 100% availability
- Low latency at the edge
- Image and video optimization
- API acceleration
- Continuous app protection without loss of performance

Proactively protect

- Defensive checks at the edge
- Threat intelligence insight
- Reduce attack surface
- Automatically inspects JSON & XML requests for malicious payloads

Simplify and scale performance

- Load balancing to meet demand spikes
- Streamlined management of edge and multi-cloud operations
- Advanced automation integrates many technologies into one centralized solution for complete, unified protections

Unify visibility and control

- Cloud-agnostic edge
- Automated discovery and inspection of all APIs, known and unknown
- Enterprise logs of activity to gain insight into traffic and threat events
- Near-real-time (NRT) situational awareness of daily activities and security events

These services streamline and accelerate the build-out of secure mission-critical capabilities. Through automation, the platform reduces the complexity and time required to deploy advanced security measures, making it essential for modern warfare. This includes defensive checks at the edge to mitigate attacks before they reach core IT, unmatched threat intelligence insight, and managed security services supported by thousands of frontline experts.

Resiliency and Global Load Balancing

The Global Edge platform builds on proven Akamai infrastructure on NPIRNet and SPIRNet as well as current usage of Akamai commercial solutions by several military departments like the Army and USAF. Akamai's Global Edge Platform is an evolution and merger of these two successful execution models within the DoD. It ensures global load balancing with traffic management to meet any demand spike, streamlining the management of multi-cloud and edge operations. This creates frictionless experiences for warfighters in every theater and domain.

Cloud Agnostic, Secure Edge Platform

The platform provides the capabilities of a commercial offering with the security DoD missions require for massive scalability, 100% availability, high performance, and unrivaled threat intelligence across multi-domain operations. It delivers data, content, and apps with the lowest latency across the DoD global theater.

Akamai Web App and API Protector (WAAP)

Akamai's WAAP is layered on the Global Edge Platform to build out Zero Trust architectures at the edge, simplifying and streamlining the security of sites, apps, and APIs. WAAP delivers holistic web applications and end-to-end protections and intelligent automations against a wide range of multi-vector attacks. Its unique features include automatic API discovery, web app firewall, and protection for API-based attacks and DDoS, integrated real-time threat intelligence, built-in bot mitigation, and continuous self-tuning that adapts to new threats and reduces alert fatigue.

Holistic Protection

WAAP delivers a complete suite of protections to defend entire web and API multi-cloud estates. This includes web app firewalls, bot visibility and mitigation, protection against injection and API-based attacks, and DDoS protections. By employing a centralized, intuitive-to-use solution, WAAP ensures a coordinated and efficient approach to security.

Self-Tuning Adaptive Security Engine

WAAP is a continuous self-tuning adaptive security engine that automatically updates using unrivaled threat intelligence from Akamai. This mechanism adapts to new threats in real-time and helps reduce alert fatigue. By constantly analyzing unique agency traffic, it ensures that the security measures are tailored to the specific risks faced by each organization.

Zero Trust Approach and API Protection

The platform applies Zero Trust principles to protect applications at the edge. It offers automatic discovery and inspection of all APIs, whether known, unknown, or changing across traffic and endpoints. This proactive approach enables seamless adaptation to evolving threats and maintains a high level of security for every aspect of the digital infrastructure.

Support for Warfighters and Enhanced Security

WAAP is tailored to support warfighters through image and video optimization, edge compute, API acceleration, and proven scalability for any demand spike. Furthermore, it augments security teams with managed services, enabling organizations to tap into external expertise to reinforce their security postures.

GovShield PDNS

Akamai's GovShield Protective Domain Name Service (PDNS) represents a significant advancement in carrier-grade internet protection. Specifically designed to identify, block, and mitigate targeted attacks such as malware, ransomware, phishing, and DNS data exfiltration, GovShield operates on a level designed to meet the rigorous demands of governmental and defense organizations.

Integration with NSA's PDNS

GovShield can be leveraged in two distinct ways to enhance cybersecurity. The integration with NSA's PDNS, which contains GovShield at its core, is available at no cost to qualified DIB partners. This free offering augments existing email and endpoint security through a combination of Akamai's global threat intelligence and NSA's government-specific intelligence. By doing so, it helps DIB partners meet the minimum DoD requirements, enhancing their overall security posture.

Private Containerized GovShield Service

For organizations requiring a more tailored approach, the deployment of a private containerized GovShield Service is an option. This offers a highly customizable and secure solution that aligns closely with specific operational needs.

Comprehensive Data Tracking and Insights

GovShield enables comprehensive data tracking, providing deep insights into malware trends and the evolution of security postures. Enterprise logs of activity for insight into traffic and threat events offer a transparent view of the cyber landscape, facilitating the identification of potential vulnerabilities and emerging threats.

Carrier-Grade Protection

NSA's carrier-grade PDNS ensures the protection of all internet connections. It blocks not only malware and phishing but also command and control (C2) mechanisms that attackers use to move laterally through a network. This level of protection is instrumental in neutralizing complex, multi-stage attacks that can cripple organizations.

Cost-Effective and User-Friendly

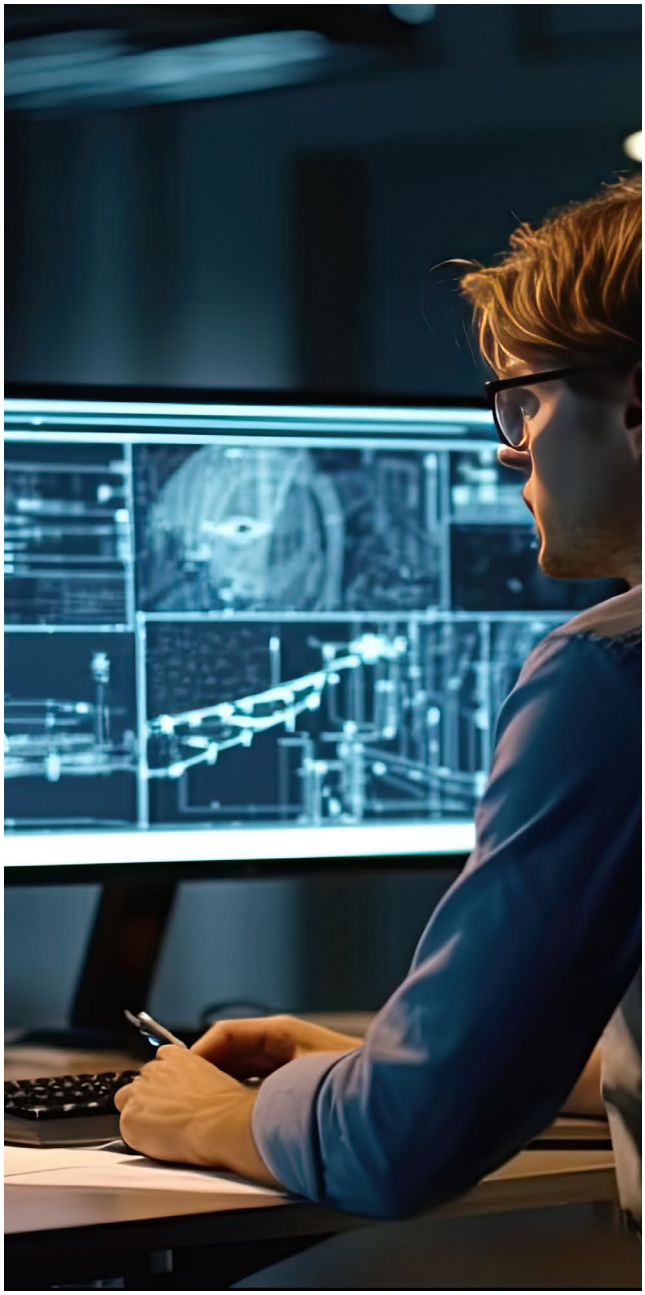
In addition to its robust protection capabilities, GovShield is cost-effective, fast, and extremely easy to install. Available to DIB partners, it's an accessible solution for bolstering cybersecurity.

The Akamai Difference: Threat Intelligence and Protection

Akamai delivers unrivaled geographic reach and threat intelligence to deliver scalable, secure, and high-performance experiences anywhere in the global theater. Our layered security solutions can help improve and extend enterprise performance and availability of hyperscale environments across the DoD enterprise and out to the edge — wherever that edge may be, regardless of the cloud hosting partner.

Our suite of services, such as WAAP, enriches the DoD's defensive measures, integrating them into mission environments. As a long-standing government collaborator with profound DoD insights, Akamai's offerings bolster the oversight, monitoring, and threat counteraction capabilities of defense security teams. Furthermore, our commitment goes beyond providing immediate solutions. We aim for a future where security evolves hand-in-hand with technological advancements, ensuring a fortified and resilient defense mechanism. Through proactive innovation and continuous adaptation, Akamai strives to remain at the forefront of security technology, safeguarding the nation's interests in an increasingly complex digital era.

The future of warfare is at the edge. Contact Akamai today to learn more about how our edge-computing technologies can help warfighters achieve their missions securely and reliably.



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.