White Paper

Global Threats, Regional Solutions: Securing Asia's Public Sector with Akamai

Foreword

As digital transformation accelerates worldwide, technological advancements have improved productivity and social interaction at a personal level and driven economic growth, information accessibility, and cultural exchange at a global level.

However, the risks of financial loss, national security threats, and misinformation due to technology being exploited by adversaries have never been higher.

We have entered an era in which cybersecurity must shift from blocking isolated cyberthreats to mitigating systemic risks that threaten entire operations. For security leaders in critical industries and the public sector, this means cyberthreats today — whether they're targeting citizen services, financial systems, or critical infrastructures — exploit vast webs of technological interdependencies. Defending against them with yesterday's tools is no longer possible.

The cyberthreat landscape is being reshaped by several intensifying forces. Three dominate nearly every conversation I have with critical infrastructure providers.

First is the democratization of offensive capabilities. Sophisticated cyber tools — once available only to nation-states or organized criminal groups — are now commoditized and easily accessible to smaller groups and even novice attackers. Artificial intelligence (AI) has facilitated this shift, allowing adversaries to scale reconnaissance, develop convincing phishing lures, and automate attacks with unprecedented precision. This has changed the balance of power: Attackers can experiment at low cost and high velocity, while defenders must safeguard against a widening set of threats in real time.

Second, rapid digital transformation has created ecosystems of interdependence that transcend traditional technological boundaries. Governments are digitizing citizen services, financial institutions are opening application programming interfaces (APIs), and digital supply chains are becoming core to business operations. While these advancements may fuel operational efficiency and innovation, they also expand the overall attack surface. A compromised AI chatbot, exploited API, or breached supplier is no longer an isolated incident — it can cascade into data exposure, regulatory violations, or large-scale disruption of critical services.

Third, the regulatory and geopolitical contexts are rapidly evolving. Cybersecurity is no longer just about preventing breaches — it's also about preserving data sovereignty, ensuring operational continuity, and maintaining public trust. Governments worldwide are imposing stricter regulations on data protection, cross-border data flows, and incident disclosure. While compliance is still necessary, it isn't a perfect solution. Security leaders should treat it as a baseline then go further by building accountability, transparency, and resilience into their security models.

For today's security leaders, the implications are clear. With adversaries broadening their reach and attack surfaces expanding, absolute prevention is impossible. The age of perimeter defenses is over; resilience must now be the standard. Applications must be secured from code to runtime, and networks must be designed with resilience from the very start.

The path forward requires stronger collaboration across governments, industries, and individuals. Cybersecurity is a shared responsibility, and no single entity can confront the entire threat landscape alone. By fostering public–private partnerships, sharing intelligence, implementing good practices, and jointly investing in resilience, we can keep digital transformation from outpacing our ability to secure it.

Reuben Koh, Security Technology and Strategy Director, Akamai

Executive summary

The global cybersecurity landscape is undergoing a profound transformation driven by rapid technological advancements and escalating threats.

While AI empowers innovation, it also fuels sophisticated cyberattacks, from hyperrealistic phishing to zero-day exploits. Software supply chain vulnerabilities, geopolitical cyber operations, and surging financial fraud further complicate the threat environment, particularly for public sector organizations.

In the Asia-Pacific (APAC) region, critical industries face unprecedented attack volumes, with over 80 billion web application attacks and 7.4 trillion Layer 7 distributed denial-of-service (DDoS) attacks recorded between 2023 and 2024, making it one of the most targeted regions in the world. The reality today is that traditional perimeter defenses can no longer keep up. As AI-enabled attacks grow more sophisticated and interconnected with supply chain compromises, geopolitical tensions, and financial fraud, public sector institutions must shift their focus from prevention to resilience, ensuring continuity even when under attack. Akamai's experience around the world shows what resilience looks like in practice. Whether it is related to defending governments during active cyberwarfare or securing critical infrastructure with Zero Trust, DDoS mitigation, and microsegmentation, Akamai has consistently helped public sector institutions stay operational when it matters most.

This white paper explores these trends, highlights Akamai's proven expertise in protecting government and critical infrastructure, and proposes collaborative strategies to strengthen cybersecurity resilience across Asia's public sector.

Which trends are driving the current threat landscape?

At Akamai, we recognize the rapid evolution of the global threat landscape, due in large part to **advancements in AI**. While these leaps forward have enabled higher productivity yields and faster innovation, they have also created opportunities for threat actors to conduct more sophisticated attacks, such as hyperrealistic phishing and impersonation campaigns driven by deepfake technologies. AI is also enabling attackers to identify application and API vulnerabilities more quickly, including zero-day exploits that can remain unknown to vendors. In fact, recent Akamai research has identified over 80 billion attacks against web applications in 2024, 11 billion of which targeted critical APIs in APAC.

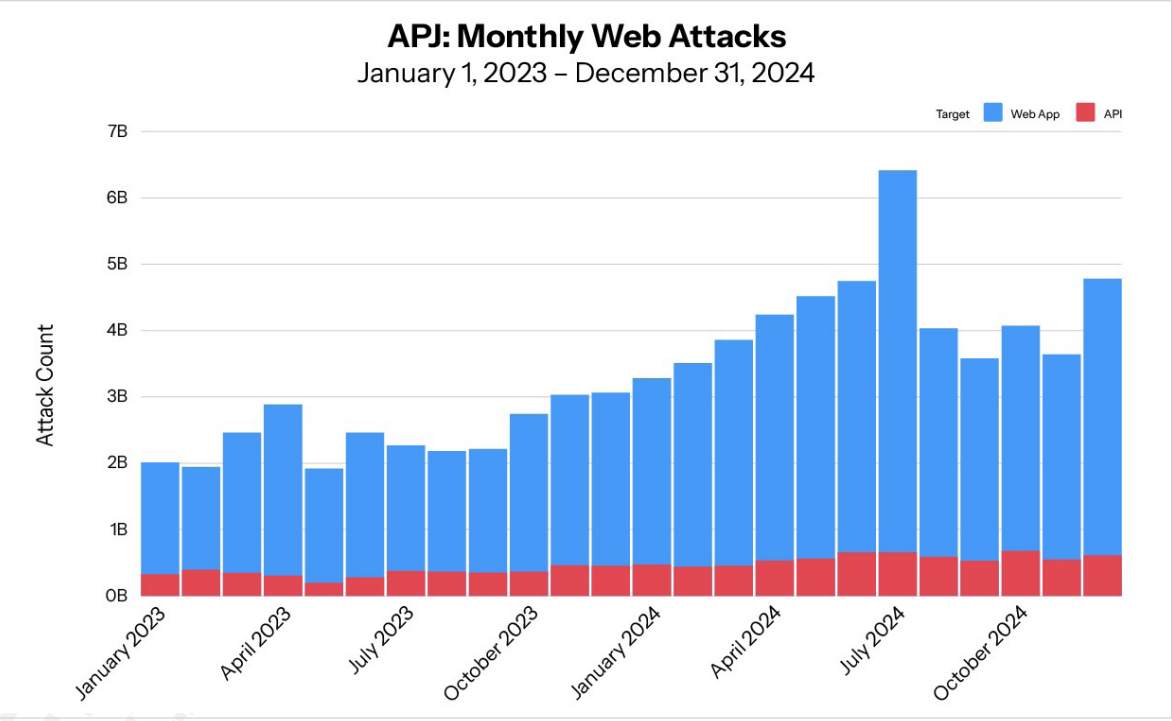

Fig 1: APJ experienced a significant 73% increase in total web attacks year over year, from 29 billion in 2023 to 51 billion in 2024 (Source: State of Apps and API Security 2025)

Software supply chains and third-party dependencies pose another escalating risk. Incidents such as the SolarWinds breach of 2020 underscore how a single compromised supplier can expose thousands of organizations, including critical government networks. In response, governments worldwide have raised the bar. In the United States, for example, security mandates (e.g., President's Executive Order 14028) have been issued to protect national critical infrastructure and software supply chains against these pervasive threats. Following global trends, APAC countries such as Australia have enacted similar regulations, including the Security of Critical Infrastructure Act, to safeguard essential systems and supply chains amid the heightened risk landscape.

Geopolitical tensions are also driving large amounts of cyber activity as state-sponsored threat groups grow increasingly aggressive and sophisticated. Global cyberattack revenue is booming, with businesses and consumers worldwide losing trillions of dollars to cybercriminals every year. As a result, cybercrime has become a low-barrier, high-growth "industry" in which profit-driven attacks like ransomware are the new normal. Meanwhile, nation-states continue to hone their use of cyber tools for espionage, intellectual property theft, and widespread disruption, often focusing on critical infrastructure and government networks. Consequently, DDoS attacks against systems and services are now commonplace, causing large-scale disruption and, at times, extortion. This is especially true in APAC, with more than 7 trillion Layer 7 DDoS attacks from 2023 to 2024 making it the second-most attacked region in the world. As nation-state activity continues to escalate, governments and their allies must brace for more intensive and persistent attack campaigns in the near future.

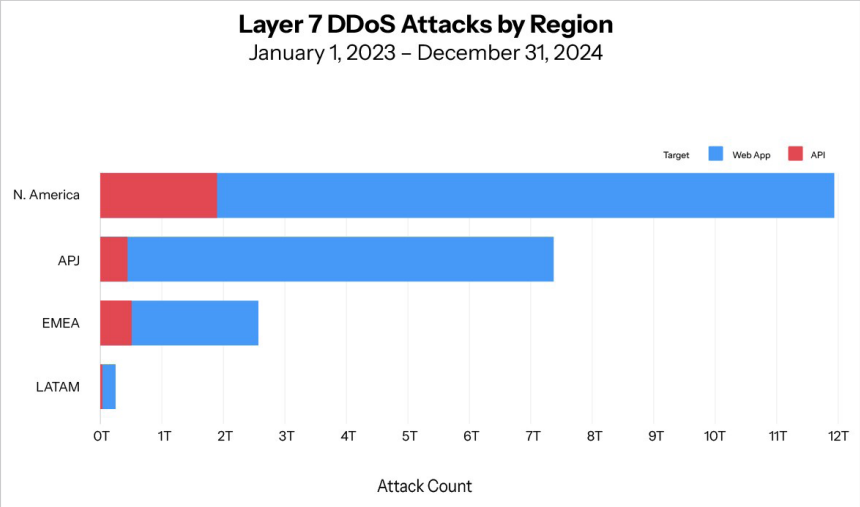

Fig 2: During the reporting period, on a global basis, APJ experienced the second highest number of total Layer 7 DDoS attacks (Source: State of Apps and API Security 2025)

Finally, **financial fraud and scams** are surging worldwide. At the consumer level, crimes like AI-powered phishing and sophisticated social engineering tactics like impersonation scams have spiked. Fraudsters are also exploiting new channels like social media, mobile wallets, and peer-to-peer payment apps. As a result, account takeover attacks using stolen credentials have risen year over year. This trend will only continue; Gartner reported that by 2027, **AI agents will halve the time it takes for attackers to take over an account**.

On the institutional side, organizations in both public and private sectors face increased API abuse and malicious bot activity, with malicious bot traffic accounting for almost 30% of all web traffic we saw in 2024. The problem many organizations face today is that their conventional security tools are no longer effective against these AI-powered threats. AI bots, for example, will easily be able to circumvent static defenses like CAPTCHA. Security needs to evolve to effectively defend against these novel attacks.

The convergence of AI-enabled attacks, software supply chain vulnerabilities, state-driven cyber operations, and skyrocketing fraud and abuse demands a more comprehensive, forward-looking defense strategy. To counter increasingly sophisticated threats, organizations in APAC are moving toward Zero Trust frameworks and prioritizing security investments. Within the next two years, we'll likely see increased investment in AI-powered security used to combat AI-powered threats, widespread maturity of Zero Trust implementations in APAC, and AI-native security like AI-native firewalls that protect large language models and AI deployments.

Attack data snapshot (Source: Akamai SOTI reports)

Attack category	Volume (APJ/global)	Top targeted industries
Web application attacks	80 billion (APAC, 2024)	Finance (~27B), Commerce (~18B)
API attacks	Web attacks: 11 billion (APAC, January 2023–June 2024) Layer 7 DDoS: 444 billion (APJ, January 2023–June 2024)	Commerce (sector with most apps/APIs attacked)
Bot attacks	Bots ~42% of web traffic; 65% malicious (Global, 2024)	Commerce
DDoS attacks (all layers)	Layer 7 (January 2023–June 2024): APAC: 7.4 trillion	Commerce, gaming, finance, video media, high-tech

Akamai's cybersecurity expertise: A proven track record in protecting government agencies and fostering collaborations

Akamai has a long track record of helping governments and critical industries worldwide meet their advanced security requirements, and our core security offerings in Zero Trust, application security, and infrastructure security have been proven in high-stakes environments.

For example, when Russia's invasion of Ukraine escalated, Akamai stepped in as a frontline defender. Beginning in March 2022, **we proactively offered cybersecurity support to the government of Ukraine** against intense cyberwarfare that included a variety of threats — from malware and web attacks to adversarial bots and DDoS campaigns. Notably, Akamai's platform absorbed and stopped highly sophisticated attacks on websites, apps, APIs, and infrastructure, allowing the government of Ukraine to maintain operational continuity amid sustained and persistent attacks.

In the **United States**, **Akamai has been a longtime partner to federal agencies**. We've deployed Zero Trust identity, credential, and access management (ICAM) solutions across both U.S. Department of Defense networks and civilian agencies that strengthen security posture by enforcing continuous, least-privilege access for users and devices. In one instance, **the U.S. Army successfully used our Zero Trust solution** to secure collaboration with contractors and allies without exposing underlying sensitive networks. Our global threat intelligence was also integrated into these services, allowing agencies to block known threats in real time. In addition, **we've protected U.S. government infrastructure with our web security services** (web application and API protection [WAAP], bot mitigation, Domain Name System [DNS]) and with Akamai Guardicore Segmentation for on-premises networks.

In May 2025, Akamai announced **a strategic collaboration with P3M Works to bring Zero Trust ICAM solutions to the U.K. government** and defense supply chains. This joint effort will expand Akamai's proven Zero Trust solutions in the U.S. government to the United Kingdom, ensuring secure third-party access and continuous authentication. This strategic partnership addresses a critical gap that has long been a concern for the U.K. government: securing third-party and contractor access to sensitive defense data.

In **Australia**, we've also strengthened government and critical infrastructure security. **In partnership with Fujitsu, Akamai introduced market-leading microsegmentation** to protect Australia's critical infrastructure networks. This solution isolates and inspects traffic within data centers and cloud environments, effectively containing breaches before they spread.

Akamai is also a founding member of the **FS-ISAC Critical Providers Program**, which aims to secure the global financial sector's supply chain and acts as a form of private sector commitment to public resiliency. As part of the program, Akamai's threat researchers regularly conduct threat intel briefings and contribute to joint research reports to inform stakeholders of shifting tactics.

Across all these cases, there are two key Akamai advantages at play:

- We provide a globally distributed edge platform with thousands of points of presence, allowing traffic and defense logic to run closer to users and devices.
- Our 24/7 Security Operations Command Center (SOCC) and security intelligence team continuously monitor global traffic patterns worldwide, enabling real-time mitigations and adaptive defenses to better protect our customers.

Security solutions built to empower public sector resilience

Akamai's comprehensive security portfolio empowers Asia's public sector to build resilience against sophisticated cyberthreats while ensuring compliance with stringent regulatory standards. The solutions include:

App & API Protector

App & API Protector provides comprehensive protection against Layer 7 attacks, including DDoS, bots, and OWASP top 10 vulnerabilities, ensuring robust security for web applications and APIs.

Bot Manager

Bot Manager provides advanced bot management that detects and blocks bad bots while allowing good bots, ensuring legitimate traffic flows smoothly and the user experience remains seamless.

Account Protector

Account Protector detects and mitigates account takeover, account opening abuse, and credential stuffing. This is crucial for protecting customer accounts and maintaining trust.

Prolexic

Prolexic protects infrastructure from DDoS attacks. It offers robust defense mechanisms to ensure uptime and reliability, even during large-scale attacks.

Enterprise Application Access

Enterprise Application Access provides secure, identity-based access to applications, enabling Zero Trust security models. It ensures that only authorized users can access critical applications, supporting compliance and secure remote access.

The Akamai Guardicore Platform

Microsegmentation helps isolate critical applications and workloads, which reduces the risk of lateral movement within the network. This containment strategy is vital for maintaining operational resilience and ensuring compliance with stringent regulatory standards.

Strengthening cybersecurity collaboration between public and private sectors

To effectively counter the multifaceted cyberthreats outlined earlier, countries in Asia can leverage the combined strengths of government and industry through collaboration between public and private sectors on threat intelligence, preparedness, and incident response. Below are some examples of how these partnerships might work and their benefits:

Establish formal information-sharing networks: Governments can formalize channels for real-time cyber threat intelligence sharing between government agencies (e.g., CERT) and key industries (manufacturers, banks, telecoms, etc.). For example, creating sector-based ISACs information sharing and analysis centers (ISACs) or a national cyber exchange as part of a country's national cybersecurity program (NCSP) can encourage companies to share anonymized threat data and receive government insights. This type of partnership is already established in the financial sector, where global models like FS-ISAC empower critical providers (like Akamai) and banks to collaborate on threat reports, encouraging early warnings for attacks.

Promote Zero Trust frameworks industry-wide: The government should champion and push the adoption of Zero Trust security frameworks across critical sectors, providing guidelines or incentives for companies to implement them. This includes persuading businesses to move beyond perimeter defense to "verify everything" via strong user authentication, network segmentation, and continuous access monitoring. Government IT and critical infrastructure operators should also lead by example (as many U.S. agencies did under federal Zero Trust mandates).

Capacity building and talent development: Collaboration efforts should also extend to building the next generation of cyber defenders through government partnerships with industry and institutions that expand cybersecurity training, simulations, and research and development. Initiatives like joint cyber simulations or internship exchanges will also enhance practical skills. Given the complexity of emerging threats, increasing the overall talent pool and skill level is a strategic imperative.

Enhanced critical infrastructure protection program: Governments can create a dedicated program focused on critical infrastructure cybersecurity. It would work closely with operators in the power, water, transport, and semiconductor sectors to conduct security audits, share threat intelligence, and deploy advanced defenses (like DDoS mitigations) at critical points. Public–private working groups for each sector can build a blueprint for identifying critical systems (e.g., supervisory control and data acquisition systems in power grids) and recommend modern solutions for remediation (e.g., Akamai Guardicore Segmentation). Collaboration with companies like Akamai can also provide insight into protecting infrastructure at the network edge and cloud level, complementing on-premises protections.

How Akamai can help strengthen digital defenses

Given these trends and Akamai's capabilities, we see several possible collaboration areas for countries in Asia:

Securing government and digital services: Akamai's edge security platform can protect online government portals, digital ID services, and public sector applications. By shielding these critical services behind Akamai's high-performing security solution, we can defend against large-scale DDoS and web attacks that aim to cause mass disruption. Our extensive experience defending governments worldwide — whether in peacetime or against cyberwarfare — has shown us what it takes to keep systems online during active attacks. Today, we protect numerous government ministries and agencies across dozens of countries in Asia.

Securing the supply chains of industries powering the global economy: Akamai can work with critical manufacturers and government agencies to assess and accelerate their Zero Trust maturity. Guardicore microsegmentation can isolate manufacturing control systems as well as IT and research and development networks, preventing lateral movement in the event of a breach. For example, Taiwan's semiconductor fabrication and related industries — critical assets both nationally and globally — can benefit from these protections. We can also extend this to logistics and suppliers by applying Zero Trust access controls (as in our U.S./U.K. government ICAM solutions), where only authenticated users can reach sensitive systems.

Defending against financial fraud and abuse: Akamai offers advanced fraud mitigation and identity protection services — such as detecting credential stuffing attacks and fake account creation by malicious bots — that can strengthen a country's vibrant financial sector. We can also help secure online, mobile payment, and financial APIs against fraud and abuse. Finance is consistently one of the most impersonated sectors used for scams. We can help detect fake websites, social media accounts, and even mobile apps pretending to be a bank and take them down to protect consumers.

Resilience in energy and utilities: Energy grids and utilities like electricity, water, and telecommunications are high-value targets for sabotage or extortion, and integrating Akamai's security into these traditionally on-premises systems can provide a critical layer of defense. For example, remote access to industrial systems can be brokered through Akamai's Zero Trust access, ensuring strong authentication, verification, and monitoring for every session. As an added layer of protection, Akamai Guardicore Segmentation operates even in limited-bandwidth environments, applying consistent security policies even if connectivity is low or unstable. Finally, Akamai's powerful DDoS defenses can also protect utility control centers from unpredictable volumetric attacks, ensuring that essential services are always available.

These opportunities align existing security initiatives in APAC countries with Akamai's global experience. By leveraging Akamai's security capabilities and rich experience in protecting governments and critical sectors, countries can develop a security posture resilient to today's wide range of attack tactics. Akamai is keen to explore collaboration on securing digital public services, protecting critical industry supply chains, preventing financial crime, and strengthening resilience across sectors critical to a country's economy.

Why Akamai?

Our strategic value can be summarized in three core strengths:

Global cloud and security platform: Akamai operates the world's most widely distributed cloud and security platform. Our network delivers web content, cloud computing, and security services from thousands of locations worldwide, minimizing latency and localizing threat mitigation. Because of this global infrastructure, governments and businesses can rely on Akamai's in-country points of presence to handle traffic surges or attacks confidently, without needing massive on-premises infrastructure. Akamai's platform was originally built to ensure content reaches users quickly and reliably, and these same qualities translate into resilience and continuity benefits for all our security customers.

Proven security capabilities: From our industry-leading WAAP and bot management to DDoS and DNS defenses — all built into our distributed, intelligent platform — we enable an effective, holistic defense regardless of a threat's origin. Our security research team continuously monitors global web traffic for emerging threats, identifying new attack patterns and campaigns daily. Crucially for countries in Asia, this provides an early warning signal on potential attacks targeting APAC. When a crisis hits, our global SOCC and incident response teams are always on call. We can rapidly route traffic through alternate paths, deploy new mitigation rules instantly, and collaborate with your response teams if needed, leveraging our proven expertise in defending under fire.

Scale in stability and crisis: A good partner will not only secure normal operations but also handle intensive attack pressures. Akamai's platform is built to absorb massive attack volumes for extended periods of time for both multicloud and on-premises environments (via Akamai Guardicore Segmentation, API Security, Prolexic, and App & API Protector Hybrid), ensuring that government agencies can adopt hybrid architectures without blind spots. Additionally, our history of global government work (in the United States, United Kingdom, Japan, Australia, and more) means we understand the rigor and strict compliance expected from us, as well as the unique situations that apply to individual countries. In practice, this also means countries get solutions that meet the highest standards, like FedRAMP in the United States or the Infosec Registered Assessors Program (IRAP) in Australia.

In conclusion, we believe that combining Asia's technological ingenuity with Akamai's experience and platform can elevate security postures across both the public and private sectors. We propose to broaden our ongoing strategic partnerships by not only delivering technology but also contributing to the cooperative development of country-specific cybersecurity standards. The threats, from AI-driven fraud to geopolitical cyber incursions, will not wait. Together, we can ensure that Asia's growing, vibrant digital economy and infrastructure remain secure and resilient.

Take the next step toward resilience

Akamai helps critical industries across APAC, such as finance and the public sector, strengthen visibility, enforce control, and reduce operational risk — without slowing innovation. Connect with our team to explore how we can help you secure what's next.

Author: Reuben Koh, Security Technology and Strategy Director, Akamai
Reviewer: Ashvini Singhal, Sr. Director Product Management, Akamai

Akamai is the cybersecurity and cloud computing company that powers and protects business online. Our market-leading security solutions, superior threat intelligence, and global operations team provide defense in depth to safeguard enterprise data and applications everywhere. Akamai's full-stack cloud computing solutions deliver performance and affordability on the world's most distributed platform. Global enterprises trust Akamai to provide the industry-leading reliability, scale, and expertise they need to grow their business with confidence. Learn more at akamai.com and akamai.com/blog, or follow Akamai Technologies on X and LinkedIn. Published 10/25.