State of the Internet | V12 Issue 01

Akamai Security

SOTI

Apps, APIs, and DDoS 2026

Prepare for the Convergence Crisis: Mitigating API, AI, and DDoS Risks

Contents

Introduction

In 2026, the big story is that the threat landscape is no longer being transformed by flashy new attack methods — it's being industrialized. The convergence of web applications, APIs, and distributed denial-of-service (DDoS) attacks that started as a trend is now standard operating procedure. What has changed are the speed, precision, and cost-effectiveness of these cybercriminal campaigns.

This year's first State of the Internet (SOTI) Security research report examines this convergence crisis. We review what happened with application security, API threats, and DDoS attacks throughout 2025, with a particular focus on how artificial intelligence (AI) has turbocharged the vulnerabilities that exist around these new industrialized attack methods. The numbers tell the story: Web application attacks continued to rise by double digits, DDoS attacks continued their explosive evolution (with Layer 7 DDoS attacks surging by 104%), and API abuse evolved from a technical headache into a legitimate business continuity crisis.

Three shifts stand out that security leaders and practitioners should keep an eye on:

Attack economics has fundamentally changed.
Thanks to automation, sophisticated campaigns that used to require deep resources and serious technical chops can now be launched at scale for next to nothing. Attack timelines have collapsed from weeks to hours. AI-powered recon, adaptive payloads, and botnet as a service platforms haven't just accelerated threats — they've eliminated the window for error entirely.

Application and API security are completely intertwined.
Organizations are still treating these as separate problems, creating ideal visibility gaps for attackers to exploit. Modern apps and their APIs are inseparable, and threat actors move between them seamlessly, looking for the easiest way in.

Damage looks different than it used to.
Some of the most harmful attacks we observed in 2025 didn't make headlines with massive outages. Instead, they showed up as degraded performance, surprise infrastructure bills, lost conversions, and burned-out security teams — business problems that often fly under the radar until the damage adds up. When organizations don't keep a focus on internet hygiene, they leave their properties with the proverbial door wide open for attackers to walk through.

This year's report gives security practitioners and business leaders data-driven insights to help them understand how these dynamics are playing out globally. The bottom line: Organizations that nail the fundamentals — access control, rate enforcement, abuse prevention, and resilience — consistently beat those that are chasing narrow, AI-specific fixes.

The attacks aren't slowing down. Let's jump in and find out whether today's cybersecurity strategies match the reality of how the attacks actually work.

Expert insight

The economics of modern internet attacks

In North America, we are seeing the trend of industrialization, not reinvention, have an impact on multiple aspects of security strategy. Capabilities that are used to optimize business operations are a double-edged sword when used as mechanisms to optimize attacks. Discussions across the C-suite have focused on understanding these patterns, their effects, and their interconnected risks so as to align their strategy with reality.

Decoding the signals

Our research reveals several patterns — and none of them exist in isolation. These include:

Convergence has shifted from an emerging trend to an operating model. Web application attacks, API abuse, bot activity, and DDoS increasingly appear as parts of the same campaigns. Attacks begin with automation, move through APIs, and escalate into availability or cost pressure when resistance is encountered. Treating these as separate problem sets obscures how attackers actually work and creates visibility gaps that persist year over year.

The economics of attacks continues to evolve. Attacks are inexpensive to launch, easy to repeat, and difficult to attribute. They are designed to blend into legitimate traffic rather than announce themselves. Manual detection and response models struggle in this environment, especially when the goal is degradation and persistence rather than immediate disruption.

Availability and cost remain top impact metrics. Many of the most damaging DDoS attacks observed do not just result in obvious outages. Instead, they manifest as performance degradation, forced scaling events, inflated infrastructure spend, or exhausted operational teams. For API attacks, these failures often surface as reliability or business issues long before they are recognized as security problems.

AI has proven to be a force multiplier, not a stand-alone category of risk. Across web applications, APIs, and DDoS, AI-driven activity reinforces existing weaknesses rather than introducing entirely new ones. Narrow, AI-specific fixes can't always provide the big picture value that the fundamentals are better positioned to deliver.

Old attacks now executed at machine speed with stealth impact

Web application attacks continue to increase, but the character of those attacks is shifting. The most meaningful change is the move away from overt vulnerability exploitation and toward the abuse of application logic and workflows. Attackers increasingly operate through authenticated paths, using automation to mimic legitimate users and persist over time.

Bots and scripted clients dominate this activity. Headless browsers and automation frameworks allow attackers to maintain state, adapt behavior, and blend into normal patterns. As a result, defenses that rely primarily on signatures or static indicators struggle to distinguish intent from volume.

AI accelerates this trend by compressing timelines. Endpoints are discovered faster. Parameters are probed more efficiently. Payloads are adjusted continuously. The underlying techniques are familiar, but the speed of execution reduces the margin for error and the window for response.

The business impact of web application attacks increasingly appears indirectly. Performance degradation, conversion loss, and alert fatigue often precede clear indicators of compromise. Over time, these effects erode trust and increase operational cost, even when no single event appears to be catastrophic.

APIs and AI expand the attack surface

APIs remain the attack surface that cybercriminals feel delivers the best return on investment. APIs expose core business logic, enable automation, and provide direct access to data and functionality. Compared with traditional web attacks, API abuse is often quieter, harder to detect, and more damaging when it succeeds.

Shadow and zombie APIs continue to be a persistent issue as development velocity outpaces inventory and governance. Forgotten endpoints, inconsistent authorization models, and assumptions about trusted use create predictable opportunities for abuse. In most cases, these failures are not sophisticated — they are structural.

As AI adoption accelerates, one reality becomes increasingly clear. AI endpoints are APIs. They accept input, invoke logic, and return output. The interfaces may be new, but the security principles are not. Prompt input is still input. When it is not validated, constrained, or contextualized, systems behave in unintended ways. Output handling matters just as much. Ungoverned responses can leak sensitive data, expose internal state, or be reused as trusted input elsewhere.

The expansion of AI-driven systems has increased both the volume and velocity of API interactions. Model endpoints, agent workflows, and tool integrations all depend on API access that was often not designed for autonomous or unbounded use. Attackers follow this dependency directly, using APIs to enumerate functionality, exploit logic flaws, and drive excessive consumption or cost-based abuse.

API security cannot stand alone

One of the most important lessons reinforced by this data is that API security cannot stand alone. API failures cascade into web applications, identity systems, and availability controls. Treating APIs as a separate problem space guarantees visibility gaps that attackers are quick to exploit.

In 2026, effective API security is less about discovering new controls and more about enforcing discipline across access, rate, and intent. APIs are not a secondary surface. They *are* the surface.

Brent Maynard
Senior Director for Cybersecurity Strategy, Akamai

Key insights of the report

APIs have become the dominant attack surface for modern enterprises, with the average number of daily API attacks up by 113% year over year.

- Approximately 61% of API attacks in 2025 involved unauthorized workflows and abnormal activity, up from 30% in 2024. This shift shows that attackers are moving away from traditional web attacks toward behavior-based threats.
- An average of 3,000 APIs per customer contained sensitive data, and 12% showed security weaknesses; 24% of those issues pertained to sensitive data exposure. The growth of agentic AI amplified this trend, reinforcing that securing AI means securing APIs.

Web attacks (including attacks that target API endpoints and web applications) increased by 73% between 2023 and 2025, underscoring the continued importance of strong cyber hygiene and security fundamentals in today's evolving threat landscape.

Layer 7 DDoS attacks surged by 104% over the last 2 years (2023–2025).

Super botnets like Aisuru and Kimwolf (TurboMirai variants) enable accessible DDoS as a service, making sophisticated attacks available to anyone.

AI is a force multiplier.

- AI reinforces existing weaknesses rather than creating new categories. Organizations that chase narrow AI-specific fixes miss the fundamentals. AI-assisted code generation (vibe coding) is introducing new vulnerabilities and misconfigurations that often reach production untested.
- Agentic AI vulnerabilities are expanding the modern attack surface. A new Open Worldwide Application Security Project (OWASP) framework identifies 10 threats specific to AI agents that make autonomous decisions (goal hijacking, tool misuse, memory poisoning, etc.).

API security

The data in this section on API attack trends comes from the Akamai API Security platform, which detects both web-based and behavior-based API attacks.

APIs are the connective tissue of modern organizations that drives digital experiences and powers real-time data exchange across applications, customers, and partners. However, this same interconnectivity creates a vast attack surface, with APIs now among the most exposed entry points in the enterprise environment. Unlike traditional web attacks that target APIs, behavior-based API attacks tend to be stealthier, more arduous to detect, and more dangerous when they slip through the cracks.

The upcoming Akamai 2026 API Security Impact Study indicates that 87% of survey respondents reported experiencing an API-related security incident in 2025. And our telemetry data further highlights the scale at which API attacks are escalating. A year-over-year comparison showed a sharp rise: The average number of API attacks per enterprise in 2025 was 258, up from 121 in 2024, accounting for a 113% increase (Table 1).

Average API Attacks per Enterprise per Day

Month	Average Attacks per Day	
	2024	2025
January	75	205
February	70	230
March	55	215
April	74	275
May	107	286
June	74	310
July	114	343
August	153	332
September	197	257
October	189	221
November	176	211
December	169	214

Table 1: APIs are now the prime targets of exploitation as exemplified by the significant growth in the average number of attacks experienced by each enterprise

Beneath those numbers lies a more troubling reality: Companies without dedicated API security solutions often never see these threats coming. Without visibility or detection tools in place, attacks can slip through unnoticed, leading to data exposure and service disruption.

Common API exposures

In the State of Apps and API Security 2025: How AI Is Shifting the Digital Terrain report, a subset of our security alerts were mapped to frameworks like MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and OWASP, along with regulatory standards including the General Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCI DSS). But for this report, we researched the top OWASP API security risks (2023) that are defining today's threat landscape, providing a granular look at the vulnerabilities and attack patterns that shaped 2025 (Table 2).

Top 5 API Vulnerabilities

OWASP Top API Security Risks	Volume of Observed Issues
API8:2023 — Security Misconfiguration	39.61%
API3:2023 — Broken Object Property Level Authorization	35.11%
API2:2023 — Broken Authentication	18.56%
API5:2023 — Broken Function Level Authorization	3.70%
API9:2023 — Improper Inventory Management	1.55%

Table 2: Misconfigurations, broken object property level authorization, and broken authentication are the top three vulnerabilities our customers encountered in 2025

In 2025, security misconfigurations, broken object property level authorization (BOPLA), and broken authentication emerged as the most prevalent vulnerabilities. Misconfigurations led the race, accounting for an average of almost 40% of observed issues. Despite being largely preventable, the rapid deployment cycles typical of DevOps environments often leave little time for proper hardening, which creates entry points for attackers.

Among our affected customers, BOPLA and broken authentication ranked second and third, representing approximately 35% and 19% of discovered vulnerabilities, respectively. Exploitation of BOPLA flaws enable unauthorized access to sensitive data, creating privacy and compliance risks, while weak authentication controls leave APIs vulnerable to brute-force and credential stuffing attacks.

All in all, these issues (misconfigurations, insecure authorization, and broken authentication) represent systemic weaknesses that attackers are increasingly exploiting. Misconfigurations, in particular, can significantly raise the risk exposure of an organization, especially as automation and AI expand their reach. And with the rise of AI-assisted code generation (often called vibe coding), developers can produce code faster and in greater volumes. However, this surge in AI-generated code often introduces errors, broadening an organization's attack surface.

Top API incidents

We also analyzed API incidents or attack attempts recorded as suspicious based on our confidence scoring. This allows us to proactively alert our customers to any malicious activity or abnormal behavior that they should look into (and confirm that it happened). Table 3 shows that, based on our telemetry data, approximately 35% of incidents per affected customer involved unsafe consumption of APIs. Additionally, more than 21% of incidents per affected customer involved broken authentication, followed by broken function level authorization at just over 17%.

Top 5 API Incidents

OWASP Top API Security Risks	Volume of Incidents per Affected Customer
API10:2023 — Unsafe Consumption of APIs	35.32%
API2:2023 — Broken Authentication	21.33%
API5:2023 — Broken Function Level Authorization	17.34%
API3:2023 — Broken Object Property Level Authorization	16.58%
API7:2023 — Server-Side Request Forgery	3.68%

Table 3: More than one-third of the API incidents per customer were caused by unsafe consumption of APIs

Authentication issues continue to challenge organizations. Vulnerabilities like broken object level authorization (BOLA) and BOPLA remain difficult to detect with traditional, signature-based tools. Addressing these flaws requires solutions capable of analyzing API behavior and identifying anomalous activity in real time. A notable example is the 2025 Tea app breach, which exposed more than 1.1 million private messages. As APIs increasingly become primary entry points for attackers, security must be integrated into every aspect of application development by default — it is no longer optional.

The risks of data leaks

When access controls are misconfigured or incomplete, APIs frequently expose a plethora of sensitive data, such as personally identifiable information (PII), protected health information (PHI), authentication credentials, user's activities online (browsing history), and financial data. This problem often stems from vulnerabilities like BOPLA and BOLA, which allow unauthorized users to view or manipulate data they shouldn't access. This risk is also compounded by shadow (undocumented) and zombie (deprecated) APIs that are active but operate outside normal governance — the lack of monitoring makes them easy targets for attackers.

The boom in agentic AI intensifies the risks of sensitive data exposure within APIs. Since AI depends on APIs for integration and data exchange, the volume of sensitive information traversing these interfaces has increased exponentially. In today's AI-driven environment, securing AI truly starts with securing APIs.

The impact is far reaching: Leaked API data fuels identity theft, fraud, privacy violations, and regulatory noncompliance. In 2025, we observed that each customer has an average of 3,000 APIs that contain sensitive data. Approximately 12% of those APIs showed security weaknesses, and 24% of those weaknesses pertained to sensitive data exposure findings such as API input validation attacks and Lightweight Directory Access Protocol (LDAP) injection, among others. Even more concerning, the number of APIs that expose sensitive data with sensitive data–related findings continued to rise, increasing from an average of 71 per customer in 2024 to 86 per customer in 2025.

Many organizations lack a complete inventory of their APIs, and even those that have a complete inventory often don't know which APIs expose sensitive data. According to the Akamai 2026 API Security Impact Study, 77% of respondents report having a full API inventory, but of those, only 23% know which of their APIs return sensitive data. This is concerning on two fronts. First, this all too common visibility gap ensures a continued lack of understanding about what sensitive information an API can return; all it takes is a single misconfiguration or overlooked API endpoint for an attacker to access valuable data. Second, the aforementioned 77% figure represents only the APIs that security teams know of; many teams use tools that can't detect unmanaged APIs. This means a large portion of the API estate lives undetected.

Compliance considerations

APIs represent a critical compliance factor beyond security risks, as regulatory frameworks increasingly mandate their protection to safeguard sensitive data flows. A single compromised endpoint can expose millions of records, ranging from credit card and banking details to personal medical histories, insurance information, and proprietary business assets. Even API keys and tokens, when stolen, can enable unauthorized system access, compounding the potential damage to affected organizations. When such incidents violate regulatory requirements, companies risk substantial fines, legal exposure, and diminished customer trust.

Although many regulations do not explicitly mention APIs, the requirements clearly apply to them. The European Union's GDPR, for example, requires any system that processes personal data (including APIs) to implement "appropriate technical and organisational measures" to prevent unauthorized access, loss, or misuse. Its principles of data minimization, access control, and data subject rights, all influence how APIs must handle and secure personal data.

The PCI DSS 4.0 standard makes API security explicit, stressing visibility, continuous monitoring, and secure development practices across the API lifecycle. It emphasizes maintaining a comprehensive API inventory and continuously monitoring API activity and behavior to detect anomalies and abuse. Similarly, the National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF) offers guidance for building secure software, keeping it protected throughout its lifecycle, and addressing vulnerabilities when they emerge. And APIs are at the core of software development.

The case for defense-in-depth strategy

One of the seismic shifts we observed in 2025 was the rise of behavioral attacks, such as business logic abuse, over more traditional web attacks against API endpoints. Our telemetry data showed that 61.18% of API attacks in 2025 involved unauthorized workflows and abnormal activity — a sharp increase from 30.01% in 2024 (Table 4). This trend indicates that attackers are moving away from familiar exploits like Structured Query Language injection (SQLi) toward logic-based abuse of how APIs handle business processes.

API Attack Types

Attack Type	2024	2025
Behavior threats	30.01%	61.18%
Web attacks	69.99%	38.82%

Table 4: One of the most significant trends in API attacks is the shift away from traditional web attacks toward more behavior-based tactics

Traditional defenses such as web application firewalls (WAFs) often fall short against these attacks because they are primarily designed to detect signature-based threats. Organizations are strongly encouraged to adopt a defense-in-depth strategy that combines WAFs with dedicated API protection solution technologies that provide visibility and detection capabilities for both conventional web attacks and behavioral risks, including business logic abuse and excessive data exposure. Equally important are API testing and runtime monitoring, which help security teams identify gaps in how APIs handle data and enforce authentication and authorization.

Expert insight

Defending against the emerging threats posed by agentic AI

We have talked a lot about large language models (LLMs) and generative AI (GenAI) at Akamai but today's primary business focus is shifting to agentic AI — and the threat actors are following suit. In the simplest terms, agentic AI is AI that is not just responding to questions but making decisions for employees and customers. This expands the attack surface and changes the threat profile.

It is time to leverage a core industry best practice from OWASP to understand how to prioritize mitigating vulnerabilities. OWASP released a white paper called Agentic AI — Threats and Mitigations in February 2025 then updated it in December to follow their more popular top 10 format. This gives cyber leaders the ability to evaluate their agentic AI capabilities and determine where they have risk.

A key feature of these white papers is the threat modeling — it is one of the links between the two documents. It demonstrates how to model agents not as applications, but as decision-making entities with memory, identity, and authority, and explains how to follow reasoning paths, state persistence, and action chains. Infosec teams can map threats back to categories to assess coverage, consistency, and residual risk, while using the Top 10 language to track and communicate findings to leadership. Together, these white papers shift threat modeling from "what could exploit the system" to "what could misdirect the agent" — which is the defining risk of autonomous AI.

Guidelines, a roadmap, and industry-standard taxonomy

For example, take an attack vector like "agent goal hijack" in which an attacker manipulates an agent's objective through techniques like prompt injection via payloads embedded in web pages or documents to redirect a system to exfiltrate sensitive data or misuse connected tools. OWASP provides a series of mitigation guidelines from AI firewall and runtime validation all the way to red team and insider threat programs. These detailed guides for each threat technique provide a great baseline and include a mapping matrix to make the review simple.

Although the top 10 is perfect for providing a prioritized roadmap, I would also point out that the original white paper has a great set of six playbooks. These don't map perfectly to the top 10 but for teams that prefer the playbook format, they provide a great starting point to leverage broader concepts.

Finally, for larger companies with more mature policy documentation, these documents provide an excellent industry-standard taxonomy. They define concepts like "tool misuse" so that the team can better coordinate within the cybersecurity team, as well as with legal, compliance, vendor management, and IT.

Mitigation of the Top 10

For reference, here are the OWASP Top 10 for Agentic Applications threat vectors for 2026:

ASI01:	Agent Goal Hijack
ASI02:	Tool Misuse and Exploitation
ASI03:	Identity and Privilege Abuse
ASI04:	Agentic Supply Chain Vulnerabilities
ASI05:	Unexpected Code Execution (RCE)
ASI06:	Memory & Context Poisoning
ASI07:	Insecure Inter-Agent Communication
ASI08:	Cascading Failures
ASI09:	Human-Agent Trust Exploitation
ASI10:	Rogue Agents

Mitigation requires a mix of managing vendors, coding, and using best practices. In many cases, the current security controls are addressing these issues but it is always a solid plan to review industry frameworks to validate the organization's security baseline. Addressing these challenges requires a combination of process and technical controls. Because of the added complexity from GenAI agents autonomously making decisions, it is not easy to map controls like web/API and runtime enforcement controls. On the technical side, basics like AI firewall, API protection, bot management, runtime defense, and DDoS protection must be reinforced by principles like Zero Trust–based microsegmentation to minimize potential impacts.

Steve Winterfeld
Advisory Chief Information Security Officer, Akamai

DDoS attacks

Today's DDoS landscape

DDoS attacks remain one of the most frequent and most disruptive tactics employed by cybercriminals. In addition to amplification attacks and direct high-volume floods launched from powerful single servers, botnets such as Kimwolf and Aisuru have been widely used to conduct crippling DDoS volumetric floods. Yet, DDoS campaigns continue to evolve beyond simple volumetric floods to also target firewalls, APIs, and application servers. They often do this by leveraging exploited vulnerabilities or misconfigurations. Additionally, botnets are often composed of compromised consumer Internet of Things (IoT) devices, cloud instances, and proxy networks, which enables these operations to be larger and more difficult to detect.

Understanding the layers of DDoS risk

Modern DDoS attacks are launching hybrid assaults that challenge traffic over ports and protocols across multiple layers of the Open Systems Interconnection (OSI) model.

Volumetric floods occur at the network and transport layers (Layers 3 and 4) through UDP, SYN, ICMP, or amplified DNS/NTP reflection floods. Application-layer (Layer 7) campaigns focus on HTTP GET/POST floods and other web protocol abuses to exhaust CPU and memory on targeted servers, APIs, GenAI services, or websites.

Botnets composed of compromised IoT devices, cloud instances, and proxy networks further make these operations larger and more difficult to detect.

As noted in the State of Apps and API Security 2025 report, attackers are increasingly turning to AI and automation to adapt their tactics in real time, enabling more precise targeting, faster scaling, and easier evasion of traditional defenses. In response, defenders are deploying AI-driven behavioral analytics, anomaly detection, and automated mitigation to identify and neutralize these sophisticated attacks. Robust protection of Layers 3, 4, and 7 with a multilayered, adaptive defense approach remains crucial to mitigate these evolving DDoS threats in 2026.

Global DDoS attack trends

Layer 7 DDoS attacks have consistently surged faster in frequency over the past two years with a cumulative 104% increase between 2023 and 2025. The year-over-year increase from 2024 to 2025 was 61% (Figure 1). Much of this is because these types of attacks are easier to launch via botnets, especially with the help of AI technology, to target APIs and web apps.

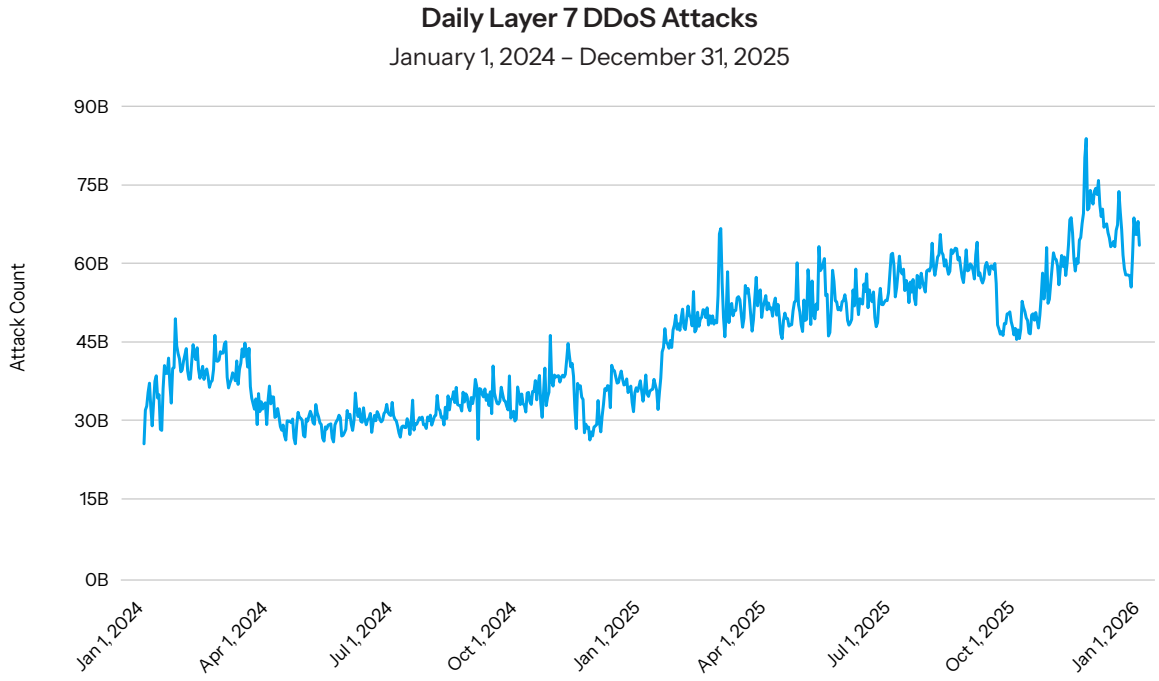

Fig. 1: Layer 7 DDoS attacks are consistently increasing in occurrence rate over time, with a 61% year-over-year increase

This steady increase over time doesn't look dramatic but adds up to a large difference, with some spikes making potentially significant impacts on networks. It is important to track the levels of both general sustained attacks and record setting peaks as organizations review their DDoS protection solutions.

Figure 2 shows that the numbers of Layer 3 and Layer 4 DDoS attacks have grown more slowly in count but the attacks have achieved massive scale (multiterabit in size). Also, Akamai researchers have been observing that while Layers 3 and 4 DDoS attacks are becoming even bigger, those larger volumetric attacks are also increasing in frequency (Figure 3).

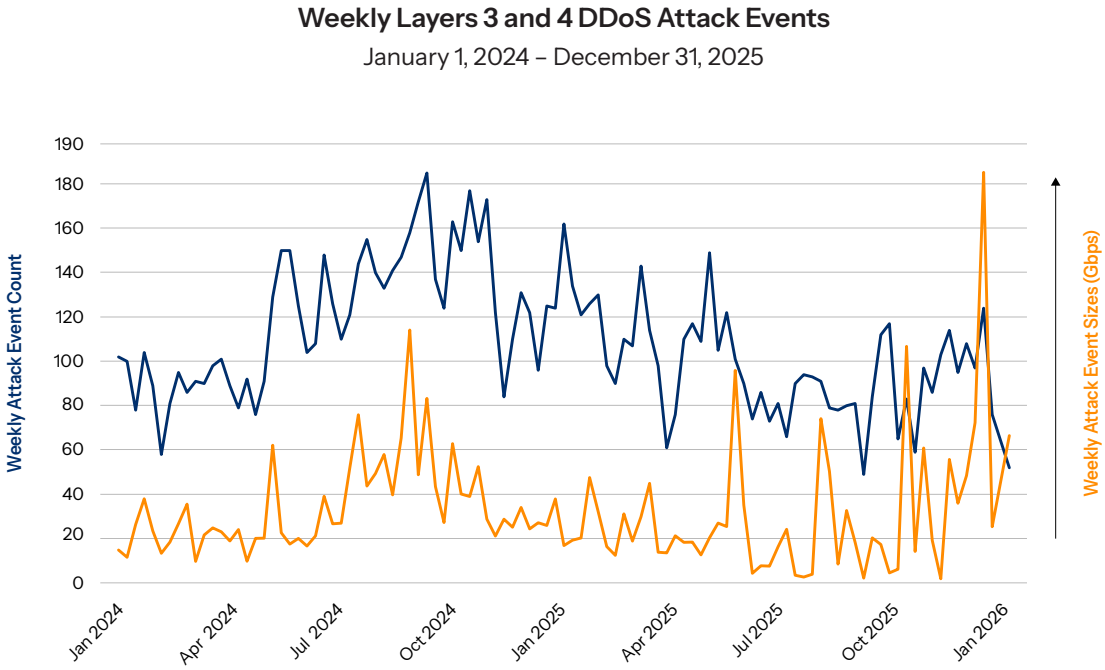

Fig. 2: Although the number of Layer 3 and Layer 4 DDoS attack events have declined slightly over time, attacks are increasing in size

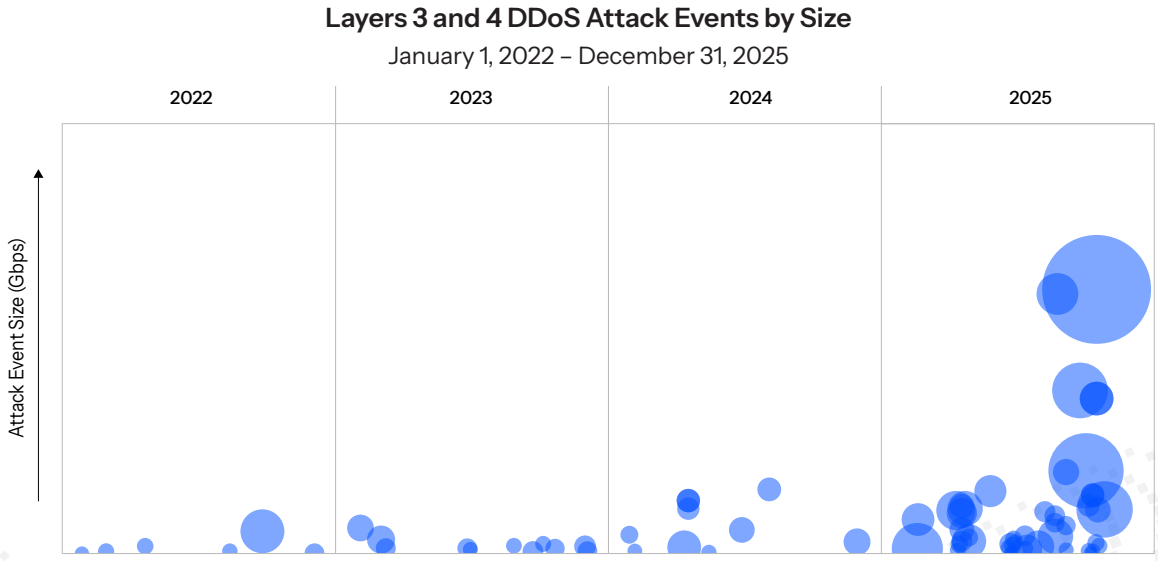

Fig. 3: A use case snapshot showing the dramatic increase in frequency of huge Layers 3 and 4 DDoS over the last 4 years

Unlike Layer 7, Layers 3 and 4 DDoS attacks can cause broad and immediate blackouts by flooding entire network bandwidths. Additionally, Layer 7 DDoS often entails cheap, basic bots firing HTTP requests without deep reconnaissance or tailored request patterns, some of which end up being nonimpactful. Therefore, some Layer 7 events, even though they are more accessible, may be more basic and not as threatening as Layer 3 and Layer 4 attacks.

A multilayer DDoS attack

DDoS attacks have also grown increasingly sophisticated in their attack methodology. Figure 4 is a snapshot of a customer that experienced a dynamic attack powered by a TurboMirai variant that shifted between Layers 3 and 4 and Layer 7.

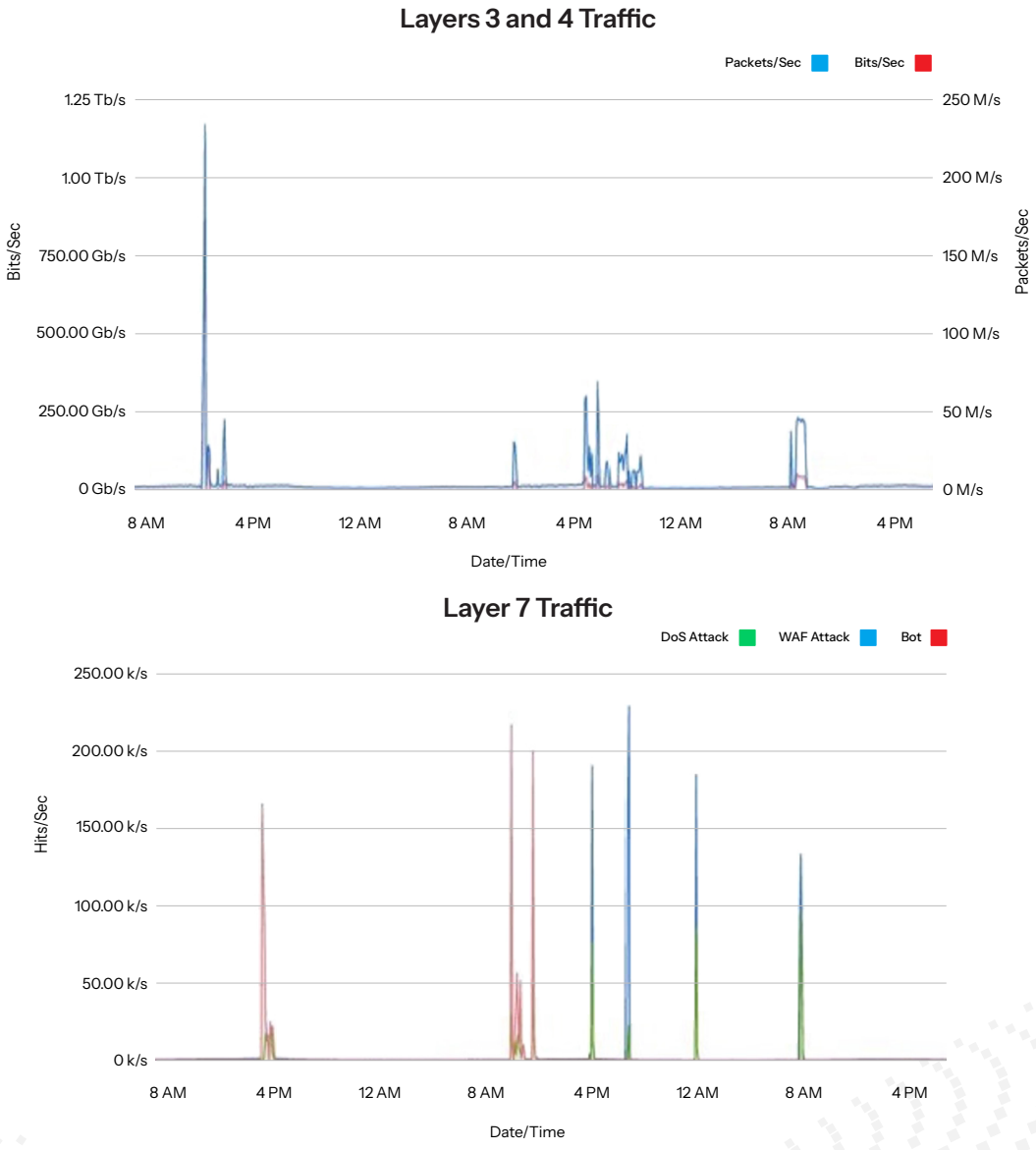

Fig. 4: A recent multilayer attack by a super botnet powered by a TurboMirai variant

Attackers are flexible, capable of shifting rapidly across systems and exploiting vulnerabilities across multiple vectors. Modern attackers can rely on a single tool or platform to coordinate complex, multilayer offensives by jumping from environment to environment and cause disruptions in real time based on the results they are experiencing. This adaptability allows attackers to probe diverse systems for weaknesses and adjust their methods on the fly, prompting companies to rely on specialized DDoS mitigation services for protection.

DDoS attacks at all layers are increasingly driving up business expenses; Layer 7 threats, in particular, are raising costs through prolonged detection and mitigation efforts at the application layer. Because these attacks are sometimes subtle (operating within typical web traffic patterns) and harder to distinguish from normal requests, they can slip past standard firewalls and basic DDoS volumetric protection tools. In turn, this forces organizations to spend more money on advanced analytics and manual investigation. The integration of AI technology further enables attackers to make malicious traffic blend in with legitimate traffic, making these threats even costlier and harder to contain. (This is in contrast to the massive bandwidth costs triggered by Layers 3 and 4 attacks due to their sheer volume, causing broad and immediate network blackouts.) So, regardless of the type of DDoS attack, businesses face rising costs, underscoring the need to tailor defenses and budgets to the specific threats that are targeting their operations.

Security spotlight

The impact of DDoS on the software and SaaS industry

Our data indicates that DDoS attack complexity and scale continue to rise across industries. Notably, software and software as a service (SaaS) has emerged as one of the top five most targeted industries worldwide for both Layer 7 and Layers 3 and 4 attacks (Table 5).

Industries Most Targeted by Layer 7 Attacks and Layers 3 and 4 Attack Events

Layer 7 Attacks	Layers 3 and 4 Attack Events
1. Media	1. Financial services
2. Commerce	2. Games
3. Games	3. Manufacturing
4. Software and SaaS	4. Software and SaaS
5. Telecom ISP and MNO	5. Commerce

Table 5: Software and SaaS is one of the top five most targeted industries worldwide for both Layer 7 and Layers 3 and 4 attacks

This marks a significant shift in the traditional ranking of DDoS targets, highlighting the expanding threat landscape faced by software and SaaS providers. We'll now take a closer look at what's driving this shift and how it is reshaping the industry's exposure to DDoS threats.

The backbone of business operations: Software and SaaS

The software and SaaS industry's attack surface continues to expand due to a rise in the use of cloud-based models, the immense value of the data these platforms manage, and the critical role these platforms play in business continuity. Software and SaaS companies are no longer just service providers but are integral operational hubs, the backbone of modern enterprises that supports critical sales, IT, and business functions. Because customers and partners rely on their continuous uptime, even brief service disruptions can cascade across entire ecosystems, halting operations and generating significant financial losses.

This high dependency and interconnectedness make SaaS environments prime DDoS targets for attackers seeking to cause widespread operational chaos, extort ransom payments, or damage reputations. Not to mention, the concentration of high-value information held by SaaS providers leads to enhanced impacts and profitability for cybercriminals.

It's critical to understand that DDoS attacks often create direct interindustry impact. An example is the financial services industry that is highly targeted by volumetric DDoS. Many SaaS companies serve financial institutions, so attacks on banks may directly disrupt SaaS availability and cause customer portals, APIs, and web apps to go offline. Hence, a successful attack doesn't just affect one company, it can disrupt thousands of downstream clients simultaneously, amplifying issues and attention. It's why leaders across the organization (e.g., CISOs, IT directors, and business continuity officers) view DDoS resilience as a top priority for SaaS security. Anecdotally, many discover the depth of their operational dependency only after a prolonged outage, reinforcing how essential proactive DDoS protection and mitigation truly are.

The role of massive botnets in enabling accessible DDoSaaS

DDoS as a service (DDoSaaS) attack traffic is generated by a botnet, but instead of remaining a private asset used solely by a single attacker, that botnet power is commercialized and rented out to others. A technically skilled actor builds or rents a large botnet and then creates a web platform that advertises various DDoS packages (e.g., different attack durations, bandwidth levels, and attack types) for fixed prices, usually paid in cryptocurrency to preserve anonymity. Customers simply select a plan with a specific DDoS attack type and length, provide the target's IP address or domain, complete the payment, and the service automatically initiates the botnet-driven attack against the specified target within minutes.

The malware known as Mirai is a prominent example of a massive IoT-driven DDoS botnet that has strongly influenced and enabled DDoS-for-hire and DDoSaaS operations. Domingo Ponce, Senior Director of Security Operations at Akamai, said with regard to Mirai, "It's surprising that after all these years, [the botnet is] still out there and attackers are still finding new flavors of using that botnet." It has infected hundreds of thousands of IoT devices (e.g., IP cameras, DVRs, and home routers) and coordinated them to launch some of the largest recorded DDoS attacks.

After Mirai's source code was publicly released, numerous variants and copycat botnets emerged, with some explicitly run as commercial DDoS services. Aisuru is a prime example of a massive botnet powering DDoS attacks; it's classified as a "TurboMirai" variant, an advanced evolution of Mirai. Also, the DDoS botnet known as Kimwolf is part of the TurboMirai/Aisuru family lineage, an Aisuru successor, reusing Mirai-style DDoS structures while primarily targeting Android TVs via proxy networks. Both Aisuru and Kimwolf have been infecting millions of IoT and Android devices and causing record flooding. These variants exemplify Mirai as both a massive DDoS botnet and a model for accessible DDoSaaS.

The Akamai Security Intelligence and Response Team (SIRT) continues to uncover new Mirai variants and campaigns. In June 2025, Akamai reported on two Mirai botnets that are exploiting a remote code execution vulnerability in Wazuh servers. The blog post describes how unsanitized JSON in API requests allowed attackers to run arbitrary commands, compromise exposed servers, and enroll them into DDoS-capable botnets that receive instructions from remote command and control infrastructure to launch DDoS attacks or scan for new vulnerable systems. One of these campaigns, dubbed "Resbot," used Italian-themed domains, suggesting a possible regional focus. Although the post does not directly illustrate the role of massive botnets in enabling accessible DDoSaaS, it provides insight into how attackers rapidly adapt proven botnet architectures (Mirai) to exploit new vulnerabilities (which may then be used for DDoSaaS attacks). The attackers grow their botnets beyond IoT devices to include servers like Wazuh and use the resulting scale for DDoS attacks.

Mirai-compromised IoT devices remain a concern, with Mirai-based attacks continuing to evolve into more advanced super botnets, like TurboMirai, that amplify their scale and sophistication. These super botnets represent the direct lineage of Mirai. They build on its open source code to create larger, more resilient networks for devastating DDoS campaigns, often enhanced by AI-driven automation. AI technology boosts these threats by powering automated vulnerability discovery, generating polymorphic malware variants to evade detection, and optimizing attack strategies like traffic amplification for more efficient DDoS campaigns.

While DDoSaaS is frequently used for booting competitors offline or as a smoke screen (i.e., a diversion while another intrusion or data theft occurs), it is also commonly used for extortion. Ransomware DDoS (RDDoS) attacks are conducted by ransomware groups to demand payment for preventing or stopping service-disrupting DDoS attacks. RDDoS, frequently powered by DDoSaaS botnets, is a persistent threat, often serving as a stand-alone extortion tactic or layered with ransomware techniques like triple or quadruple extortion to amplify pressure on victims. In the case of triple extortion, DDoS is paired with other ransomware (e.g., encryption, data theft) to further persuade victims to pay; quadruple extortion tags on third-party harassment, as well (Figure 5).

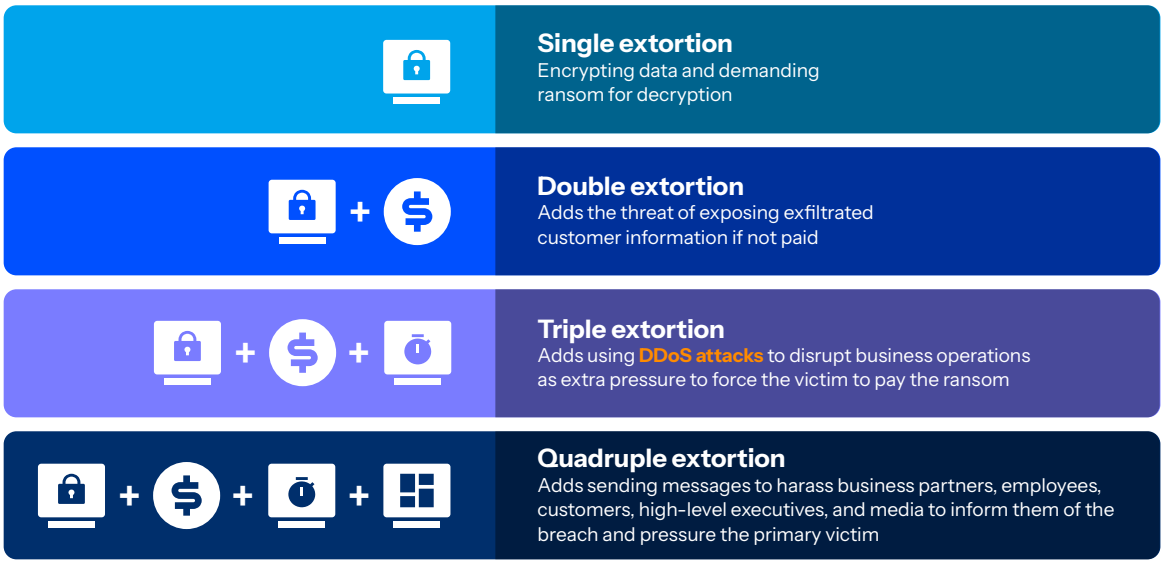

Fig. 5: Ransomware groups leverage escalating ransomware extortion tactics to coerce payments from victims

Additionally, ransomware as a service (RaaS) groups with DDoS capabilities are also trending. For example, Qilin, also known as Agenda, is a Russia-linked RaaS group first observed in 2022 that has more recently enhanced its extortion toolkit to reportedly incorporate DDoS attack capabilities. In Q2 2025, when many RansomHub affiliates joined Qilin after RansomHub's collapse, Qilin surged to become the top ransomware threat targeting the United States.

DDoS and hacktivists

Today's DDoS threat actors represent a wide spectrum of motivations — from financial gain and competitive disruption to political or ideological agendas. We've explored the various incentives behind these malicious attacks, and hacktivism stands out as one of the most volatile and unpredictable forces shaping the modern DDoS landscape. Hacktivist operations are mostly fueled by ideology, national allegiance, or social causes, often in response to real-world geopolitical events. This politically charged environment has given rise to aggressive groups like NoName057(16), DieNet, and CARR that conduct large-scale disruption campaigns that continue to blur the line between activism and cyber warfare.

Hacktivist-driven DDoS activity continues to surge, which reflects that politically motivated threat actors are adapting to shifting global tensions. As instability intensifies across regions like Europe and Venezuela, a potential resurgence of grassroots hacktivism is emerging, with decentralized groups rallying around social and political causes. At the same time, the boundary between cybercriminals and hacktivists is becoming increasingly blurred, as both groups exploit shared infrastructure and high-capacity botnets to spread narratives, extract data, and disrupt critical services.

Europe has remained a primary focal point of DDoS-related hacktivist claims, while Israel, the United States, and Ukraine were also top targets in H1 2025. Among these hacktivist groups, NoName057(16) has been sustaining its dominance, and continuing its established pattern of high-frequency attacks intended to generate media attention rather than permanent disruption. We expect to see the trend of geopolitical events tied to state-sponsored hacker groups continue. This will cause collateral damage to critical infrastructure in the countries involved and the countries believed to be supporting one side of these events.

Hacktivist groups have become more well-resourced and have been displaying notable technical escalation and persistence. The past notion that DDoS attacks pose little threat is outdated, and, in recent years, hacktivist groups have been taking advantage of the dramatically evolved DDoS landscape. These campaigns have intensified alongside growing efforts to erode trust and destabilize governments amid geopolitical conflicts. Collectively, such hacktivist DDoS attacks, easily enabled by accessible rentable botnets, demonstrate an ongoing convergence between ideological motives and professionalized DDoSaaS operations.

Best practices for prioritization, testing, and validation exercises

With DDoSaaS making sophisticated, large-scale attacks accessible to virtually anyone, organizations must ensure that their defenses are robust, well-coordinated, and rigorously tested. Effective protection requires alignment across internal teams, service providers, and vendors, along with a multilayered security strategy capable of mitigating diverse attack vectors.

Three key process areas to prioritize

1. Stakeholder alignment — Internally, ensure that teams (security operations center, IT, incident response, crisis management) collaborate seamlessly to detect and mitigate threats. Externally, confirm that vendor SLAs define clear escalation paths for rapid response.
2. Incident preparedness — Establish a well-defined playbook, eliminating ambiguity during an attack. This playbook should include:
    - Designated decision-makers and contacts at every level (with up-to-date contact lists)
    - Step-by-step response protocols for varying attack scenarios

3. Multilayered defense — Protect against all potential vectors:
    - Infrastructure security (Layers 3 and 4)
        i. Ensure that the company is keeping its attack surface small by pushing as much of the Layer 4 rules to the DDoS provider as possible
        ii. Have a proven strategy for the ports and protocols that must be open to the internet
            - Ensure that DNS is resilient by using a cloud provider or multiple cloud providers
    - Application layer (Layer 7)
        i. The organization's critical host names should all be resolving to a CDN with a web application and API protection (WAAP) solution that is able to mitigate millions of requests per second without leaking traffic to the origin
    - DNS
        i. Implement Domain Name System Security Extensions (DNSSEC)
        ii. Implement DNS posture management, firewall, and filtering

Testing and validation

- Regularly test playbooks (at least biannually) to ensure relevance and effectiveness.
- Conduct DDoS simulations to validate defenses under realistic conditions and confirm that the mitigation strategies perform as expected.
- Stress-test internal systems to handle zero-day attacks that might slip through the DDoS provider.

A proactive, regularly tested approach ensures resilience when it matters most, before systems are compromised and downtime escalates into a crisis.

When DNS becomes a business risk

Throughout 2025, customers consistently shared that DNS was where risk quietly accumulated. Across industries, security teams described DNS as the layer most likely to outlive infrastructure, vendors, and even entire business units. Cloud migration, SaaS adoption, developer self-service, and third-party integrations all increased the rate at which DNS records were created, modified, and abandoned. What customers needed was not better alerting, but more clarity. They wanted to understand what their internet-facing identity actually looked like at any given moment, and whether it still reflected reality.

Validation with research from Akamai DNS Posture Management began to surface disproportionate insights. At enterprise scale, basic DNS misconfigurations — such as dangling CNAME records, leaked internal network data, and disabled registry locks — remain widespread, leaving thousands of domains vulnerable to takeover and hijacking. In regulated sectors such as financial services, more than 85% of observed domains failed foundational DNS controls, including Start of Authority integrity, Certificate Authority Authorization enforcement, or DNSSEC, while nearly half lacked modern email authentication. Customers were often surprised by these findings, not because the issues were unknown in theory, but because they persisted unnoticed despite otherwise mature security programs. Several organizations' security teams used familiar operational shorthand and said, "It's not DNS. It can't be DNS. [Expletive], it was DNS." Our research did not reveal a new class of failure. It revealed how often unresolved DNS drift quietly underpinned incidents discovered elsewhere.

These patterns became most visible during periods of organizational change. Mergers and acquisitions repeatedly acted as a forcing function for DNS risk discovery. During integration efforts, customers uncovered large volumes of orphaned DNS records tied to decommissioned cloud instances, retired CDNs, legacy marketing platforms, and former vendors. DNS entries remained resolvable long after the underlying assets were gone, creating real exposure to subdomain takeover, impersonation, and unauthorized certificate issuance. What made these findings actionable was context. DNS Posture Management showed that these were not isolated misconfigurations, but structural artifacts of how enterprises evolve faster than their ownership and decommissioning processes.

Outside of mergers and acquisitions, customers described similar failure modes during ongoing modernization. Cloud re-architectures left behind stale CNAMEs. Email migrations broke SPF, DKIM, or DMARC alignment long after projects were considered complete. Business units created domains for campaigns that were never retired. Vendor relationships ended, but DNS trust persisted. Over time, teams began to treat DNS posture as a proxy for organizational discipline. When DNS drifted, it often signaled broader breakdowns in ownership, accountability, and change control.

Customers also pointed to certificates and cryptographic posture as an emerging DNS-adjacent risk area. While HTTPS adoption is widespread, fewer than 4% of the live enterprise domains we observed were quantum safe, leaving the vast majority exposed to future cryptographic breakage. More immediately, certificate risk was driven by scale rather than rare failure. Nearly 40% of the certificates we observed were already expired or would expire within 90 days, and trust was increasingly concentrated among a small number of certificate authorities.

As certificate lifetimes continue to shrink toward sub–50-day validity windows, customers recognized that certificate management is no longer a periodic hygiene task. It is a continuous availability and security requirement. What elevated DNS posture from a technical concern to a business issue was not the presence of misconfiguration, but its impact. DNS failures surface as outages, email delivery breakdowns, impersonation, or loss of customer trust. By the time they are visible, the cost is already being absorbed by the business.

To move from insight to action, many customers asked for a practical reference model for DNS resilience and security. Unlike web applications, DNS has historically lacked a widely adopted operational checklist, despite its being foundational infrastructure. In response, security teams increasingly aligned around a set of core controls that consistently reduced DNS-driven risk across environments, providers, and acquisitions. These practices form an emerging DNS posture management top 10 for operational resilience.

DNS posture management top 10 list 2026

Uptime and basic hygiene

1. Use distributed, cloud-hosted DNS services designed to withstand DDoS and regional failure.
2. Segregate internal and external DNS environments and routinely remove expired or unused records.
3. Keep DNS infrastructure independent from application and website hosting to prevent cascading failures.
4. Enforce strong access control through role-based access control, multi-factor authentication, audit logging, change management, and DNSSEC.
5. Manage time to live values deliberately to balance caching efficiency with rapid recovery and failover.

Posture management and compliance

6. Automate discovery of DNS assets across all clouds and providers to maintain a complete inventory.
7. Continuously analyze configurations to detect drift, misconfigurations, and ownership gaps.
8. Proactively manage certificates by monitoring expiration, vulnerabilities, and lifecycle compliance.

Emerging risk and future readiness

9. Monitor for DNS-based threats such as typosquatting, look-alike domains, and brand impersonation.
10. Prepare for post-quantum cryptographic transition through crypto agility and standards-aligned planning.

Customers emphasized that the value of this list is not theoretical alignment, but operational leverage. It gives security, infrastructure, and compliance teams a shared language for DNS risk and a concrete way to embed posture checks into cloud migration, vendor off-boarding, and merger and acquisition workflows. This allows leadership to provide an integrated view of the cyber risk for DNS infrastructure.

Web application attacks

The API and web application attack data in this section comes from Akamai App & API Protector, which focuses primarily on web attacks.

Web attack volume was up by 73% from the beginning of 2023 through the end of 2025. The sustained growth trend in web attack volume is a testament to unrelenting these attacks have become, as adversaries continuously probe enterprise environments, from customer-facing websites to back-end APIs, for exploitable security gaps that can lead to full-scale breaches (Figure 6). For the defenders, this means facing emerging threats while contending with the compounding risks of legacy infrastructures, delayed patching, and overlooked misconfigurations that expand the attack surface.

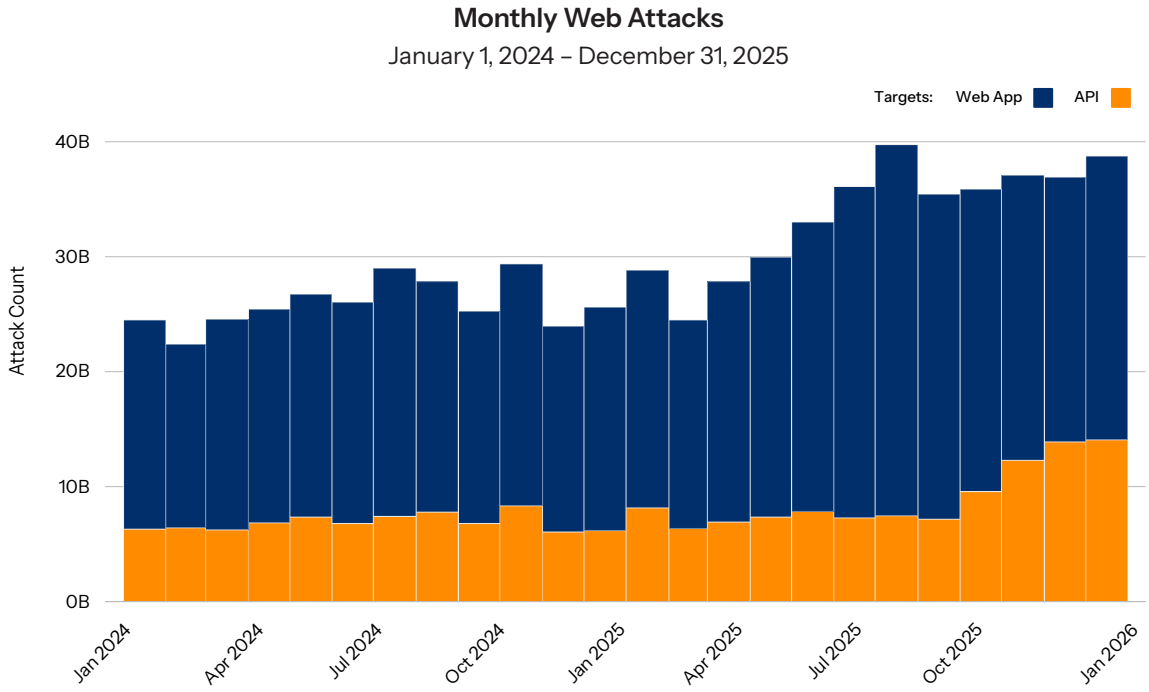

Fig. 6: The number of web attacks against apps and APIs continued an upward trajectory from January 2024 to December 2025, demonstrating their prevalence as a major threat to organizations

The fallout from web application attacks more often appears in subtle ways than through obvious, full-blown incidents, as evidenced by the declining conversions, alert fatigue, and reduced performance that are seen well before a compromise is detected. Over time, these underlying effects diminish customer trust and raise operational costs, even without a large-scale breach.

At its core, web applications and APIs remain prime targets because of the valuable data they expose and their central role in digital business operations. Moreover, web attacks continue to be a proven and widely used tactic for threat actors seeking an initial foothold in enterprise environments.

Updated OWASP Top 10 highlights the importance of security basics

In Q4 2025, OWASP published the OWASP Top 10:2025, its latest ranking of the most critical web application security risks (Figure 7). For this installment, OWASP ranked categories based on the data, and allowed two categories to be promoted or highlighted by responses from the community survey. The update underscores a major shift in the threat landscape: the growing danger of software supply chain attacks.

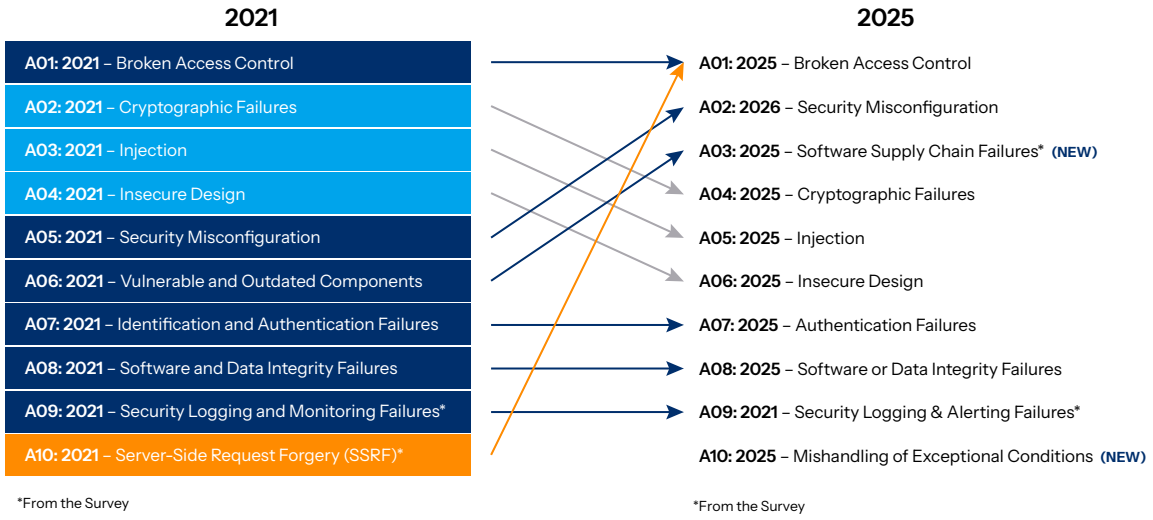

Fig. 7: The updated list of OWASP web application security risks includes a new category on the dangers of supply chain attacks

At the center of this update is A03:2025 — Software Supply Chain Failures, a redefined category that replaces A06:2021 — Vulnerable and Outdated Components. The change signals a recognition that modern attacks extend far beyond the traditional network perimeter; threats increasingly arise from interconnected vendor ecosystems, reliance on third-party services, and the widespread use of open source components. With the highest average exploitability and potential impact among all categories, supply chain failures now represent one of the most consequential risks facing organizations. In our Year in Review 2025 blog post, Akamai experts spotlighted how critical third-party risks will be in 2026.

Additionally, high-profile incidents highlight the urgency of this shift — from the 2019 SolarWinds compromise and the 2021 Log4Shell exploitation to more recent cases like the one dubbed React2Shell. This critical vulnerability in React Server Components and Next.js can lead to remote code execution through unsecure deserialization in Flight requests. Given the widespread use of these frameworks, a significant number of websites may be affected. Each of these incidents underscores how gaps in deeply embedded third-party dependencies can potentially become attack vectors.

A01:2025 — Broken Access Control retains its top spot on the list, now encompassing Server-Side Request Forgery (as indicated by the orange line in Figure 7). A02:2025 — Security Misconfiguration moves up to second place, emphasizing the continued significance of configuration hygiene in maintaining a secure posture. Although Injection has dropped from third place to fifth place, injection attacks remain a pervasive and exploitable weakness, particularly in legacy and unpatched systems. Our data shows that from 2024 through 2025, SQLi and command injection (CMDi) together accounted for 15% of web application attacks (Figure 8).

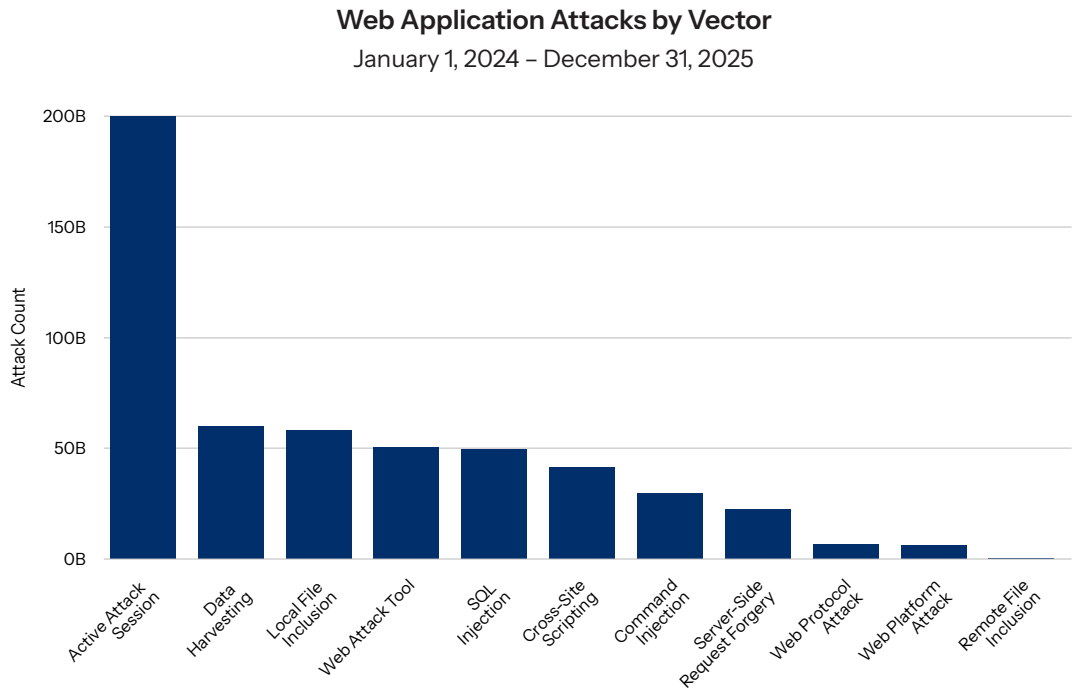

Fig. 8: Tried-and-true methods like SQLi and CMDi continue to have a significant impact on organizations

Overall, the OWASP Top 10:2025 reinforces a familiar truth: Security fundamentals remain essential. Whether tightening third-party governance (for Software Supply Chain Failures), enforcing least-privilege access (for Broken Access Control), or addressing design flaws early in development (for Insecure Design), the basics continue to matter and to define resilience in application security.

Regional trends

The API and web application attack data in this section comes from Akamai App & API Protector, which focuses primarily on web attacks.

Organizations face markedly different cybercrime challenges depending on their geographic location, with regional factors shaping both threat types and security priorities. In the following two regional trends sections — the snapshots from Asia-Pacific (APAC) and Europe, the Middle East, and Africa (EMEA) — our subject matter experts share their perspectives on the attack types and trends that are top of mind for CISOs in their respective regions. Within this context, we also provide data and insights from Akamai researchers on web and DDoS attacks during the reporting period from January 1, 2024, through December 31, 2025.

APAC snapshot

Expert insight

How AI, APIs, and digitization are reshaping web and DDoS attacks

In 2025, CISOs faced a nuanced set of security challenges due to the economic and operational realities in the APAC region. Insights into key web and DDoS attack trends in this region during that year show that despite technical maturity, we're still dealing with some very basic security problems.

Web attacks are being amplified

For a complete picture of why web attacks continued to grow in APAC, CISOs should view web applications and APIs through a single lens, as they have become inseparable. Many CISOs tell me that this broadening development ecosystem has created some fundamental challenges, including:

- **Shadow APIs**
- **Vibe coding**
- **Regional disparity in cybersecurity skills**

Shadow APIs. According to the Postman 2025 State of the API report, APAC regularly churns out more APIs than any other region. Shadow APIs (i.e., APIs that are unknown and undocumented) are a natural consequence and a massive issue for organizations. Development teams are stretched thin in terms of building and rolling out APIs for production. Oversight and accountability are often lacking — from testing to documentation and implementation — which can lead to shadow APIs. Security and IT teams struggle to work with compliance teams to ensure they have an accurate inventory of APIs and adequate security controls.

Vibe coding. In the rush to digitize their economies and build apps and APIs faster, teams are adopting "vibe coding," a method of software development that uses AI to help accelerate in-house development. CISOs value the enhanced productivity AI-assisted coding can bring to the table. However, vibe coding isn't failproof and can blindside organizations with vulnerabilities and misconfigurations. As with APIs, these vibe-coded apps often go into production without sufficient testing to pinpoint risks. CISOs concerned about zero-days must continuously try to figure out the best way to mitigate these attacks in 2026.

Regional disparity in cybersecurity skills. Another challenge for defenders, which is particularly pronounced in APAC, is the disparity in cybersecurity skills among different economies. Highly digitized economies have more mature skill sets to secure investments in the latest technologies more effectively; cybersecurity skills of developing economies are still quite scarce. Less skilled teams that are trying to grow and digitize operations very quickly tend to roll out APIs and AI elements without the benefit of security maturity. The mismatch exacerbates risk. Given the pace of innovation, the gap will likely widen.

From an attacker's perspective, for every web application there are APIs that expose functions and (potentially) data. The more vulnerable and easier the apps and APIs are to compromise, the quicker the threat actors can reach their objectives.

The rise of AI agents that consume APIs to interact with the real world amplifies the problem. Whether booking a flight, getting a ride, or transferring money, organizations need controls that help discern who is interacting with APIs and why. Although the crown jewels are typically secured in the back-end workload, they risk being directly exposed via vulnerable APIs. When viewed through this lens, it's clear why web attacks continue to escalate.

DDoS attacks remain prominent

Whether targeting Layer 7 or Layers 3 and 4, DDoS attacks remain a weapon of choice for threat actors targeting the APAC region for the following two reasons:

1. **Multiple geopolitical hot spots.** APAC is a region with multiple geopolitical hot spots. During times of geopolitical upheaval, we see massive spikes of DDoS attacks meant to disrupt critical infrastructure, take highly visible services offline, and damage the economy of targeted areas. Adding to the fray, hacktivists are increasingly playing an active role in the cyberthreat landscape to promote politically motivated agendas. Botnets for hire and other tools as a service make it easy and inexpensive for groups with less technical knowledge to launch a DDoS attack.

2. **Digitization.** The digitized states of certain mature economies in APAC make them enticing targets since they are dependent on ensuring that services like finance, commerce, healthcare, and public sector services are online and available. As developing economies accelerate digital transformation, they too become targets and need to factor DDoS protection into their controls. Always-on services need always-on protection. However, many organizations have not taken a proactive stance to mitigate risk, opting instead to turn on protection while a DDoS attack is in progress. Others add a baseline DDoS mitigation subscription from an ISP or a cloud hyperscaler, which may not be sufficient when dealing with massive multi-vector attacks. The average ISP is just not prepared to address the increasing complexity and scale of these modern AI-powered DDoS attacks.

Nuanced challenges across the region make it impossible to find a consistent way to protect all things everywhere. Organizations need an approach that protects their investments, aligns with their operational and economic reality, and still enables growth.

Reuben Koh
Director of Security Technology, APJ

APAC data and trends

As the web attack surface expanded with the growing reliance on APIs and AI in the APAC region, web attack attempts continued to rise. Akamai researchers observed nearly 65 billion web application and API attacks in APAC in 2025, representing a 23% year-over-year increase (Figure 9).

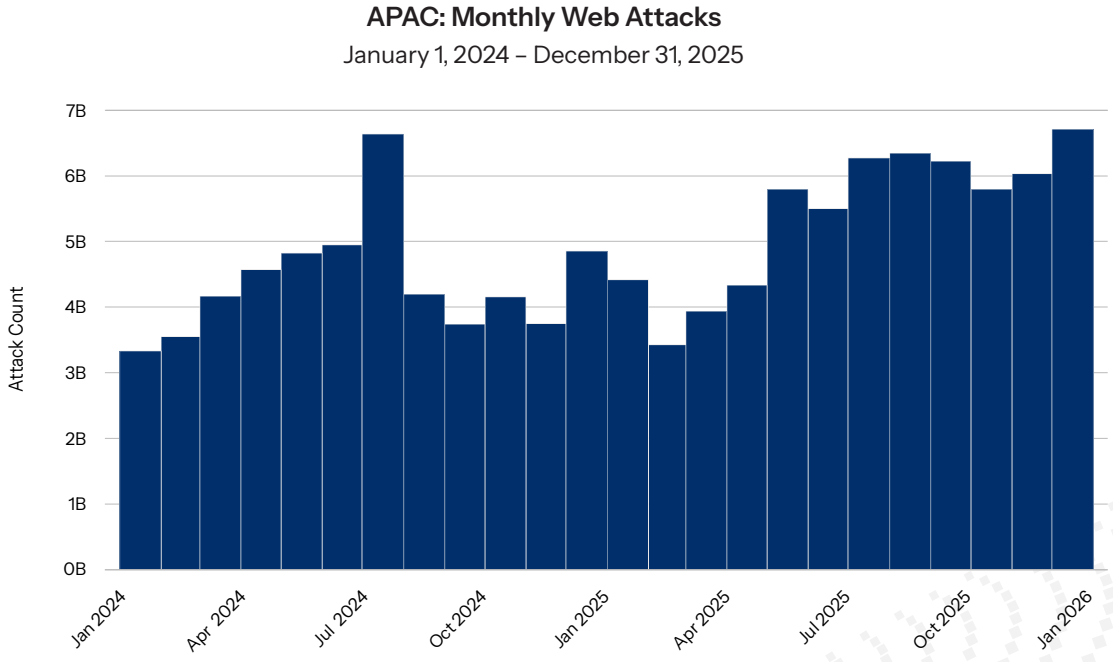

Fig. 9: Web attacks in APAC became a more consistent threat in 2025, averaging 5.4 billion per month vs 4.4 billion per month in 2024

The combination of ongoing digitization in the region and the challenges in securing the digital ecosystem contributed to making APAC an attractive target for web attacks. Attacks are also coming faster, fueled by AI-assisted tools. To manage the risks that shadow APIs and AI-assisted coding introduce, organizations should prioritize tools and processes to help discover, test, and protect APIs throughout their lifecycle. The aim is to ramp up operational resilience, not just prevent breaches.

In light of the tense geopolitical atmosphere in APAC and the intensifying ideological unrest, DDoS attacks also remain a persistent concern as they are routinely weaponized to disrupt critical and highly visible services.

As automation, AI, and DDoSaaS increased accessibility to attack tools, threat actors targeted organizations across the region with Layer 7 DDoS attacks in 2024 and 2025 (Figure 10).

APAC: Layer 7 DDoS Attacks by Target Area

January 1, 2024 – December 31, 2025

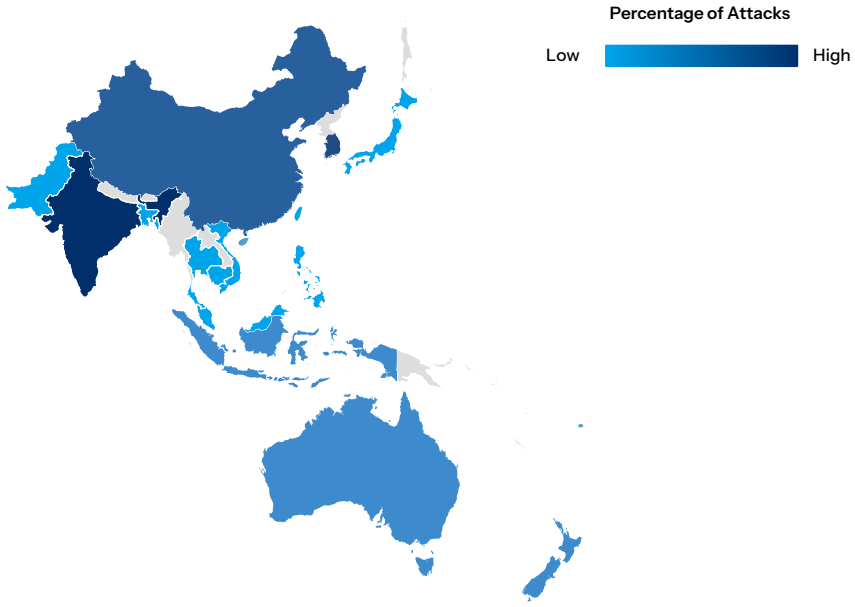

Fig. 10: Layer 7 DDoS attacks were geographically widespread in APAC

Additionally, the use of multiple vectors and massive botnets as a service have made it easier to launch larger, longer Layers 3 and 4 DDoS attacks (Figure 11).

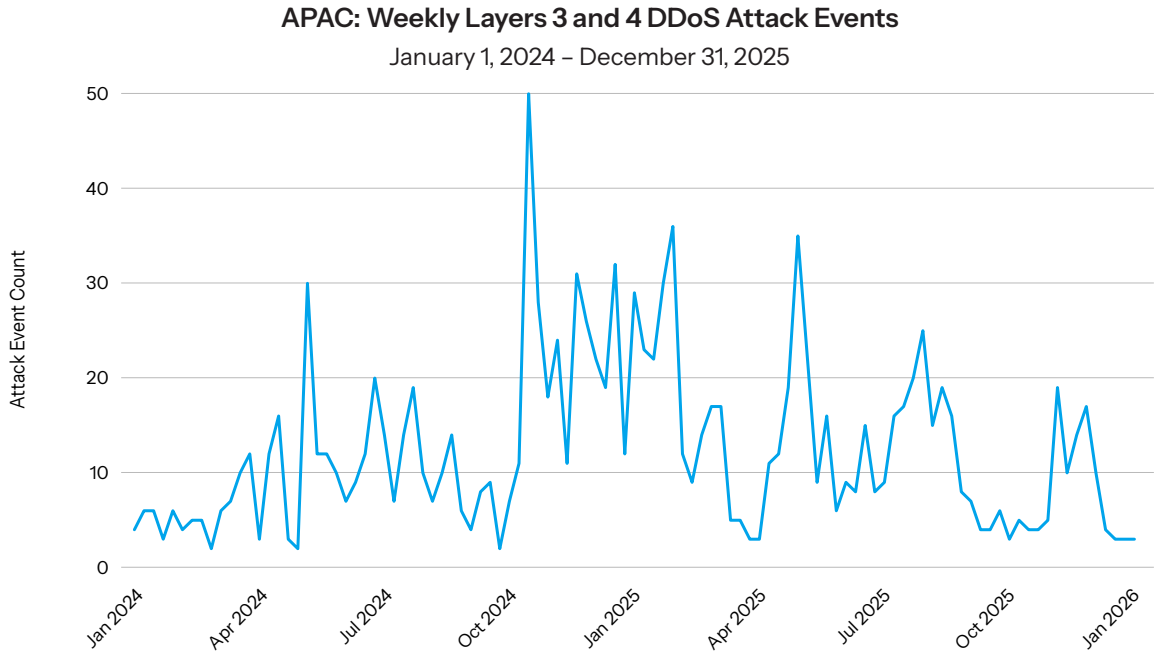

Fig. 11: Volumetric Layer 3 and 4 DDoS attacks became more prevalent in APAC and often coincided with heightened military exercises, geopolitical tensions, and border conflicts

EMEA snapshot

Expert insight

As attacks rise, CISOs prioritize resilience

Security leaders expect web application, API, and DDoS attacks fueled by geopolitical tensions, hacktivism, and the pursuit of financial gain to increase year after year. In EMEA, 2025 was no exception. So, conversations with CISOs didn't focus on numbers or attribution. Instead, they focused on resilience.

How to mitigate the impact of these cyberattacks on the supply chain and how to navigate regulatory compliance to build operational resilience were the top stories in EMEA.

The existential threat to supply chains

According to the World Economic Forum's Global Cybersecurity Outlook 2025, 54% of the large organizations surveyed identified supply chain challenges, including their increasing complexity, as the biggest barrier to achieving cyber resilience. Notable attacks against major retailers and some large manufacturers in EMEA brought to light the very real potential for an existential crisis for supply chains. CISOs are asking themselves:

- How comprehensive is our resiliency plan?
- Can we continue to meet the needs of our employees, suppliers, and customers in the event of a massive attack that brings down operations and lingers for months?
- Do we have a pen-and-paper plan, as recommended by the United Kingdom's National Cyber-Security Centre (NCSC), to maintain operations when digital systems go down?

Large enterprises, owned by a massive conglomerate, can absorb the financial impact of a significant attack. But the supply chain impact is a different story and "winging it" isn't a strategy, particularly if the company relies on hundreds of small suppliers that are critical to the organization's ability to deliver. If those suppliers go under because the organization has no way to pay them and no way to keep the supply chain moving via a manual plan, the organization will have an existential crisis on its hands. When remediation extends from days to weeks to months, there may be no one to support the company once its systems are restored.

Companies that have to rebuild their supply chain may never reach "business as usual" as it was.

With financial viability on the line for themselves and their partners, companies are focused on how to mitigate supply chain risk by protecting systems with proven security controls and maintaining integrity through comprehensive resiliency plans.

EMEA's complex and evolving regulatory environment

Regulatory bodies in the United Kingdom and the European Union (EU) are known for being at the forefront of cybersecurity regulation and they continue to beat the drum for operational resiliency.

The Network and Information Security (NIS2) Directive emphasizes operational resilience by requiring organizations to implement comprehensive cybersecurity measures and risk management practices designed to protect systems and data from cyberthreats. Compliance has become increasingly urgent as the adoption of APIs and AI-driven SaaS tools has broadened the attack surface for organizations, and as DDoS attacks have continued to grow. Although NIS2 was due to be transposed into national law across the EU by October 2024, implementation has proven challenging for several Member States, and transposition efforts are still ongoing.

The Digital Operational Resilience Act (DORA) focuses on cybersecurity resilience specifically within the financial sector. As a regulatory framework, it has been relatively easier to adopt than NIS2, despite a large amount of effort by affected organizations, and has been applicable across the EU as of January 17, 2025.

Other regulations that organizations in EMEA are planning to comply with include:

- **The Cyber Security and Resilience Bill.** Introduced on November 12, 2025, the Cyber Security and Resilience Bill is currently progressing through the UK Parliament and will review the existing NIS regulations to focus on the resilience of the essential services people rely on every day (e.g., data centers, critical ICT suppliers, and food supply chains) and greater economic stability.
- **The EU AI Act.** Recognizing that AI will stoke the rise in cyberattacks, but is also valuable for defenders, the EU AI Act introduces a compliance framework to secure AI-enabled systems. For example, social engineering is being used to compromise AI chatbots, not only human service agents. Security teams must deploy compliant controls to properly lockdown systems.
- **The Cyber Resilience Act.** The Cyber Resilience Act (CRA) aims to strengthen the resilience of IoT devices. This includes addressing security weaknesses in these devices, such as the hardcoded passwords that the Mirai botnet and its derivatives discover and exploit to launch DDoS attacks.

In the face of rising attacks that grow more disruptive, security leaders in EMEA are focused on readiness — proving that resilience is the foundation for continuity and confidence.

Richard Meeus
Senior Director of Security Technology & Strategy, EMEA

EMEA data and trends

Akamai research shows that web attacks remained an ongoing threat in EMEA between January 1, 2024, and December 31, 2025, culminating in a sustained two-year high in Q4 2025 and reinforcing the need to prioritize resilience (Figure 12).

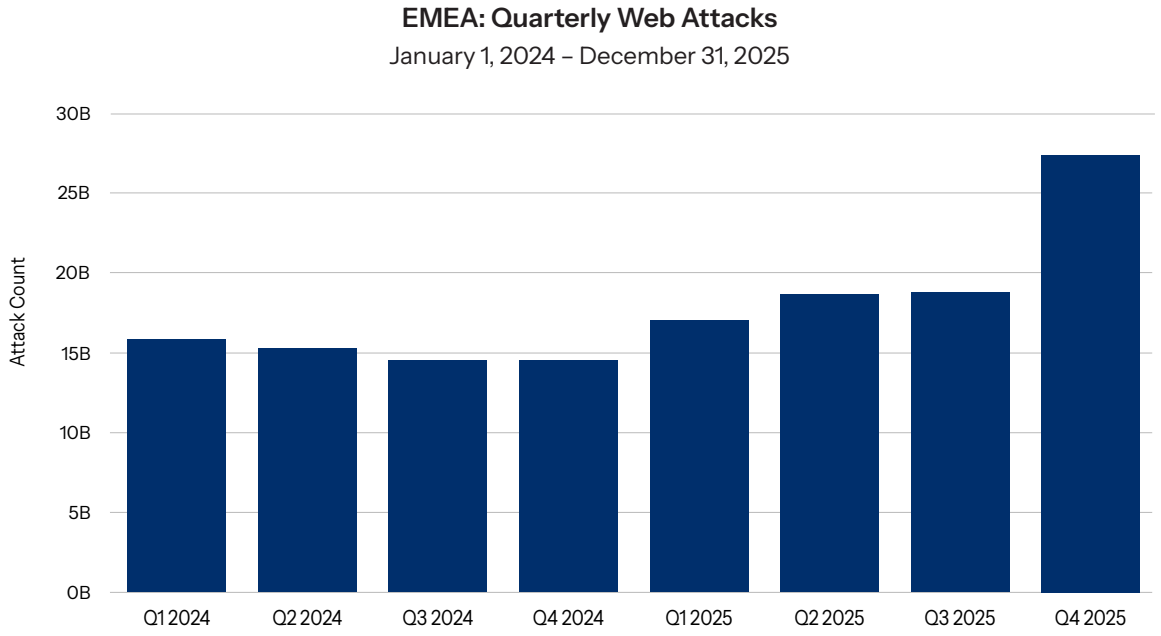

Fig. 12: Web attack attempts continued to rise in EMEA, with Q4 2025 averaging 69% more attacks than each of the prior seven quarters, and translating to 36% year-over-year growth

We can attribute this growth, in part, to a focus on attacks against organizations that are increasingly dependent on complex, hard-to-secure supply chains. For example, retailers were among the top targets for web attacks in the region during 2025 (15.5 billion attacks), joined by manufacturers who experienced 12 billion web attack attempts in 2025, a 30% year-over-year increase. The disruption is not only immediate but long-lasting as recovery requires coordinated effort across organizations of various security capabilities and resources.

DDoS attacks also continued to rise in EMEA. Akamai research shows EMEA was the most targeted region for Layers 3 and 4 DDoS attacks over the last two years (4,750 attacks). Additionally, the traffic patterns are consistent with adversary behavior observed by our Security Operations Command Centers. Diligent attackers continue to come after a target with high-powered infrastructure to launch very large attacks (Figure 13).

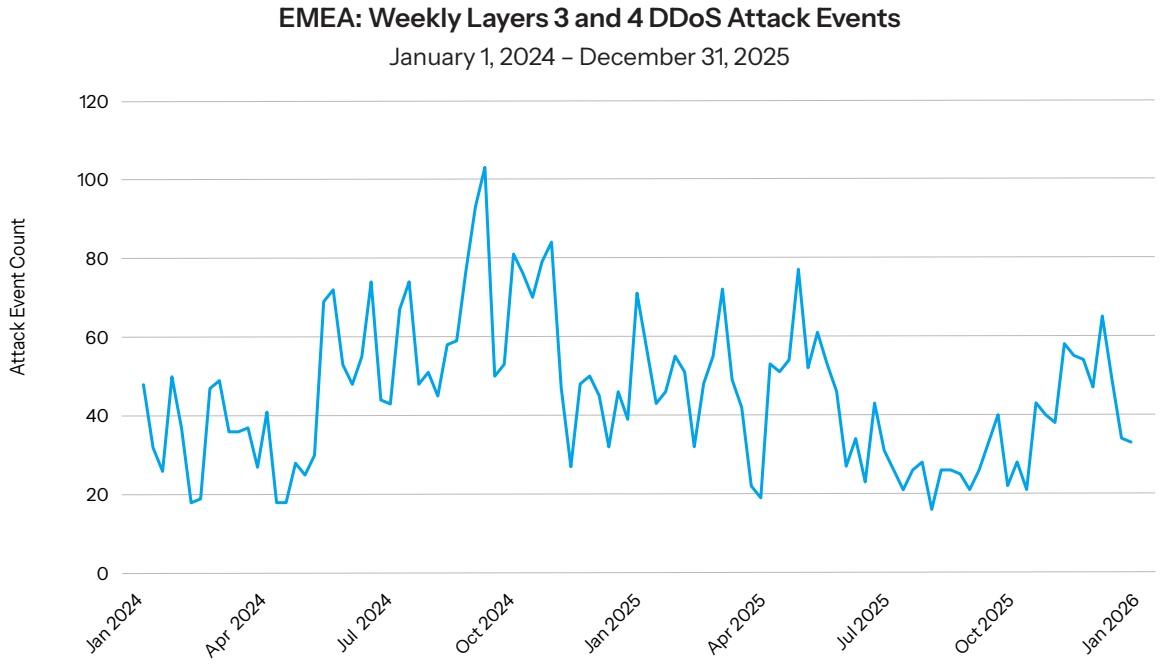

Fig. 13: EMEA has been persistently targeted by volumetric DDoS Layer 3 and 4 attacks, often correlating to geopolitical events and intensified efforts to combat cybercrime

The peaks and valleys reflect the typical intent of these attacks; that is, to cause substantial and immediate impact triggered by geopolitical circumstances and hacktivist agendas. Regulations such as DORA, NIS2, and CRA encourage measures that prevent the creation of such attacks and strengthen resilience against them.

Organizations also have to remain vigilant against Layer 7 DDoS attacks, which increased 37% year over year (Figure 14).

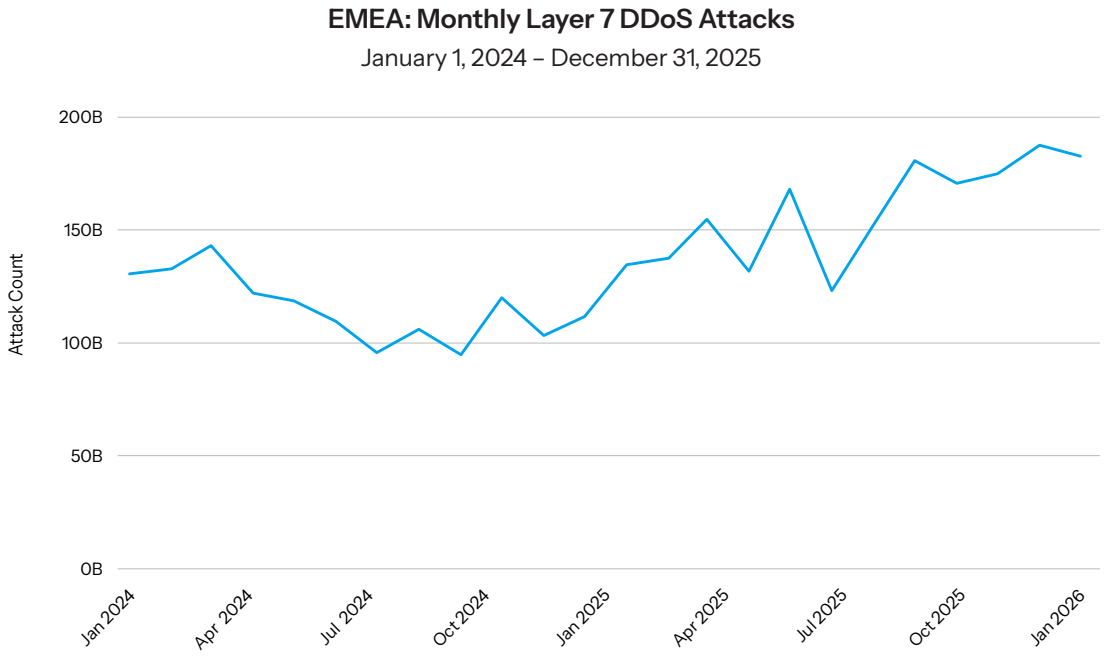

Fig. 14: Layer 7 DDoS attacks trended up in EMEA, reaching the highest volume (188 billion) in November 2025

The state of cybersecurity in Latin America

Akamai experts in Latin America identified three topics that conversations with regional security leaders have consistently centered on: the increasing threat of online fraud, the expanding attack surface, and the rising threat of hacktivism.

Top of mind: The increasing threat of online fraud, particularly from credential stuffing, dominates the conversation in Latin America. In addition to online fraud, cybersecurity professionals in the region have their hands full with the typical WAF and API attacks that surged 70% year over year.

Big takeaway: As in the other regions, the attack surface is exploding. APIs, mobile apps, partner integrations, and AI agents are creating new pathways to disruption, while AI-powered bots are turbocharging credential stuffing attacks. Yet the 80/20 rule still holds: Organizations achieve the biggest security gains by fixing foundational gaps such as visibility, access control, training, testing, validation, and patching.

Looking ahead: The increasing potential for political turbulence across the region lends itself to the rising threat of hacktivism. As tensions rise, so does the potential for DDoS attacks. Organizations that haven't prioritized a multilayer security strategy that includes DDoS monitoring and mitigation may soon find it moves from the back burner to the front burner — fast.

Mitigation strategies

This report has covered a lot of ground based on Akamai's full platform of capabilities, from which we are drawing data. Let's discuss how to use this information to better protect organizations.

- **At the highest level, the first capability an organization needs to stop DDoS, app and API attacks, and emerging AI threats is visibility.** Once an organization is confident that it has visibility of the environment, it must deploy an integrated platform of security controls that can be adjusted according to the risk tolerance of leadership. Finally, the organization must invest in the people and processes via training and validation exercises. Cybersecurity is a team event and it's critical to have a culture in which developers, IT, infosec, vendor management, and legal teams are all following the latest best practices and regulatory guidance.
- **Whether talking to the board or the infosec team, it is always key to use industry best practices.** OWASP is a great resource for prioritizing training, deploying security controls, driving red team and blue team pen testing, and analyzing vulnerability. The foundational OWASP Top 10 for web application security doesn't update often so it is worth reviewing regularly. Even more critical is OWASP's coverage of emerging trends like agentic AI, which gives organizations the opportunity to get ahead of the tech debt and build security into the development phase of deployment.
- **Finally, while many of the activities across the threatscape tend to change incrementally, it is important to use reports like this one to validate that the organization's controls are able to deal with the latest attacks.** This means aligning protections across DDoS mitigation, WAF, API security, bot and abuse prevention, and identity-aware controls, rather than treating them as isolated point solutions. Controls should be reviewed regularly to ensure that they reflect current threat behavior, not last year's assumptions.

These steps can enable security leaders to move from reactive control updates to proactive, data-driven resilience.

Conclusion

Today's evolving DDoS threatscape demonstrates that amplified automation, AI, and increasingly massive botnets are transforming traditional bandwidth busters into increasingly complex attacks. Over the past three years, the number of Layer 7 DDoS attacks has surged, largely driven by the accessibility of botnets via DDoS-for-hire campaigns and AI-enabled attack scripts that make targeting APIs and web applications faster and easier than ever. Meanwhile, volumetric DDoS attacks continue to achieve record-breaking scale and remain capable of rendering entire networks unreachable within seconds. Super botnets like Aisuru and Kimwolf, which evolved from Mirai's foundational architecture, sustain DDoSaaS ecosystems and enable both cybercriminal and hacktivist groups to rent high-powered infrastructures.

The expansion of DDoS attacks on the software and SaaS industry stems from cloud-based models, high-value data, and critical business reliance that make these platforms ideal targets for disruption, extortion, and reputational damage. The impacts extend beyond immediate downtime; customers and partners depend on continuous uptime, so brief disruptions can cascade across ecosystems, halting operations and creating significant financial losses. As attackers increasingly deploy automation, AI, and hybrid multilayer tactics, defenders must adopt adaptive, intelligence-driven protection strategies across Layers 3, 4, and 7 to remain resilient against evolving DDoS threats.

As attackers pivot to using APIs as their primary entry points, the convergence with AI threatens to transform these vulnerabilities into critical organizational risks. The use of GenAI in code creation (vibe coding) has inadvertently introduced more vulnerabilities through misconfigurations and unsecure default settings. More than ever, organizations need to embed security throughout the entire API lifecycle and prioritize protection before production. As we stated previously, API security shouldn't be treated as a stand-alone domain but as an integral part of the broader application ecosystem, in which a single weakness can ripple across interconnected systems.

Meanwhile, web application attacks continue their steady rise, aided by persistent lapses in cyber hygiene that leave many organizations vulnerable. OWASP's two latest lists — covering top application security risks and agentic AI vulnerabilities — highlight how third-party integrations are expanding the modern attack surface and amplifying the hazards of supply chain attacks.

These challenges aren't new, but they're intensifying the need for an organization to know whether it has the right tools for visibility and mitigation to be truly prepared.

Methodology

Web application and Layer 7 DDoS data

This data describes application-layer alerts on traffic seen through our App & API Protector. The web application attack alerts are triggered when Akamai detects a malicious payload within a request to a protected website, application, or API.

The Layer 7 DDoS alerts are triggered when we detect volumetric anomalies in the number of requests to a protected website, application, or API. These alerts can be triggered by both malicious and benign requests. Typically, the requests themselves are benign, but the high volume of requests indicates malicious intent. The alerts do not indicate the successfulness of an attack. Although these products allow for a high level of customization, the data analyzed here does not consider custom configurations of the protected properties.

The data was drawn from an internal tool for analysis of security events detected on Akamai Cloud, a network of approximately 340,000 servers in more than 4,000 locations on nearly 1,300 networks in 130+ countries. Our security teams use this data, measured in petabytes per month, to research attacks, flag malicious behavior, and feed additional intelligence into Akamai's solutions.

Layers 3 and 4 DDoS data

Akamai Prolexic Routed protects organizations from DDoS attacks by blocking malicious traffic before it reaches applications, data centers, and cloud and hybrid internet-facing infrastructure (public or private), across all ports and protocols. Experts in Akamai's Security Operations Command Centers (SOCCs) deploy proactive mitigation controls to detect and stop attacks instantly and to conduct live analysis of the remaining traffic for further action. These mitigated attacks are organized into attack events and are recorded for analysis.

API data

Akamai API Security has enhanced our API threat research and reporting capabilities by including analysis of both web- and behavior-based vulnerabilities and attacks. For this report, we took a daily snapshot of 2024 and 2025 data to analyze the breakdown of API security alerts according to their corresponding security frameworks and compliance standards.

All the data in this report covered the 24-month period from January 1, 2024, through December 31, 2025, unless otherwise noted.

Guest contributors

Brent Maynard
Senior Director for Cybersecurity Strategy

Brent Maynard is the Senior Director for Cybersecurity Strategy at Akamai. With more than 17 years of experience in driving innovation in cybersecurity, Brent has led teams across the financial services sector and major cloud service providers, developing groundbreaking security solutions and advancing the industry's approach to threat detection and response. Brent's contributions include holding a patent for automated security investigations and shaping transformative products that enhance the security operations center experience.

As a trusted advisor to the intelligence community and federal law enforcement, Brent has guided high-profile cyber investigations and collaborated on solutions to complex security challenges.

Richard Meeus
Senior Director of Security Technology & Strategy, EMEA

Richard Meeus is the Senior Director of Security Technology and Strategy for Europe, the Middle East, and Africa (EMEA) at Akamai. With more than 30 years of experience, Richard is responsible for helping design and build secure solutions for some of the world's most influential organizations. During his time at Akamai, Mirapoint, and Prolexic, he had a strategic role across a broad range of projects, including the transformation of the United Kingdom's largest corporate email implementation and the deployment of DDoS solutions for multinational organizations to protect critical infrastructure and sensitive data.

Richard is a chartered member of the British Computer Society and is a Certified Information Systems Security Professional.

Steve Winterfeld
Advisory Chief Information Security Officer

Steve Winterfeld is Akamai's Advisory CISO. He has a strong background in building operational security programs that are compliant with industry regulations. Before joining the team, he served as CISO for Nordstrom Bank, Managing Director of Incident Response and Threat Intelligence at Charles Schwab, and Senior Technical Director Cybersecurity & Group CTO at Northrop Grumman. Before working in the commercial sector, he was an Airborne Ranger in the United States Army and built out the first regional emergency response center (today called security operations centers) for Southern Command.

Steve focuses on collaborating with Akamai's customers to enable them to be successful in defending themselves and their customers. He also helps determine where Akamai should be focusing its security platform's capabilities. Steve has published a book on cyber warfare and holds CISSP, ITIL, and PMP certifications.

Reuben Koh
Director of Security Technology, APJ

Reuben Koh is the Director of Security Technology and Strategy for the Asia-Pacific and Japan (APJ) region at Akamai. With over two decades of leadership in the cybersecurity industry, Reuben is responsible for driving Akamai's strategic security initiatives, helping organizations navigate the complexities of digital transformation while maintaining a robust defense against an evolving cyberthreat landscape.

Throughout his career, Reuben has been a trusted advisor to large enterprises, particularly in the financial and energy sectors, on the implementation of Zero Trust architectures, SecOps optimization, and various industry frameworks. His current research focus centers on the intersection of artificial intelligence and cybersecurity, specifically the risks posed by agentic AI and the protection of intelligent digital assets.

Credits

Research director

Kimberly Gomez

Writing and editing

Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Maria Vlasak

Review and subject matter contribution

Ryan Barnett
Roger Barranco
Gabriel Bellas
Reuben Koh
Brent Maynard
Richard Meeus
Stas Neyman
Menachem Perlman
Juan Carlos Rivera
Yariv Shivek
Rubens Waberski
Steve Winterfeld

Data analysis

Galit Belkov
Chelsea Tuttle

Promotional materials

Ashley Linares
Ellen O'Brien

Marketing and publishing

Georgina Morales Hampe
Kimberly Gomez

State of the Internet/Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet/Security reports.

Akamai threat research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research.

Akamai security research

Read the Akamai security research blog for a rapid response perspective on today's most important research.

Access data from this report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided that Akamai is duly credited as a source and the Akamai logo is retained.

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 03/26.