V11 ISSUE 02

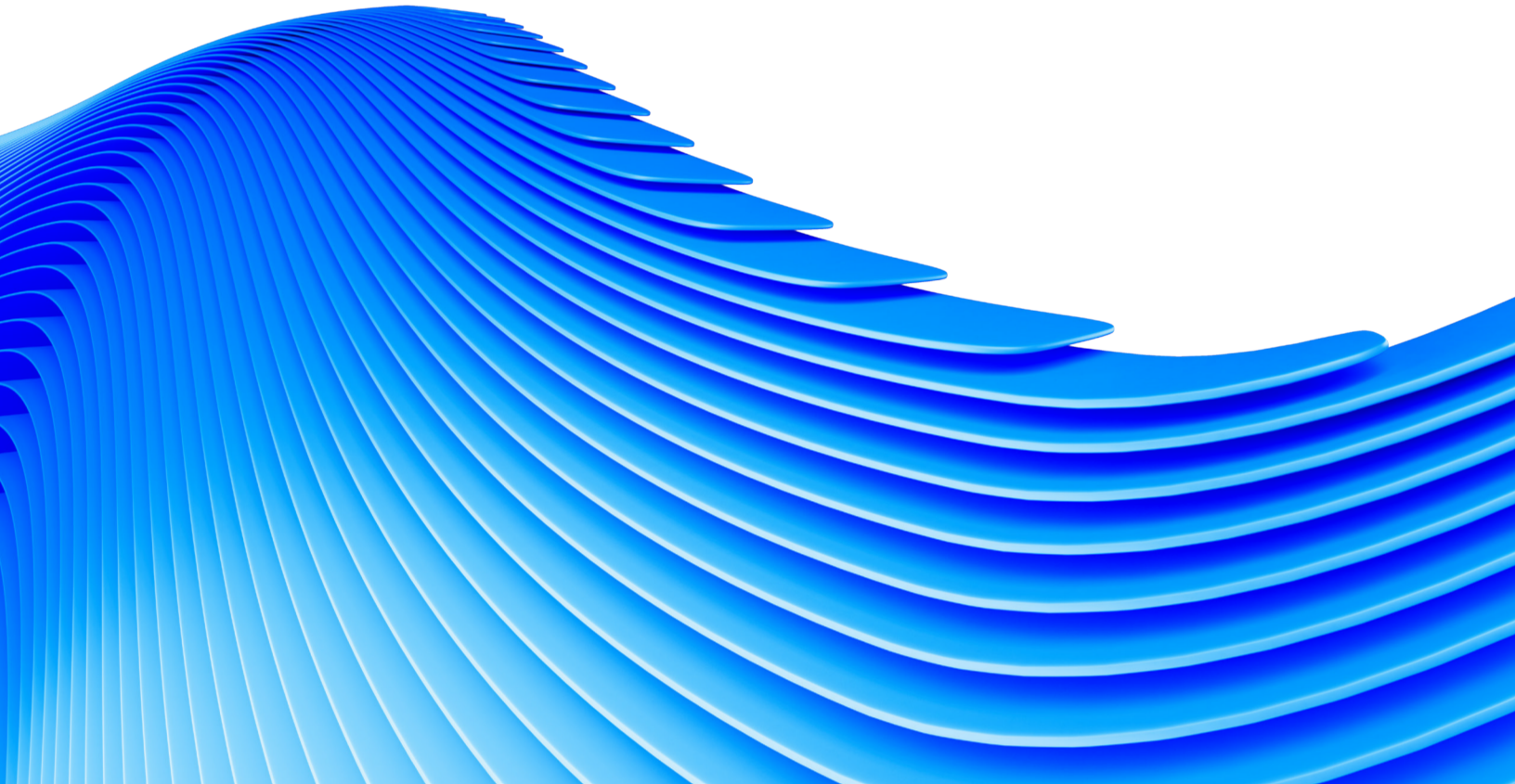
State of Apps and API Security 2025

How AI Is Shifting the Digital Terrain

Akamai

State of the Internet/Security

Contents



Introduction

The web application security landscape in early 2025 reflects unprecedented complexity and sophistication in threat vectors. Organizations are confronting a marked increase in attacks that target web applications — Akamai observed more than 311 billion web application and API attacks in 2024 alone, representing a 33% year-over-year increase. This surge correlates directly with the accelerated adoption of cloud services, microservices architectures, and artificial intelligence (AI)–powered applications. Geopolitical factors have further intensified this landscape, with the high technology, commerce, and social media industries experiencing the most significant volume of Layer 7 (application-layer) distributed denial-of-service (DDoS) attacks. Notably, threat actors are now deploying AI-generated kill chains that automate the entire attack lifecycle.

Concurrently, APIs have emerged as primary targets, with Akamai documenting more than 150 billion API attacks from January 2023 through December 2024. The integration of AI-driven software as a service (SaaS) tools with core platforms via APIs has substantially expanded the attack surface. The financial implications are severe — API security issues currently cost organizations approximately US$87 billion annually, and projections indicate that this figure could exceed US$100 billion by 2026 without adequate intervention. Shadow and zombie APIs present particularly vulnerable attack vectors within increasingly complex API ecosystems.

The role of AI in web application and API security

AI is transforming both web application and API security landscapes by enhancing threat detection and response capabilities, while also introducing new challenges. In web applications, AI is used to automate threat detection, predict potential breaches, and improve incident response times. However, AI also enables attackers to generate AI-driven malware and sophisticated web scraping and to automate the attack lifecycle with dynamic attack methodologies.

For APIs, AI plays a crucial role in managing and securing the vast number of API interactions. AI-powered tools are essential for detecting anomalies, identifying misuse patterns, and automating responses to threats in real time. AI-driven API management will continue to evolve by integrating predictive analytics and automated security measures to protect against increasingly sophisticated attacks. Despite these advancements, AI-powered attacks on APIs, such as credential stuffing and business logic exploits, remain a significant concern, necessitating robust security frameworks to counter these threats effectively.

Divergent yet interconnected: Web application and API attack strategies

Web application attacks and API attacks, while related, target different aspects of an application's infrastructure:

- **Web application attacks** target user-facing components of web applications, such as public-facing login pages, and often employ less sophisticated techniques.
- **API attacks** focus on exploiting vulnerabilities in an application's API endpoints and back-end logic, requiring a deeper understanding of the API's structure and behavior.

The key differences lie in their attack surface and complexity. Web application attacks typically target the visible parts of an application, while API attacks exploit the communication channels among different software components. However, they can both provide unauthorized access to sensitive data and system resources when successful.

Understanding cybersecurity measures for both web application and API attacks simultaneously is critical because modern applications increasingly rely on APIs for functionality. Organizations expect a 39% increase in web applications within two years, so the interdependence of web and API security has become more pronounced. Neglecting either aspect can leave an organization vulnerable to sophisticated, multi-vector attacks that exploit weaknesses in both the front end and back end of applications.

Akamai's unique perspective: Unveiling threat patterns

Akamai's analysis of this complexity benefits from its network infrastructure, which processes more than one-third of global web traffic, providing unmatched visibility into threat patterns. This perspective, combined with insights from its research and data science teams, enables Akamai to deliver intelligence that is both comprehensive and actionable. Its findings offer security leaders the strategic insights necessary to make decisions on where to focus on reducing risks to maximize the return on security investments.

Key insights of the report

AI-powered APIs are more unsecure than their counterparts.
The majority of artificial intelligence (AI)–powered APIs are externally accessible and many rely on inadequate authentication mechanisms — a vulnerability that's compounded by the growing array of AI-driven attacks that are targeting them.

AI fuels technical advancement for threat actors.
This includes advancements like AI-driven malware, vulnerability scanning, attacks on AI-integrated systems, and sophisticated web scraping capabilities.

32%

The percentage of increase in OWASP API Security Top 10–related incidents

API security incidents are rising, with Open Worldwide Application Security Project (OWASP) API Security Top 10 issues revealing authentication and authorization flaws that expose sensitive data and functionality.

30%

The growth in security alerts related to the MITRE security framework

Attackers are using advanced techniques, including automation and AI, to exploit APIs. The MITRE framework can help defenders more quickly and accurately identify these attacks.

33%

The percentage of increase in global web attacks year over year

The surge in attacks directly correlates with the rapid adoption of cloud services, microservices, and AI applications, which expand attack surfaces and introduce new security challenges.

230 billion+

The number of web attacks that hit commerce organizations,

making it the most impacted industry with nearly triple the number of attacks experienced by high technology (the second most attacked industry).

73%

The increase in total web attacks year over year in the Asia-Pacific and Japan (APJ) region,

rising from 29 billion in 2023 to 51 billion in 2024.

37%

The percentage of web attacks in the Europe, Middle East, and Africa (EMEA) region targeted APIs,

which is the highest concentration of such attacks across all regions.

94%

The growth in quarterly Layer 7 distributed denial-of-service (DDoS) attacks

between Q1 2023 and Q4 2024.

11.9 trillion

The number of Layer 7 DDoS attacks that targeted North America

during the two-year period Q1 2023 through Q4 2024.

7 trillion

The number of Layer 7 DDoS attacks that targeted the high technology industry

from January 2023 through December 2024, making it the most affected industry.

7.4 trillion

The number of Layer 7 DDoS attacks that targeted the APJ region

during the two-year period Q1 2023 through Q4 2024.

20%

The percentage of Layer 7 DDoS API-related attacks that targeted the EMEA region,

representing the highest concentration of this attack type across all regions.

Evolving our API threat intelligence

Akamai's integration of Noname Security has significantly enhanced our API threat research and reporting capabilities, offering a fresh perspective on API-specific risks. Akamai is using this new dataset (still in the early stages of data integration) to enhance our existing threat intelligence and provide an expanded view of API security issues.

Mapping alerts to security frameworks

Over time, this new dataset will map deeper security alert details to critical cybersecurity frameworks and compliance standards, including the:

- MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)
- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- International Organization for Standardization (ISO)
- Open Worldwide Application Security Project (OWASP)

These enhancements significantly strengthen Akamai's ability to provide robust protection for clients. By aligning with these frameworks, organizations can gain a clearer understanding of their security posture, meet regulatory requirements, and effectively prioritize their security efforts. This comprehensive approach empowers organizations to allocate resources strategically and develop targeted strategies to safeguard their APIs and sensitive data.

Analyzing a 30-day data sample

For this report, we've analyzed a 30-day data sample to highlight general activity by threat actors across each of the cybersecurity frameworks and compliance standards (Figure 1). We provide a deeper perspective on MITRE and OWASP alerts, as well. We also examine how these risks and security incidents can impact compliance standards.

	30-Day Activity	Monthly Increase
OWASP	**5,907,000**	**32%**
MITRE	**2,817,000**	**30%**
ISO	**832,000**	**22%**
GDPR	**669,000**	**21%**
PCI DSS	**881,000**	**16%**

Fig. 1: Breakdown of security alerts according to security frameworks and compliance standards

MITRE alerts

Over a 30-day period, we observed a 30% increase in incidents related to MITRE techniques among our customers. Notably, attackers frequently employed T1078 (Valid Accounts), leveraging legitimate credentials to gain unauthorized access to systems or networks. Since APIs often rely on tokens for authorization, adversaries who obtain these tokens can access sensitive data without detection.

We also identified T1566 (Phishing), in which attackers launched phishing campaigns to steal API tokens or credentials for future attacks. As APIs expand the attack surface, threat actors increasingly exploit them to gain entry. Additionally, alerts related to T1190 (Exploit Public-Facing Application) revealed attackers using application flaws to infiltrate networks. Another observed technique was T1580 (Cloud Infrastructure Discovery), in which adversaries used APIs for reconnaissance by probing exposed cloud endpoints via API calls.

Although MITRE does not have a dedicated API security matrix, its framework remains crucial for security teams and organizations seeking insights into attacker techniques that are targeting APIs. By mapping adversary tactics to API-specific behaviors, security teams can enhance incident response and threat detection by identifying attack stages and associated tactics, techniques, and procedures. This approach enables defenders to mitigate risks more effectively.

OWASP alerts

The OWASP API Security Top 10 serves as a vital resource, providing actionable insights into vulnerability impact and severity. It empowers developers and security teams to prioritize initiatives effectively, with updates that keep the information relevant in the rapidly evolving threat landscape.

During the 30-day sample period, our analysis revealed a 32% increase in OWASP-related incidents. Notably, vulnerabilities such as Broken Object Property Level Authorization (BOPLA), Broken Function Level Authorization, and Broken Authentication expose sensitive data or critical functions directly to attackers. Insufficient authorization mechanisms enable adversaries to escalate privileges, take over accounts, and access confidential information, making them some of the most dangerous attack vectors targeting APIs.

Broken Object Level Authorization (BOLA) remains a critical API security vulnerability, but its detection is challenging due to its reliance on business logic flaws. This often results in underreporting or low detection rates. To address this, organizations should employ API security solutions that establish clear relationships among users and the resources they typically access. This requires setting behavioral baselines via sophisticated machine learning algorithms that are capable of recognizing anomalous access patterns.

BOPLA exploits granular field-level access issues in APIs, which are often overlooked during security testing. Unlike BOLA, which requires changing entire object IDs, BOPLA attacks target specific properties within objects. For instance, a DELETE API call that exposes sensitive personally identifiable information (PII) in its response constitutes a BOPLA vulnerability. This subtlety makes BOPLA issues more prevalent than BOLA attacks.

Security alerts related to PCI DSS and GDPR increased by 16% and 21%, respectively, while ISO 27001–related alerts rose by 22%.

A practical example involves an unsubscribe request using only an email address, where the API response inadvertently includes the user's full name and address. Such exposure of sensitive data to unauthorized parties occurs because security testing typically focuses on entire objects rather than individual properties. This oversight contributes to the increased detection of BOPLA vulnerabilities in API security assessments.

Another critical vulnerability is Unrestricted Resource Consumption, which attackers can exploit to cause service disruptions through resource exhaustion or DDoS-like attacks. This vulnerability poses risks beyond service impacts, including increased operational costs from the overuse of cloud resources and heightened risks of brute-force attacks. Without proper rate limiting, attackers can rapidly probe APIs, potentially compromising security. Moreover, these attacks generate substantial traffic, leading to significant cost increases for organizations.

Unsafe consumption of APIs, which stems from inadequate validation, filtering of data, and lack of security mechanisms during third-party API integrations, presents another significant threat vector. This issue is increasingly concerning as organizations rely more heavily on third-party APIs for digital transformation. A recent study revealed that more than 80% of surveyed organizations faced problems with third-party APIs, highlighting the importance of adopting a Zero Trust security model. Although this vulnerability alone may not be immediately catastrophic, it can become a major security threat when combined with other weaknesses, such as poor validation or unsecure dependencies. For instance, a financial API's trust of unverified third-party transactions could lead to security breaches.

Ensuring API compliance

Best practices for ensuring API compliance include tagging each alert with the specific compliance and regulatory standards it violates, giving organizations immediate insights into critical compliance issues and providing actionable guidance to address them. This proactive approach helps organizations maintain regulatory compliance, which reduces the risk of regulatory fines, legal repercussions, and reputational damage that can lead to significant financial losses. For example, an airline faced a £20 million fine after an API vulnerability exposed the data of 400,000 customers, highlighting the severe consequences of inadequate API security under GDPR.

Compliance standards serve as essential guardrails for organizations to protect sensitive data, safeguard customers, and meet legal and regulatory obligations. Standards such as the PCI DSS, the GDPR, and the Health Insurance Portability and Accountability Act (HIPAA) require the secure handling of sensitive information like payment data and PII. According to our data analysis, security alerts related to PCI DSS and GDPR increased by 16% and 21%, respectively, while ISO 27001–related alerts rose by 22%.

GDPR

The GDPR emphasizes integrating data protection and customer privacy throughout the entire API lifecycle. This involves secure design, strong authentication and authorization, rate limiting, regular vulnerability testing, encryption, and ongoing risk assessments, even during early development stages. These measures ensure data confidentiality, integrity, and availability.

PCI DSS

Similarly, the PCI DSS emphasizes securing APIs that handle payment card data by integrating security into design, coding, and testing phases. It mandates protection against web vulnerabilities and regular testing to identify and address security flaws.

Requirements 10 and 11 specifically call for comprehensive logging and monitoring of API activities, including requests, responses, authentication attempts, and system changes. Logs must be retained for at least 12 months, with the most recent three months readily accessible for analysis. Additionally, it recommends that organizations perform external vulnerability scans after significant changes. To ensure PCI compliance, organizations must implement strict controls, including rate limiting, logging, role-based access control (RBAC), and session management to ensure APIs are resilient against threats and risks.

ISO 27001

The ISO 27001 standard provides a solid framework for effectively managing information security risks, improving an organization's security posture, and building trust among peers and customers. Recommended practices include:

- Implementing access control (e.g., API keys) to verify user identity
- Employing end-to-end data encryption
- Monitoring APIs for anomalous behavior
- Conducting thorough risk assessments to identify potential API vulnerabilities

These compliance requirements highlight the critical intersection between API security and regulatory frameworks. Proper implementation not only protects sensitive data but also satisfies multiple compliance mandates simultaneously. For more information on existing and emerging global standards, jump to the Compliance section of this report.

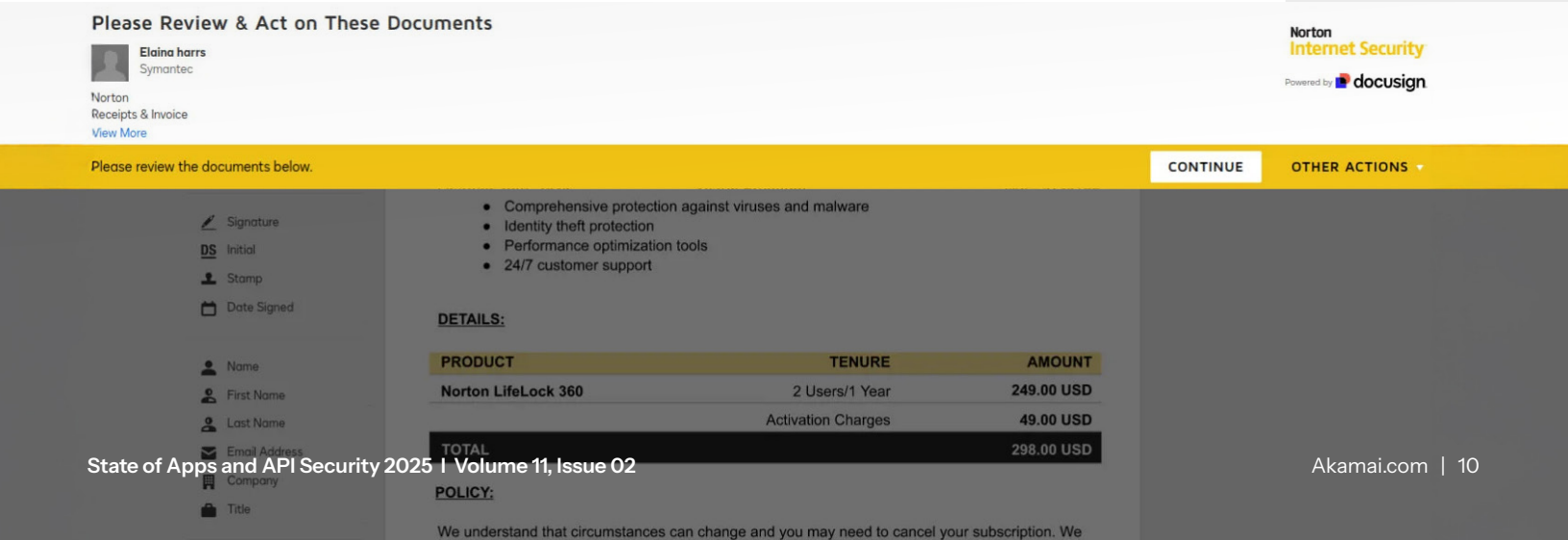
API visibility gaps: The hidden passages to data

API abuse

In November 2024, Bleeping Computer reported a significant attack against an electronic signature solutions provider. Threat actors exploited a core component of the provider's document management and tracking API, enabling them to send fraudulent invoices to numerous potential victims. If recipients unwittingly signed these documents, attackers could then solicit payments from various organizations.

This incident underscores the pernicious impact of API abuse — malicious actors can exploit APIs beyond their intended design and transform them into unintended conduits for attacks. The emergence of generative AI has further exacerbated these risks by automating vulnerability discovery and rate limiting bypasses, facilitating more rapid and sophisticated attacks.

Source: bleepingcomputer/Wallarm



Challenges in API abuse detection

Security teams encounter substantial obstacles in detecting API abuse, primarily due to the necessity of establishing a baseline for normal versus suspicious behavior. This challenge emphasizes the critical need for real-time behavior monitoring to identify anomalies and threats preemptively.

Our 2024 API Security Impact Study reveals a concerning trend: Only 13% of surveyed organizations test their APIs daily, which is a marked decrease from 37% in 2023. This decline is particularly alarming given the current threat landscape. The sharp reduction in daily API testing exposes organizations to heightened security risks, as it significantly diminishes their ability to detect and respond to rapidly evolving threats, potentially leaving critical vulnerabilities unaddressed for extended periods.

Frequent automated testing during development cycles enables organizations to identify and address issues early, averting costly remediation in production environments. In an era when API exploitation increasingly employs automated and covert methods, proactive testing plays a pivotal role in risk mitigation.

Unmanaged APIs: Zombie and shadow APIs

API estate visibility remains a critical challenge for organizations, encompassing both official API tracking and sensitive data identification. The 2024 API Security Impact Study reveals a significant gap: 47% of AppSec teams maintain full API inventories but fail to identify APIs that handle sensitive data. Senior security professionals report similar limitations, with 42% of them facing this oversight issue. Alarmingly, the number of enterprises with complete API inventories and knowledge of sensitive data exposure has decreased from 40% in 2023 to 27% in 2024. The Security Impact Study also highlights zombie and shadow APIs as one of the leading causes of API security incidents.

Incomplete inventories primarily miss zombie and shadow APIs. Zombie APIs (that is, outdated interfaces that remain active because of incomplete decommissioning, staff turnover, or other reasons) create vulnerable attack vectors. Shadow APIs (those developed as rapid solutions outside of the standard approval processes) pose comparable threats. Research indicates that one-third of malicious API transactions target shadow APIs.

Traditional security measures like web application firewalls (WAFs) prove inadequate against these threats. Organizations require advanced API discovery and monitoring solutions to identify vulnerable endpoints effectively.

A comprehensive API inventory forms the cornerstone of effective security strategy, enabling organizations to monitor usage patterns, track version histories, identify vulnerabilities, and meet compliance and regulatory requirements. This strategic approach provides clear visibility into an organization's digital infrastructure, which can ultimately strengthen risk management and enhance overall security posture.

Akamai

Security spotlight

In the first quarter of 2025, we identified an attack on an ecommerce company via API abuse. The company's send SMS API lacked proper authentication, allowing attackers to exploit it by using more than 200 different IP addresses, a single authentication token, and numerous random mobile numbers (both legitimate and fake).

The attack strategy was straightforward but effective: Overwhelm the company by registering multiple mobile numbers and sending SMS messages to fraudulent numbers to directly cause financial damage. When the attackers registered a mobile number, the impacted company, which pays for an SMS gateway service to facilitate text messaging between their applications and mobile devices, incurred unexpected financial charges that could damage their brand or reputation. A defense-in-depth strategy with multiple layers of security measures can counter this type of attack and significantly mitigate the associated risks.

Our alerts revealed that threat actors launched 11,057 POST requests during this attack, with 5,659 successful responses (Figure 2).

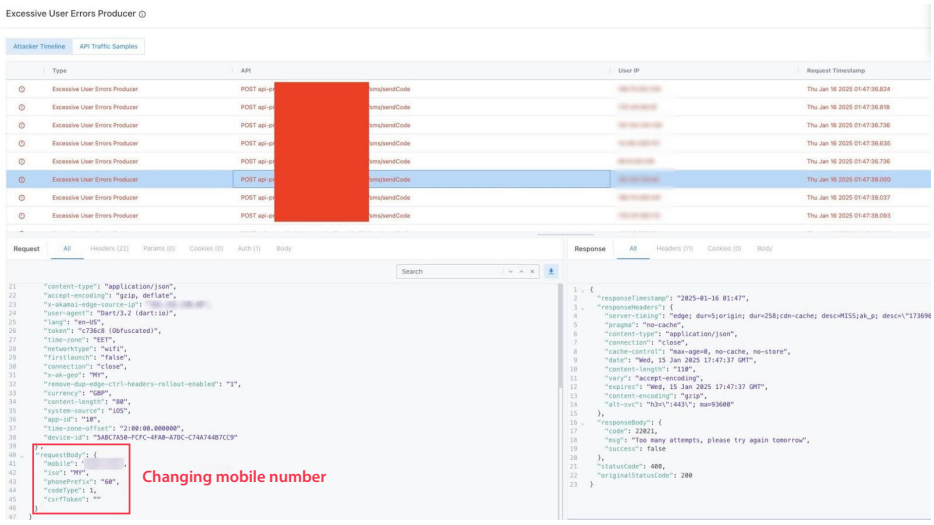


Fig. 2: Threat actors flood the unsecure API with requests

These automated requests were identical, with the exception of one critical parameter:

Body param **mobile**: the following pattern is detected - **<number>**

Such requests can overload the server and lead to denial of service, or they can indicate successful unauthorized access to the API. Traditional WAFs lack the capability to detect these sophisticated attacks. However, advanced API security solutions that create a baseline for normal API behavior can identify such attacks through behavior analysis, mitigate risks proactively, and prevent attackers from escalating damage.

Web attacks: Year-over-year comparison and trends

Akamai's research revealed a substantial increase in web attacks that targeted web applications and APIs during the reporting period of January 2023 through December 2024 (Figure 3). Monthly attack volumes increased from nearly 14 billion at the beginning of 2023 to more than 29 billion by October 2024. This represents a 65% growth in web attacks from Q1 2023 through Q4 2024.

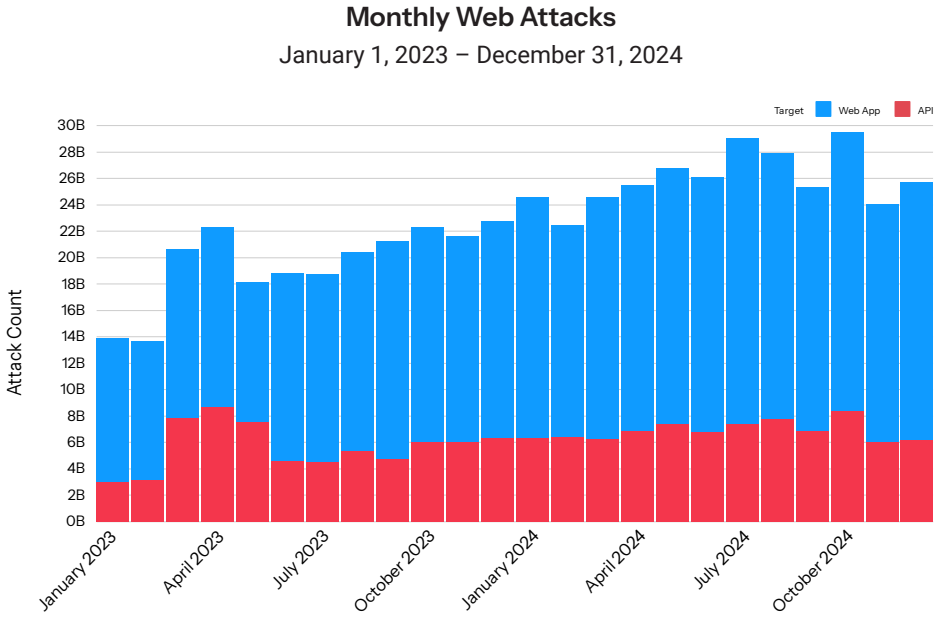


Fig. 3: Traditional web attacks targeting web applications and APIs continue to be on the rise, as shown by a 65% increase between Q1 2023 and Q4 2024

Top vectors: A blend of traditional and modern behavior-based risks

Cybersecurity professionals confront escalating complexities when safeguarding their organizations' digital infrastructure against a spectrum of threats, ranging from traditional web attacks to modern exploits targeting inherent vulnerabilities and misconfigurations.

API request constraint violations: A growing threat

A comprehensive analysis of API endpoints over a two-year period reveals that API request constraint violations represent an area of concern for organizations (Figure 4). These violations manifest when requests or responses fail to adhere to predefined parameters or established requirements, such as exceeding rate limits or submitting invalid data inputs.

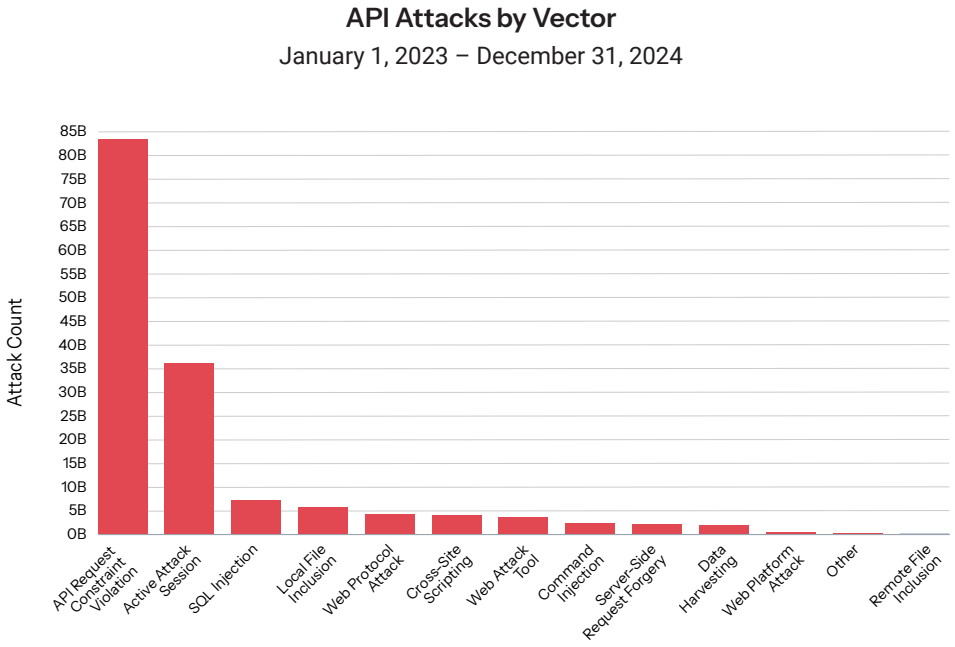


Fig. 4: More than 83 billion request constraint violations were recorded in two years

API request constraint violations present a growing threat, with more than 83 billion attacks recorded in a two-year period. This attack vector saw a substantial 24% surge from 2023 to 2024, underlining the dangers of API abuse. The prevalence of these violations serves as a critical indicator of potential API abuse, which can precipitate a cascade of adverse effects, including system performance degradation, service disruptions, and increased vulnerability to targeted attacks.

Active attack sessions: Unique attacks that call for a creative solution

Akamai's solutions employ innovative security tools to combat the unique challenges posed by API-specific attacks. At the core of these solutions lies a proprietary mechanism to detect active attack sessions, which serves as a strategic defense tool. This system uses Akamai's own threat intelligence to identify and track suspicious behavior, enabling organizations to proactively thwart threats before they escalate into full-scale attacks.

The system flags threat actors and implements a “penalty box” approach. When it comes to modern attacks, adversaries predominantly use automation to execute their reconnaissance and attacks. Akamai quickly identifies these vulnerability scanning sessions, reacts by blocking the client temporarily, and labels these as active attack sessions. This strategy effectively deters potential threat actors from conducting reconnaissance and exploiting network vulnerabilities.

By constraining the window of opportunity for malicious actors, organizations can substantially bolster their API security posture. This approach provides robust protection against a diverse array of potential attacks and significantly enhances overall cybersecurity resilience.

The importance of this strategy is evident in our data. Active attack sessions claimed the top position for both web apps and APIs in terms of overall ranking (Figure 5). In 2023, it accounted for more than 69 billion attacks. This figure surged to more than 113 billion attacks in 2024, which is a remarkable 63% year-over-year increase.

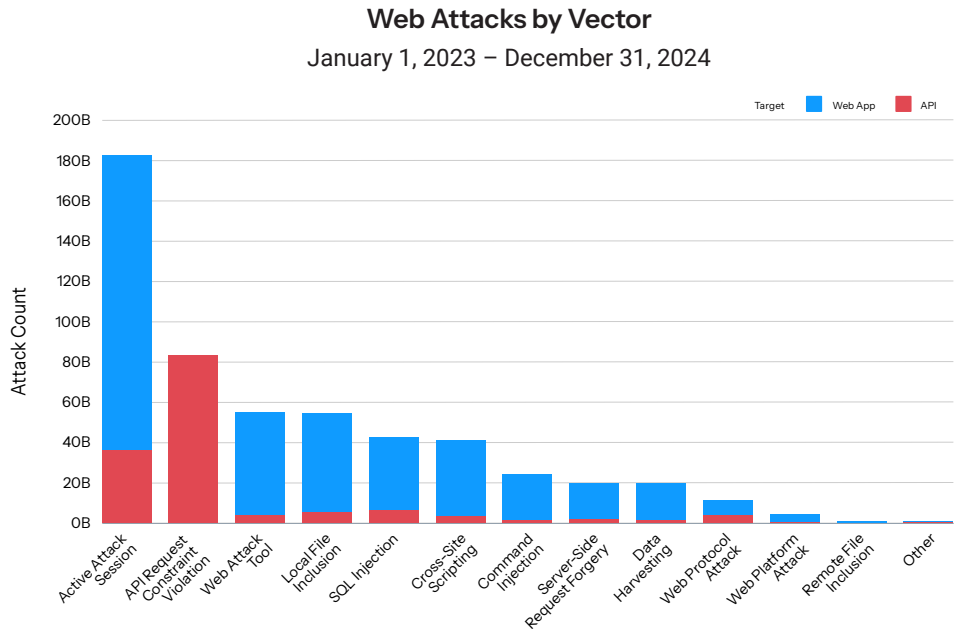


Fig. 5: Active attack session towers over all other vectors for both web apps and APIs, highlighting attackers’ relentless pursuit of vulnerabilities in their intended targets’ networks

Why we can't ignore traditional web vulnerabilities in modern infrastructure

Injection attacks continue to demonstrate high efficacy despite the emergence of sophisticated, behavior-based attack methodologies and increased awareness of traditional web vulnerabilities. Our data from January 2023 to December 2024 indicates a significant surge in attack volume, with Structured Query Language injection (SQLi) and command injection experiencing 60% and 34% year-over-year growth, respectively. These vulnerabilities enable malicious actors to execute unauthorized commands, compromise system integrity, and access sensitive data without proper authentication, highlighting their ongoing relevance in the cybersecurity domain.

The enduring prevalence of SQL databases, renowned for their reliability and scalability in data storage, contributes to the persistent targeting of these systems. Notably, the four most widely used databases employ SQL-based architectures, further emphasizing the critical nature of this attack vector.

Although the OWASP Top 10 API Security list has undergone revisions, such as replacing injection attacks with security misconfiguration in its 2023 update, the risk associated with injection attacks remains paramount. Concurrently, other established vectors such as local file inclusion (LFI) and cross-site scripting (XSS) continue to manifest in high volumes. Our Defenders' Guide 2025 elucidates the sophistication of XSS exploitation techniques, including remote resource injection, cookie theft, website defacement, and session riding, based on real-world attacks observed in 2024.

These findings underscore the imperative for implementing multilayered defense strategies. Cybersecurity professionals must employ a combination of proper output encoding, robust content security policies, and advanced WAFs to effectively counter these increasingly sophisticated attacks.

Layer 7 DDoS attacks: Year-over-year comparison and trends

From January 2023 through December 2024, Akamai research documented a dramatic rise in Layer 7 (application-layer) DDoS attacks against web applications and APIs (Figure 6). Monthly attack volumes surged from slightly over 500 billion in early 2023 to more than 1.1 trillion by December 2024. This represents a 94% growth in Layer 7 DDoS attacks from Q1 2023 through Q4 2024.

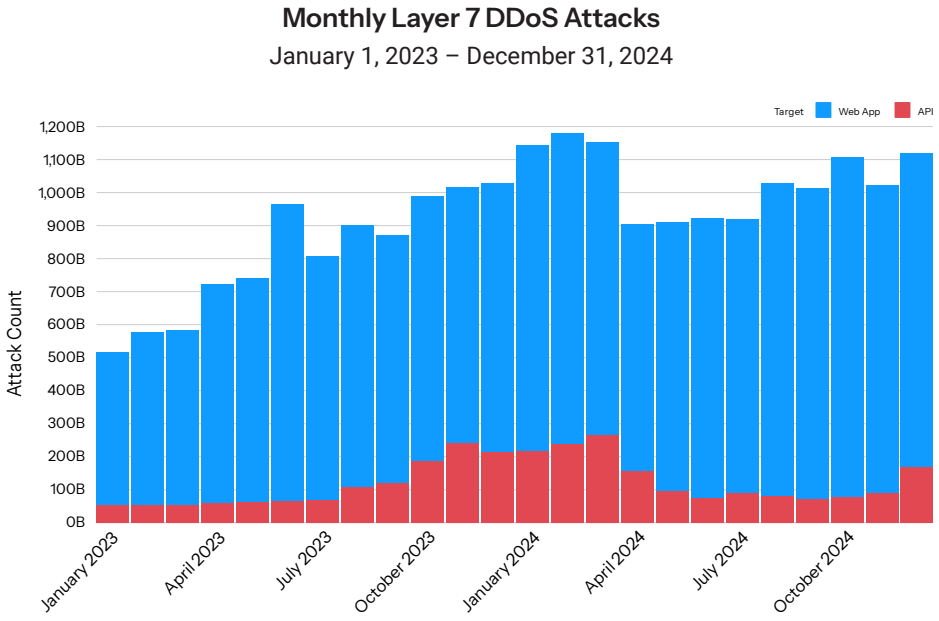


Fig. 6: The number of Layer 7 DDoS attacks targeting web applications and APIs continues to rise, as shown by a 94% increase between Q1 2023 and Q4 2024

Layer 7 DDoS attacks on apps and APIs

HTTP floods persist as a primary threat vector in the ongoing evolution of Layer 7 DDoS attacks targeting web applications and API endpoints. These attacks overwhelm API resources by inundating them with high volumes of seemingly legitimate requests that focus on resource-intensive operations. Attackers have refined their techniques, crafting Layer 7 DDoS attacks to exploit specific vulnerabilities in web application logic or APIs, thus complicating detection and mitigation efforts. Furthermore, bot-driven attacks have grown increasingly sophisticated, generating traffic patterns that closely emulate legitimate API usage.

The attackers' AI transmission: Driving the API road via manual or automatic

Generative AI technologies have revolutionized business integration through APIs, which is "driving" the widespread adoption and practical application of APIs. The AI API market is set to experience explosive growth, projected to reach US$179.14 billion by 2030, up from US$44.41 billion in 2025, with a compound annual growth rate of 32.2%. However, this surge in AI adoption has coincided with a significant increase in AI-driven attacks on APIs. The rise in exposed API vulnerabilities can be largely attributed to attackers leveraging AI as a tool for both reconnaissance and exploitation, whether manually or automatically.

AI-powered API attack strategies

Strategic targeting: Attackers employ AI tools to identify and analyze specific components in target APIs, crafting tailored exploits with AI-generated malicious code for specific vulnerabilities. This approach allows for precise and effective attacks on API weaknesses.

Automated attacks: By automating the attack process, cybercriminals significantly reduce their time and effort, rapidly identifying and exploiting API security weaknesses. This automation often involves AI-powered bots that pose a critical threat to both businesses and individuals.

Volumetric attacks: Attackers weaponize AI to overwhelm APIs with traffic, inundating security systems with significant volume and speed. Automated DDoS attacks exemplify this strategy in which AI-powered bots launch continuous assaults while dynamically adapting to defensive measures.

Behavioral-based attacks: AI analyzes traffic patterns to create low and slow attacks that evade detection by operating below typical alert thresholds. These attacks often target common API vulnerabilities such as BOLA and Broken Authentication.

The irony of AI-powered APIs

Paradoxically, APIs powered by AI have proven to be notably unsecure. The majority of AI-powered APIs are externally accessible, with a significant portion relying on inadequate authentication mechanisms, which renders them more vulnerable to attacks. Our 2024 API Security Impact Study revealed that APIs in generative AI tools were the primary cause of API incidents reported by retail/ecommerce security teams.

The evolving AI threat landscape

The advancements in AI technology have significantly contributed to the evolving threat landscape for APIs. Record increases in AI-driven API vulnerabilities have been reported over the past year, with sources claiming that, for the first time, the majority of all the exploited vulnerabilities recorded by the U.S. Cybersecurity and Infrastructure Security Agency were API-related.

AI-powered web application attacks and defense strategies

The influence of AI on web application security by introducing new attack vectors and defensive capabilities has also been profound. Key areas in which AI has significantly altered the cybersecurity landscape for web application attacks include AI-enhanced malware, AI powered vulnerability scanning, attacks on AI involved systems, sophisticated web scraping, and AI powered WAF systems.

AI-enhanced malware

Cybersecurity experts have observed advanced malware leveraging AI to attack web applications. In a 2024 email campaign that targets French users, attackers deployed malicious code, likely designed with generative AI assistance, to execute the AsyncRAT malware. This example highlights the growing trend of AI-assisted malware creation and deployment, which poses new challenges for web application security professionals.

AI-powered vulnerability scanning

AI has revolutionized vulnerability scanning for web applications, offering both defensive and offensive capabilities whether for beneficial or malicious use. These AI-driven tools now automate searches for common vulnerabilities such as SQLi, XSS, cross-site request forgery, and server-side request forgery (SSRF). Furthermore, they conduct AI-driven analyses of potential impacts and generate AI-powered recommendations for remediation steps.

Attacks on AI-involved systems

The integration of AI, particularly large language models (LLMs), into web applications has introduced new security vulnerabilities. *Prompt injection attacks* target AI systems to override model safeguards. A notable example includes a now-patched Slack AI vulnerability that allowed data gathering from private channels through indirect prompt injection. *Data poisoning attacks* corrupt AI model behavior by manipulating a small percentage of datasets, potentially leading to compromised system integrity. *Jailbreaking techniques* bypass LLM safeguards, allowing attackers to override restrictions, extract sensitive data, and produce harmful outputs. These emerging attack vectors necessitate heightened vigilance and novel defense strategies.

Sophisticated web scraping

AI has enhanced web scraping capabilities, which creates new challenges for web application security. These AI-powered scraping tools now offer more efficient data extraction methods and improved evasion of anti-scraping measures. Since the early 2020s, sophisticated web scraping has been leveraging AI to process data, but there's been a recent substantial increase in the frequency of LLM scraping. Much of this is due to the rise of agent-based querying, which is driving the demand for real-time (nonstatic) data sources.

Unfortunately, this has led to the average web application request (depending on factors such as request complexity, hosting infrastructure, and so forth) costing anywhere from US$0.01 to US$0.50 per request. And while commerce was originally the industry most impacted by the increase of LLM scraping, the tide has turned — other industries (e.g., financial services, gambling, digital media, and video media) have now been experiencing the brunt of this shift.

AI-powered WAF systems

On the upside, advanced WAF systems are being powered by AI to more effectively identify and mitigate a range of cyberthreats, including bots, DDoS attacks, scrapers, and scanners. AI-powered WAF systems help in combating sophisticated cyberattacks since traditional WAFs with static rulesets struggle with zero-day threats and require manual updates.

The multilayer machine learning strategy enables pattern recognition, adaptive learning, anomaly detection, and enhanced response time. Through training on billions of daily events and implementing a layered approach with continuous monitoring, AI-powered WAF systems aim to proactively prevent evolving threats and keep customers protected.

Industry trends

Among industries, commerce towered over all the others with nearly triple the number of overall web attacks experienced as high technology (the second most attacked industry) from Q1 2023 through Q4 2024 (Figure 7). Additionally, the number of API attacks experienced by the commerce industry during the same period greatly outweighed the total API attacks of the remaining top 10 industries.

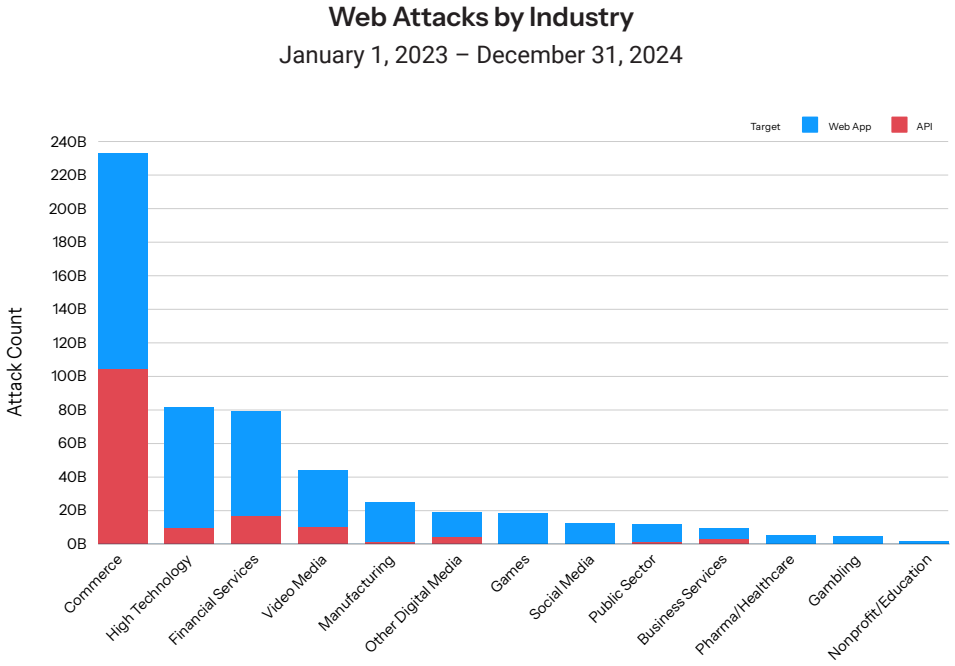


Fig. 7: Commerce, high technology, and financial services were the top three most targeted industries by web attacks

For overall Layer 7 (application-layer) DDoS attacks, the high technology industry was targeted more than any other industry, with attacks reaching more than 7 trillion for the period of Q1 2023 through Q4 2024. High technology was followed by social media and commerce (Figure 8). However, during the same time frame, the number of API-targeted Layer 7 DDoS attacks on the commerce industry once again substantially surpassed that of all the other industries combined.

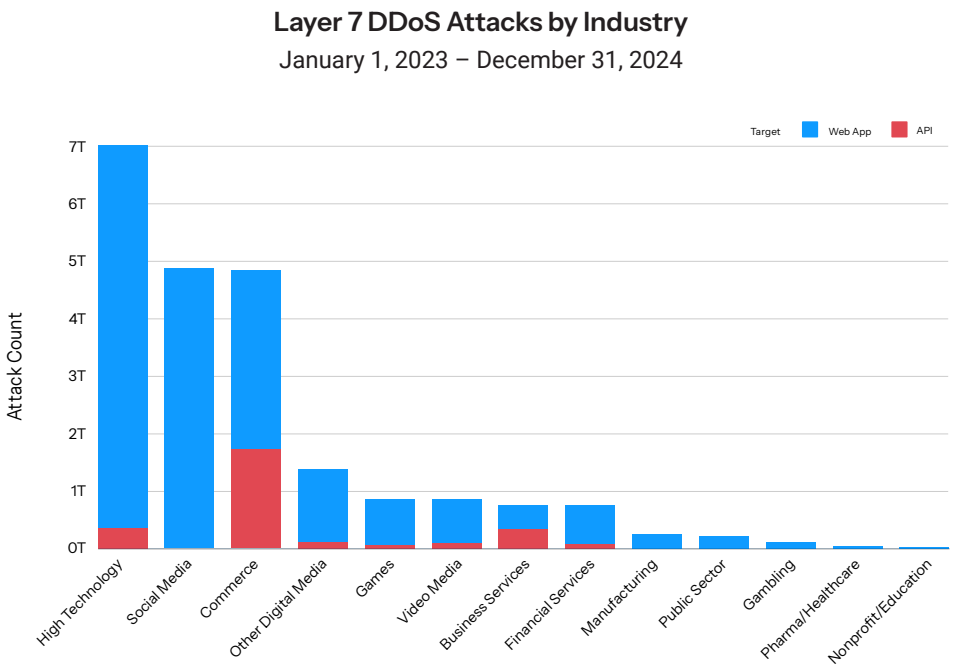


Fig. 8: Layer 7 DDoS attacks by industry

Commerce

In addition to incurring more than 230 billion web attacks — which is more than 40% of the overall web attacks — from 2023 through 2024, the commerce industry faced an unprecedented scale of Layer 7 DDoS attacks, with Akamai data revealing more than 4.8 trillion attacks during 2023 and 2024.

This combined volume represents a strategic targeting pattern in which web applications absorb approximately 64.25% of attacks, while APIs account for the remaining 35.75%. This distribution reflects the dual vectors attackers employ to compromise commerce platforms and highlights the multifaceted nature of the modern threat landscape.

Commerce entities represent particularly lucrative targets because of their concentration of sensitive customer data, payment information, and financial transactions. The direct path to monetization through stolen payment credentials, compromised customer accounts, and sensitive PII creates immediate financial incentives for threat actors. Unlike some industries in which compromised data requires additional steps to convert it into financial gain, commerce platforms often provide attackers with directly exploitable assets.

Retail as the primary target

Retail stands as the most heavily targeted industry segment within the broader commerce industry, facing disproportionate attack volumes because of several distinctive characteristics.

Retail operations typically maintain complex digital ecosystems, incorporating various platforms and systems. Their aggressive digital transformation initiatives often prioritize speed to market over comprehensive security, creating security gaps. The adoption of omnichannel strategies inadvertently increases attack surface complexity. Additionally, the extensive reliance on third-party suppliers creates a complex supply chain with numerous potential compromise points.

Seasonal traffic patterns create predictable high-volume periods that attackers specifically target, with cybercrime incidents spiking by 25% to 30% during the winter holiday season, according to the FBI's Internet Crime Complaint Center. Ecommerce platforms also face heightened threats, with a 31% increase in cyberattacks during December compared with the yearly average.

The evolution of web application attacks

Web application attacks are undergoing a significant transformation, driven by technological advancements and changing attacker methodologies. Threat actors use increasingly sophisticated techniques to exploit vulnerabilities in web applications, adapting their strategies to circumvent evolving security measures. The rise of automated attack tools, coupled with the integration of machine learning algorithms, has enabled attackers to launch more precise and targeted campaigns against retailers' web applications.

Furthermore, the shift toward microservices architectures and API-driven development has expanded the attack surface, necessitating a reevaluation of traditional security paradigms. This evolution demands a proactive approach from cybersecurity professionals, emphasizing continuous monitoring, adaptive defense mechanisms, and a deep understanding of emerging attack vectors in the web application landscape.

The bot threat landscape

The bot threat landscape is rapidly evolving through technological advancement, particularly with attackers integrating generative AI capabilities. This evolution has enhanced attack strategies through faster zero-day exploits and sophisticated evasion techniques that bypass traditional defenses. Evidence shows AI-based bot fraud attacks against retailers increased consistently between August 2022 and April 2024, with a striking 137% spike in January 2024. Detection challenges further exacerbate these threats, with businesses typically taking four months to identify bot attacks while suffering financial and reputational damage.

Bots now function as central vectors in the retail cyber landscape, facilitating account takeover, credit card fraud, and gift card abuse. They serve as enablers for broader attack campaigns by using data stolen from one compromised site to fuel credential stuffing attacks against others, which creates a compounding effect across retail ecosystems. This activity contributes to the "industrialization" of online fraud, with global crime rings using automated tools to scale operations far beyond what manual methods could achieve.

For a list of recommendations on how to better protect your retail operation's web applications and APIs against AI and bot-related attacks, jump to the Mitigation section.

Financial services

The financial services industry has become a prime target for web attacks and continues to see Layer 7 DDoS attacks. Web attacks totaled more than 79 billion between January 2023 and December 2024, while Layer 7 DDoS attacks totaled more than 761 billion against both web application and APIs for the same period.

This unprecedented volume underscores the industry's vulnerability and attractiveness to threat actors. Several factors drive this surge, including the industry's critical role in global economic infrastructure, the high value of financial data, and the potential for significant disruption.

The digitization of financial services

The digitization of financial services has expanded the attack surface for cybercriminals. The adoption of AI-driven personalization, banking as a service, and embedded finance solutions have introduced novel vulnerabilities. Geopolitical conflicts, particularly the Russia-Ukraine war, have fueled hacktivist activities targeting financial institutions. Economic factors, including the rise of cryptocurrencies and potential implementation of a crypto reserve, have heightened threat actors' interest in the financial industry.

Web application attacks are rapidly transforming, adapting to new technologies and exploiting emerging vulnerabilities. Attackers now leverage sophisticated AI and machine learning algorithms to bypass traditional security measures and launch more targeted, persistent attacks. The rise of serverless architectures and microservices has created new attack vectors, while the increasing use of APIs has expanded the potential entry points for malicious actors. Furthermore, the shift toward mobile and cloud-based applications has necessitated a reevaluation of security strategies, as these platforms present unique challenges in terms of data protection and access control.

The banking segment's prominence as an attack target

Within the financial services industry, banking stands out as the most targeted segment for web attacks (Figure 9). As in the commerce industry, credential stuffing attacks are also emerging as a leading threat vector in banking.

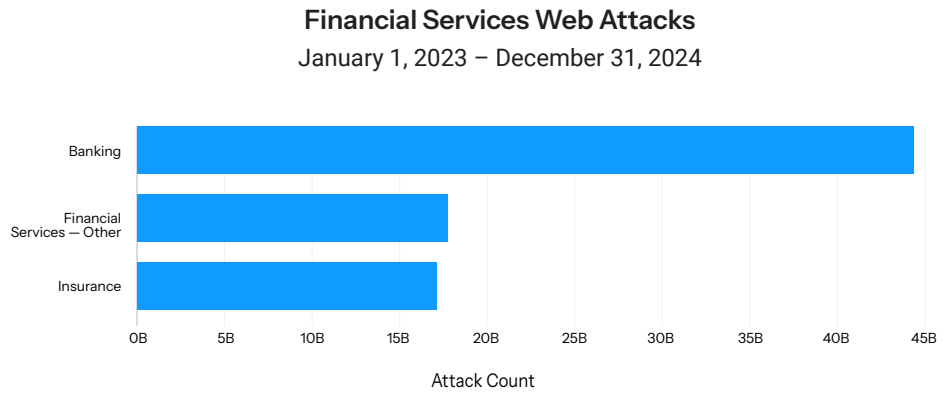


Fig. 9: Banking is the most targeted industry segment among financial services web attacks

The prevalence of online banking services, coupled with the critical nature of account access, attracts cybercriminals. Financial incentives for successful attacks are substantial — even a small number of compromised accounts may yield significant gains. The banking segment's reluctance to implement stringent security measures that might create user friction, such as multi-factor authentication, has inadvertently contributed to its vulnerability.

The banking segment's prominence as an attack target is further exacerbated by several factors. Sensitivity to downtime presents an opportunity for extortion, as threat actors exploit concerns about service disruptions. Additionally, the increasing sophistication of attack techniques, including the use of AI and machine learning to evade detection, poses significant challenges to traditional defense mechanisms. The regulatory landscape, with stringent compliance requirements and potential fines for security breaches, adds another layer of complexity to the banking segment's cybersecurity challenges.

High technology

High technology remains a top attacked industry for web and Layer 7 DDoS attacks. High technology for the purposes of our reporting includes the industry segments of telecommunications, enterprise software and hardware, and consumer software and hardware. Our data showed that this industry was second to commerce in the number of overall web attacks with more than 81.7 billion attacks during the 2023–2024 period. Also, high technology was the industry targeted with the most Layer 7 DDoS attacks: more than 7 trillion during the two-year period.

High technology web applications frequently employ complex database queries and dynamic content, creating vulnerabilities that attackers exploit to easily overwhelm servers. These vulnerabilities contribute to the high rate of Layer 7 DDoS attacks experienced by the industry. Notably, blockchain networks have seen a significant uptick in DDoS attacks, with attackers using methods such as HTTP flooding and spam transactions to impede legitimate transactions, despite blockchain's decentralized architecture. The critical financial impact of operational downtime in the high technology industry motivates attackers to deploy DDoS attacks capable of incapacitating essential services. Modern software development's reliance on API-centric architectures introduces additional risk, as attackers frequently exploit unsecurely coded endpoints in HTTP flood attacks.

The telecommunications segment faces similar challenges

The telecommunications segment, which is affected by a significant number of API attacks, faces similar cybersecurity challenges. Web application and API threats in this high technology industry segment include data breaches, DDoS attacks, and supply chain vulnerabilities. These vulnerabilities have resulted in several high-profile data breaches.

For example, in January 2025, researchers uncovered critical API vulnerabilities in a major telecom network, exposing 3,000 companies to security risks. The investigation revealed significant security gaps, including weaknesses in the Know Your Customer verification process, and a back-end API path traversal vulnerability that was granting access to internal systems.

The Internet of Things introduces new attack vectors

The high technology industry continues to grapple with evolving web application and API vulnerabilities in an era of rapid technological advancement. This evolution encompasses the widespread adoption of Internet of Things (IoT) devices, which introduces new attack vectors because many devices lack robust security measures. The accelerated adoption of multi-cloud infrastructures often results in improperly configured environments, creating potential entry points for exploitation.

Vulnerabilities in unsecurely built IoT devices and cloud systems increasingly fall prey to sophisticated AI-driven attacks. SaaS platforms face elevated risks of API attacks because of their expansive attack surface. The proliferation of AI solutions and increased reliance on third-party SaaS platforms has significantly expanded the overall API attack surface in the high technology industry. As organizations continue to adopt these technologies, the potential for exploitation grows, necessitating robust security measures and vigilant monitoring.

Regional trends

NOTE: We have changed the format for our regional reporting to make the data more accessible to readers and easily highlight attack trends across regions, including North America (N. America); Asia-Pacific and Japan (APJ); Europe, Middle East, and Africa (EMEA); and Latin America (LATAM). We've also included an at-a-glance chart for a quick look at the data that we discuss in this section (Figure 10).

Web Attack Data Layer 7 DDoS Attack Data

Region	Web Attack Counts	Layer 7 DDoS Attack Counts	Top Web Attack Vectors	Top Target Areas	Top Target Industries
APJ	80B, 14% API	7.4T, 6% API	Active attack session, LFI, XSS	Australia (20.3B), India (17.3B), Singapore (15.9B)	Financial services, commerce, social media
				Singapore (4.7T), India (607B), South Korea (283B)	Social media, other digital media, commerce
EMEA	116B, 37% API	2.6T, 20% API	Active attack session, API request constraint violation, LFI	United Kingdom (30.3B), Netherlands (19.5B), Spain (14.2B), Germany (12.8B)	Commerce, video media, financial services
				Germany (569B), United Kingdom (506B)	Commerce, other digital media, video media
LATAM	3B, 12% API	258B, 18% API	Active attack session, WAT, SSRF	Brazil (19.3B), Mexico (2B)	Commerce, financial services
				Brazil (175B), Mexico (39B)	Commerce, financial services
N. America	327B, 29% API	11.9T, 16% API			

Fig. 10: Regions at a glance, January 2023–December 2024 (LFI denotes local file inclusion; XSS, cross-site scripting; WAT, web attack tool; SSRF, server-side request forgery)

Two application and API attack trends

Our analysis of regional comparisons of web application and API attacks and Layer 7 DDoS attacks during the 24-month reporting period from January 2023 through December 2024 reveals two overarching trends (Figure 11).

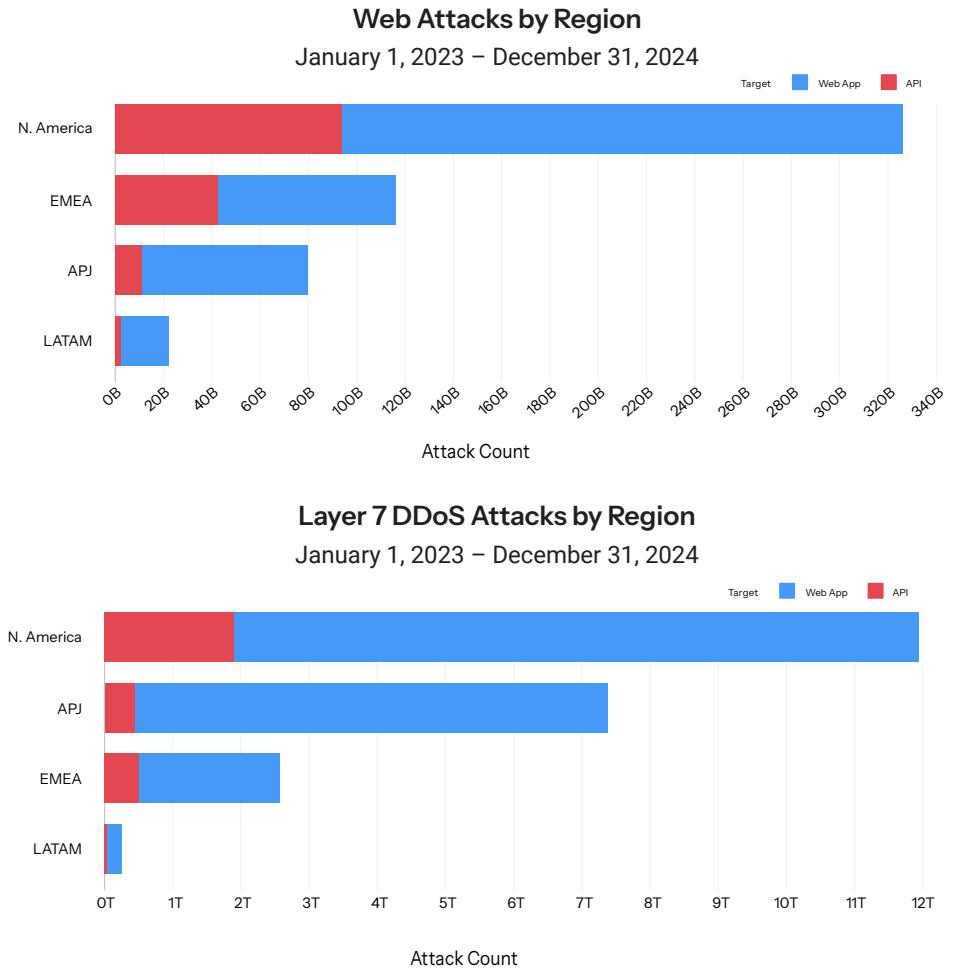


Fig. 11: During the reporting period, on a global basis, EMEA experienced the highest percentage of API attacks, while APJ experienced the second highest number of total Layer 7 DDoS attacks

Attack trend 1: API attacks were widespread in EMEA, which could be attributed to higher API adoption rates than in other regions, as well as to open banking and the PCI DSS v 4.0 that are driving the use of APIs and can introduce security risks. (See the Evolving our API threat intelligence section for an extensive discussion of API-specific risks.)

Continuing the trend we first observed in 2023, EMEA experienced the highest concentration of web attacks on APIs during the 24-month period: Of the 116 billion total web attacks in the region, 37% targeted APIs. In contrast, North America recorded 327 billion total web attacks, 29% against APIs. In APJ, 14% of the 80 billion web attacks targeted APIs with LATAM following at 12% of 3 billion.

EMEA also experienced the highest concentration of Layer 7 DDoS attacks that targeted APIs (20%), followed by LATAM (18%), North America (16%), and APJ (6%). In general, Layer 7 DDoS attack attempts against APIs accounted for a relatively small percentage of total web attacks in each region. We anticipate that these percentages will rise over time for a variety of reasons, including more advanced bot-driven attacks and a surge in AI-driven attacks on API vulnerabilities.

Attack trend 2: APJ experienced the second highest level of Layer 7 DDoS attacks on a global basis at 7.4 trillion (versus 11.9 trillion in North America). EMEA followed at 2.6 trillion and LATAM at 258 billion. This trend was initially observed in our Digital Fortresses Under Siege SOTI report, and we continue to attribute it to a high concentration of attack attempts against social media in APJ.

A deeper dive into APJ, EMEA, and LATAM

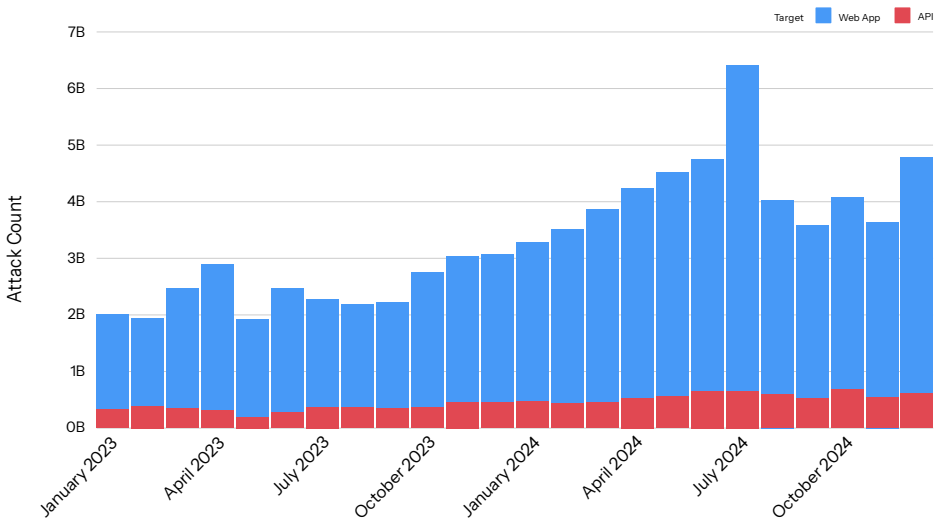
In this section, we highlight some key trends within APJ, EMEA, and LATAM. We also include data specific to areas within these regions where we have sufficient attack event data to provide statistically significant insights.

Web application and API attacks: Traffic analysis

A comparison of monthly web attack trends between regions is a study in contrasts (Figure 12).

APJ: Monthly Web Attacks

January 1, 2023 – December 31, 2024



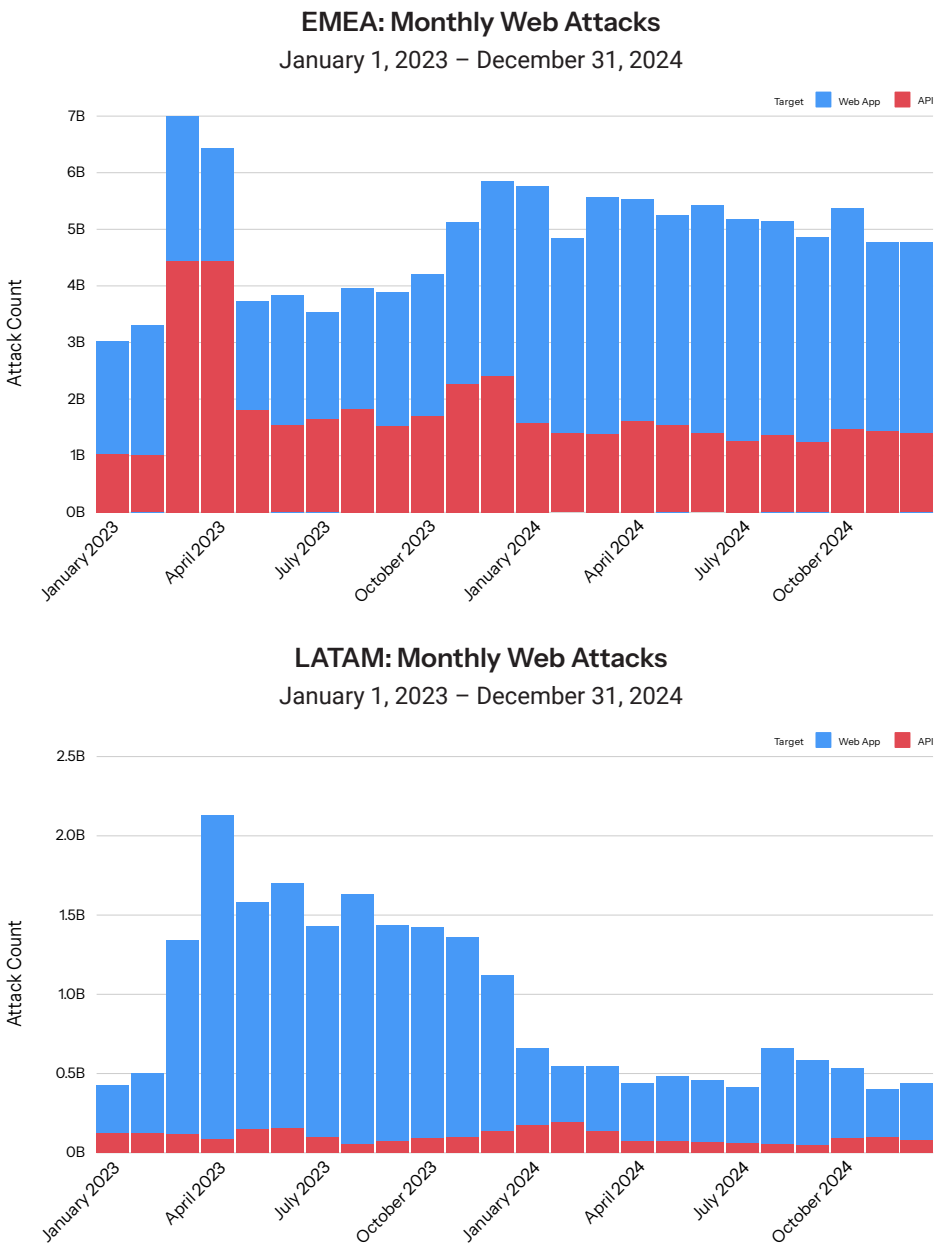


Fig. 12: Web application attack activity drove an increase in the total number of web attacks in APJ and EMEA, while attacks in LATAM declined steeply

APJ experienced a significant 73% increase in total web attacks year over year, from 29 billion in 2023 to 51 billion in 2024. In EMEA, the year-over-year increase was a moderate 16% (from 54 billion to 62 billion) — but this smaller increase is affected by an outlier event recorded in the data that, if removed, would boost the number closer to 33%. In LATAM, web attacks dropped considerably from a total of 16 billion in 2023 to 6 million in 2024, a 61% year-over-year decrease.

Growth in web application attacks appears to be driving an increase in total web attack counts since API attacks remained at low levels, particularly in APJ and LATAM.

In EMEA, following the spike in the first half of 2023 (which was related to large-scale focused attacks on the commerce sector in Spain), API attack levels declined and remained at lower levels throughout 2024, though they were still comparatively high with respect to other regions.

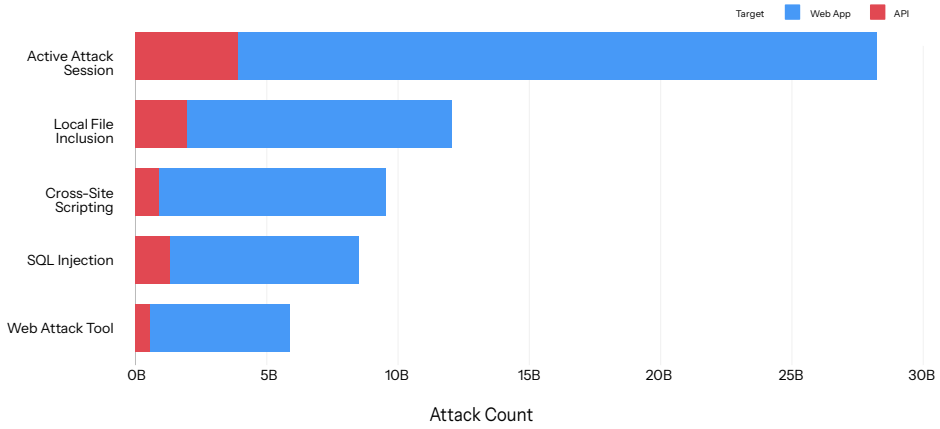
In LATAM, web attacks declined as threat actors shifted their focus from the commerce sector to other industries, including pharmaceuticals and business services, and to other attack types such as ransomware.

Web application and API attacks: Trending tactics

Over the last two years, threat actors continued to rely on traditional tried-and-true methods, but modern, behavioral-based web attack vector use was also high (Figure 13).

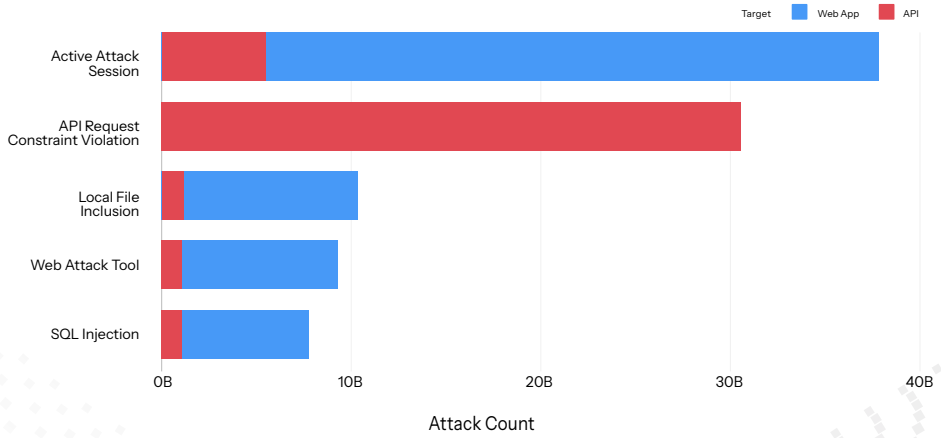
APJ: Web Attacks by Vector

January 1, 2023 – December 31, 2024



EMEA: Web Attacks by Vector

January 1, 2023 – December 31, 2024



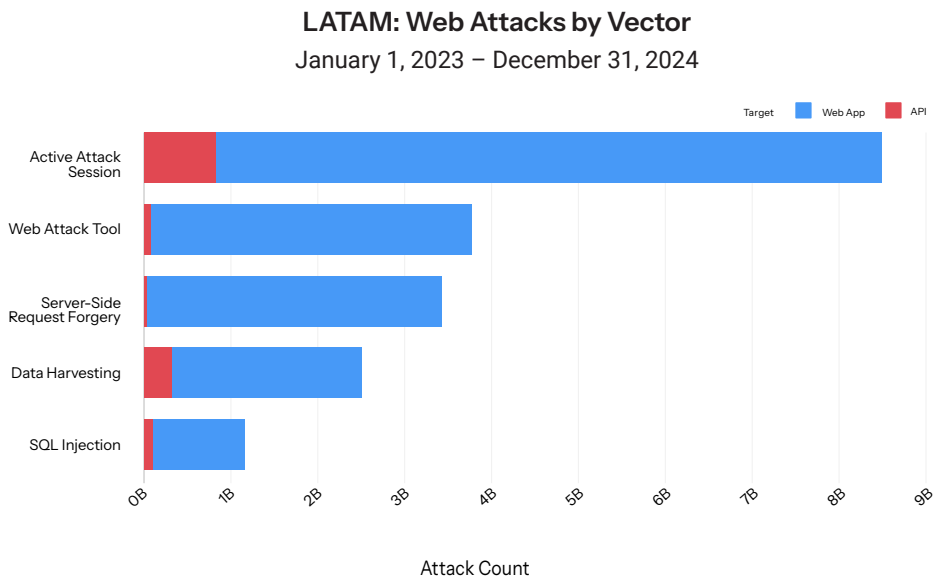


Fig. 13: Across the regions, top attack vectors included traditional methods and modern behavioral-based methods specifically aimed at API abuse

Consistent with global trends, across the regions, traditional attack vectors persist, including LFI, SQLi, and XSS, along with SSRF observed in LATAM. We underscored the staying power of XSS and its continued relevance for protection against traditional web vulnerabilities in our Defenders' Guide 2025.

What's different during this period, as threat actors increasingly focus on API abuse, is the increase in issues with modern, behavioral-based attack vectors. Threat actors use these vectors to discover vulnerabilities to exploit. Tracking these vectors at a regional level, Akamai researchers observed:

- The top attack vector in each region was active attack session, for which our intelligent controls are used to proactively block requests from known threat actors for a length of time.
- API request constraint violation was the second most prevalent in EMEA, where the concentration of API-focused attacks is greatest. Attackers attempt to abuse APIs by evading requirements such as rate limits and data inputs.
- In each region, web attack tool was in the top five. Threat actors use this vector to probe the target to solicit information about its security, configurations, or potential vulnerabilities that could be leveraged for nefarious purposes.

For more details on these top vectors, see the Web attacks section.

Web application and API attacks: Top targets

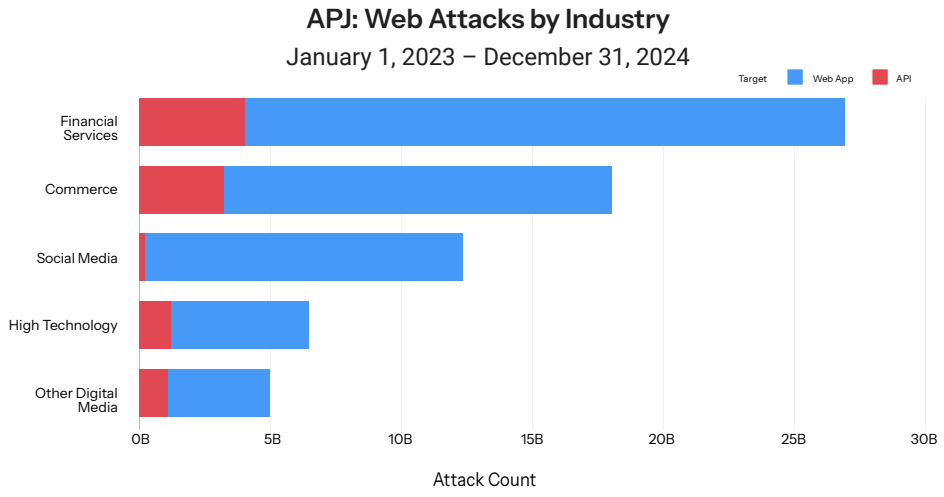
By looking specifically at where attackers focused within each region, we see that in APJ, Australia (20.3 billion), India (17.3 billion), and Singapore (15.9 billion) bore the brunt of web application and API attacks, followed by Japan (6.3 billion), China (6.2 billion), South Korea (4.9 billion), New Zealand (2.9 billion), and Hong Kong SAR (2.2 billion).

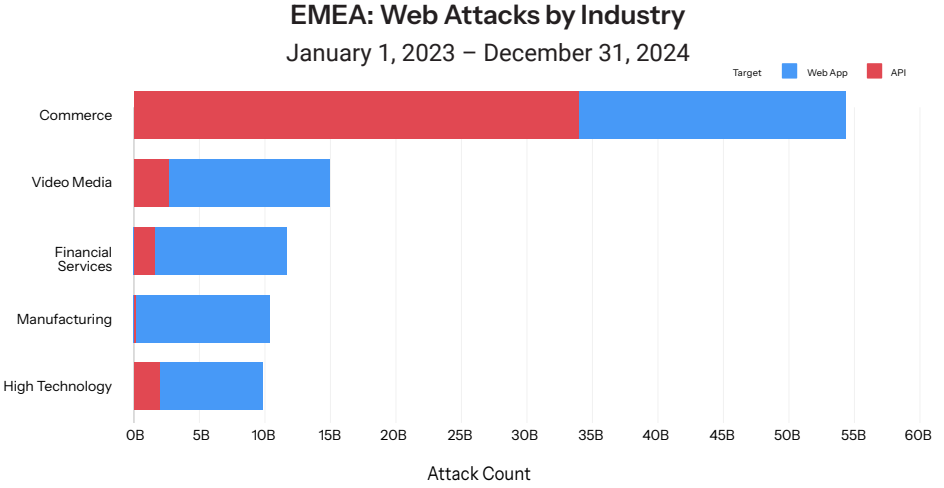
In EMEA, the countries most impacted by web application and API attacks were the United Kingdom (30.3 billion), the Netherlands (19.5 billion), Spain (14.2 billion), and Germany (12.8 billion). Austria followed at 8.2 billion, along with France (7.5 billion), Italy (4.1 billion), Switzerland (3.7 billion), Belgium (3.5 billion), and Israel (3.3 billion).

In LATAM, web application and API attack volume was concentrated in Brazil (19.3 billion), with the next closest countries, Mexico (2.0 billion) and Chile (0.4 billion), experiencing just a fraction of attacks in the region.

Industry targets

Analysis by industry trends found that across APJ, EMEA, and LATAM, commerce and financial services were consistently among the top three industries targeted by web attacks (Figure 14).





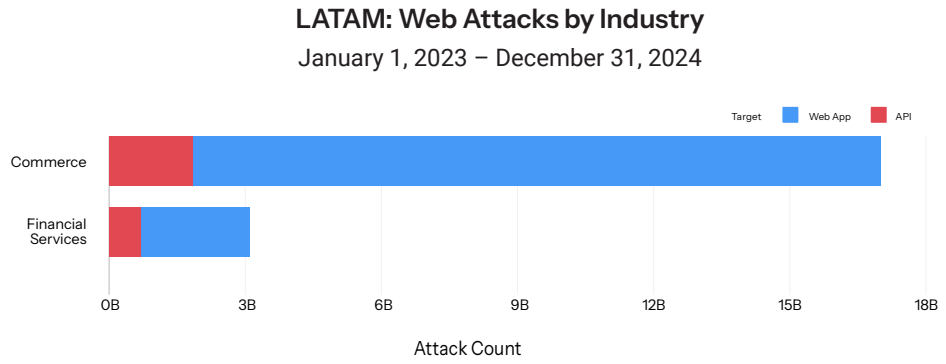


Fig. 14: Commerce and financial services were among the top three targeted industries in the APJ, EMEA, and LATAM regions

In APJ, the financial services industry had the highest number of total web attacks at 27 billion; commerce was second at 18 billion. This represents a year-over-year growth of 52% and 161%, respectively. Other digital media was the most targeted industry for API attacks at 22%, followed by commerce (18%), and financial services (15%).

In EMEA, commerce was the industry that was most impacted by web attacks at 54 billion, which is more than three times the number of the next closest industry. Despite the high concentration, total web attacks against commerce entities decreased by 10% year over year because of a spike in 2023 that skewed the data in the region. However, EMEA still recorded a 16% year-over-year increase in total web attacks driven by an uptick in attacks against other industries, including financial services (152%) and manufacturing (96%). By taking a closer look at API-directed attacks in the region, we see that 63% of total web attacks against commerce targeted APIs.

We see a similar trend in LATAM, where the total number of web attacks against commerce reached 17 billion, towering over other industries, but year-over-year attacks on the commerce industry decreased by 76%. Meanwhile, the pharmaceuticals and business services industries experienced year-over-year increases of 107% and 129%, respectively. Additionally, 11% of attacks that targeted commerce focused on APIs, and financial services had an even higher concentration of attacks against APIs at 23%.

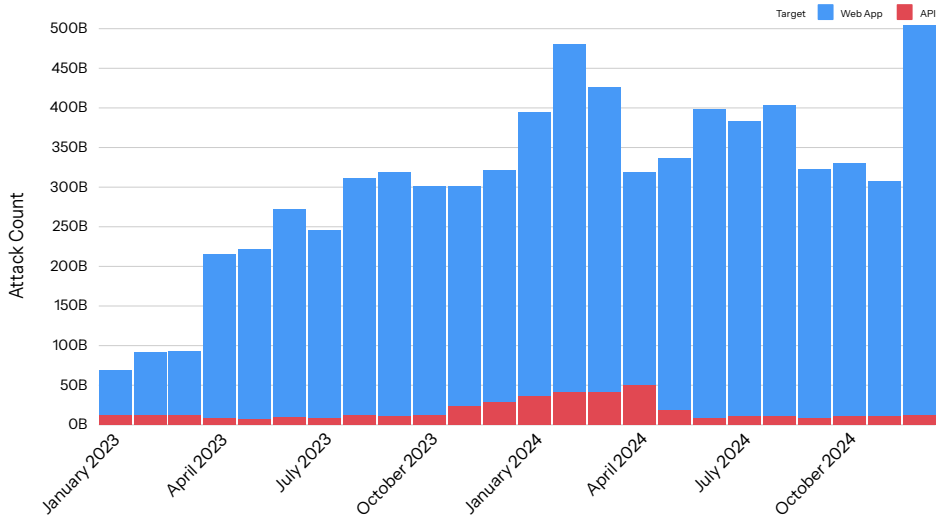
The financial services and commerce industries share attributes that contribute to their appeal as targets for web application and API attacks: both operate within complex ecosystems, have a high reliance on APIs, and possess valuable data. Threat actors use a blend of traditional and emerging attack techniques to achieve their goals.

Layer 7 DDoS attacks: Traffic analysis

A comparison of monthly Layer 7 DDoS attack trends among regions reveals that APJ was a hotspot, and EMEA and LATAM experienced an ebb and flow of attacks (Figure 15).

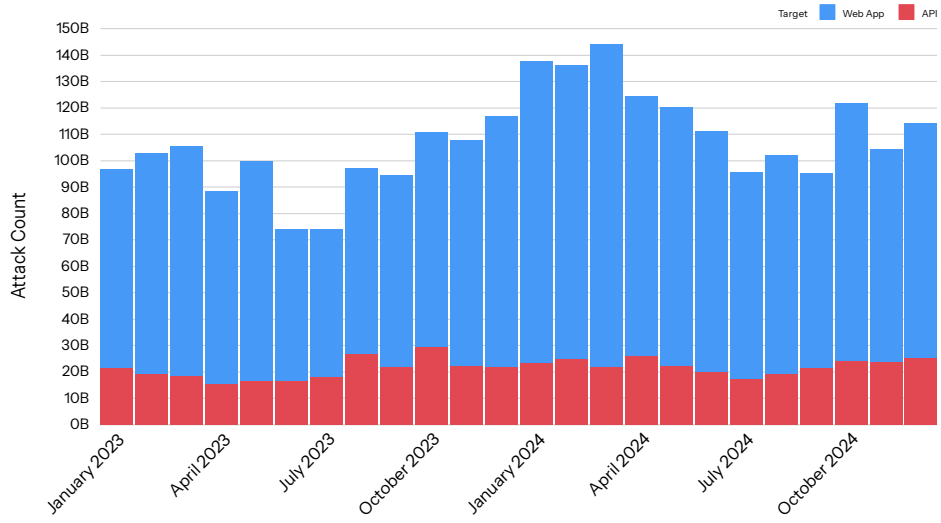
APJ: Monthly Layer 7 DDoS Attacks

January 1, 2023 – December 31, 2024



EMEA: Monthly Layer 7 DDoS Attacks

January 1, 2023 – December 31, 2024



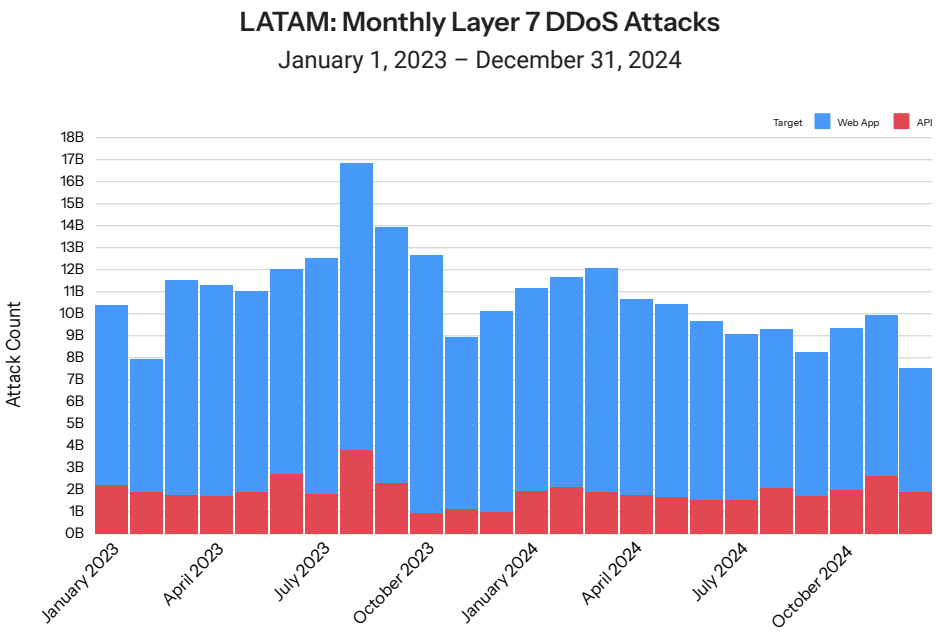


Fig. 15: Layer 7 DDoS attacks were on the rise in APJ and EMEA, whereas attacks in LATAM declined in 2024

APJ experienced 66% year-over-year growth in Layer 7 DDoS attacks and reached a 24-month high, peaking at 504 billion in December 2024. The growth was primarily driven by attacks focused on the social media industry.

In EMEA, Layer 7 DDoS attacks peaked in March 2024 at nearly 145 billion and, after a drop, resumed climbing, realizing 20% year-over-year growth. This can be attributed to a confluence of geopolitical and technological factors. Ongoing tensions in the region have fueled hacktivist activities. This trend is exacerbated by the rise of AI-enhanced tools and DDoS as a service platforms, which have lowered the barrier to entry for cybercriminals.

LATAM experienced a significant increase in Layer 7 DDoS attack attempts earlier in the reporting period, which coincided with an increase in HTTP flood attacks aimed at overwhelming API resources (an attack vector discussed in more detail in the Layer 7 DDoS attacks: Year-over-year comparison and trends section. Activity peaked in August 2023 at 16.8 billion and then declined during the remainder of the period to bottom out at 7.5 billion, marking a 15% year-over-year decrease in attacks.

Layer 7 DDoS attacks: Top targets

Within each region, we observed little to no change to the areas and industries targeted by threat actors as compared with our previous Layer 7 DDoS attack analysis.

In APJ, Singapore experienced the highest concentration of attacks at 4.7 trillion, followed by India (1.1 trillion), South Korea (607 billion), Indonesia (283 billion), China (246 billion), Japan (111 billion), Australia (108 billion), and Taiwan (81 billion).

In EMEA, the countries with the highest number of Layer 7 DDoS attacks were Germany (569 billion) and the United Kingdom (506 billion), followed by Israel (205 billion), Sweden (193 billion), and Malta (160 billion). Italy (158 billion), Switzerland (147 billion), France (129 billion), the Netherlands (111 billion), and Spain (96 billion) rounded out the top 10.

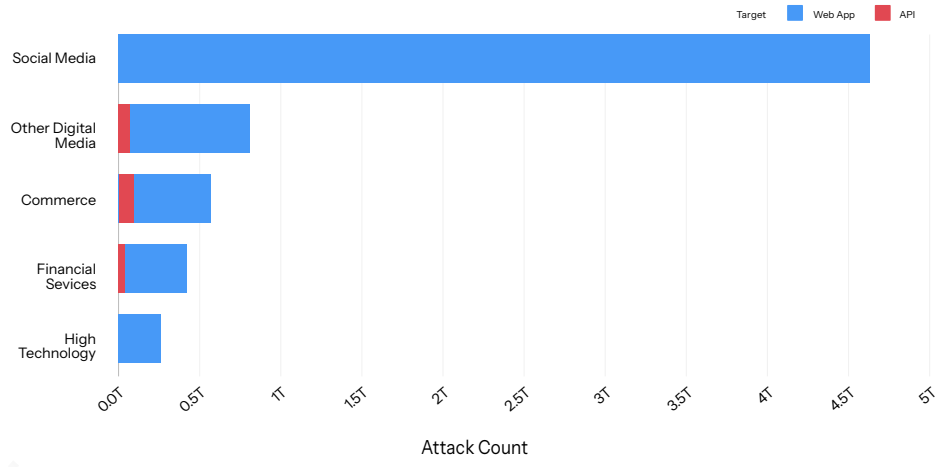
In LATAM, Brazil experienced the highest concentration of Layer 7 DDoS attacks at 175 billion, followed by Mexico (39 billion) and Costa Rica (19 billion).

Industry targets

The top industries impacted by Layer 7 DDoS attacks in APJ and EMEA (Figure 16) have not changed since our previous secure apps SOTI report. As we discussed in greater detail in that report, Layer 7 DDoS attacks on social media platforms in APJ surged from January 2023 through June 2024 in correlation with broader military conflicts and highly mediated electoral events worldwide — which is not surprising since social media platforms receive heavy traffic volumes during times of geopolitical upheaval. As anticipated, the trend intensified during the remainder of 2024 due to elections in both APJ and the United States. These factors contributed to the 130% year-over-year growth in attacks on the sector.

APJ: Layer 7 DDoS Attacks by Industry

January 1, 2023 – December 31, 2024



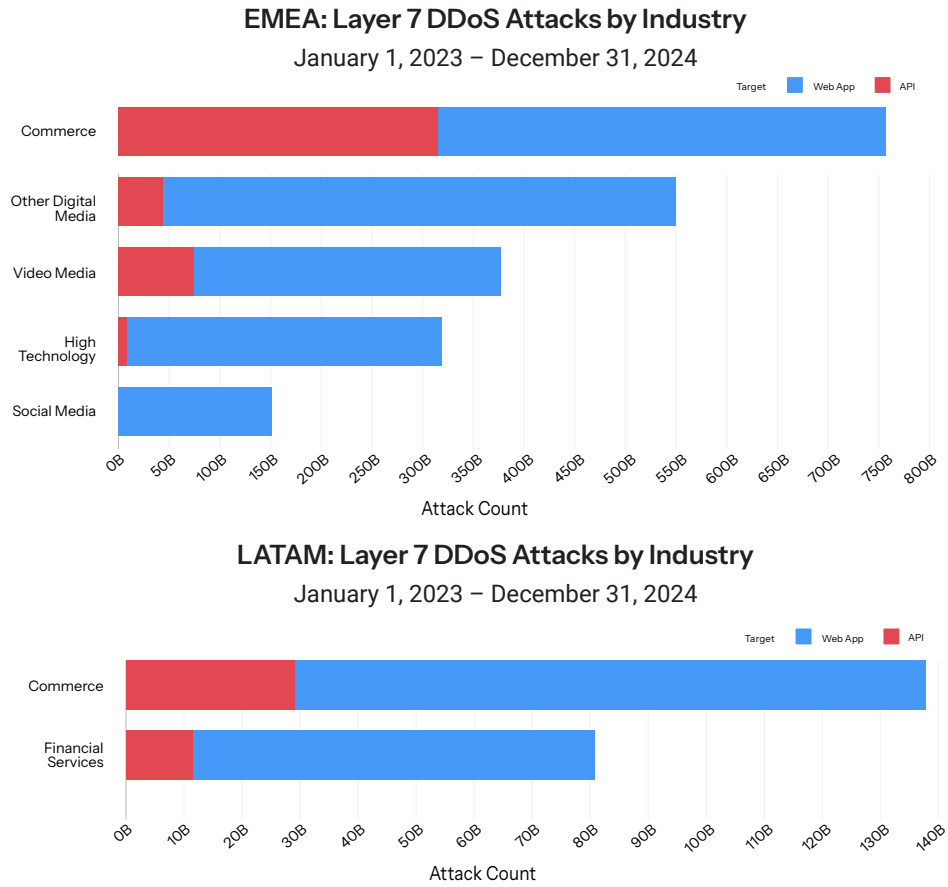


Fig. 16: The top impacted industries per region remained unchanged since our past analysis; commerce was consistently the industry that was most targeted by Layer 7 DDoS attacks on APIs

In EMEA, commerce remained the most impacted industry for Layer 7 DDoS attacks, followed by other digital media and video media. The industries that experienced the greatest year-over-year growth in these attacks included high technology (70%), social media (23%), and commerce (14%). These shifts show how quickly attackers can change their focus among industries and regions and illustrate that it is worth tracking broader trends.

Commerce was also the top targeted industry in LATAM for Layer 7 DDoS attacks, with financial services second. During the reporting period, ongoing levels of Layer 7 DDoS attack activity remained fairly consistent across industries.

Reflecting the global trend, among the industries most targeted by Layer 7 DDoS attacks, the commerce industry experienced the highest concentration of attacks on APIs in each region. In EMEA, 43% of attacks against commerce targeted APIs, 21% in LATAM, and 16% in APJ.

For reasons including the geopolitical upheaval and the potential economic impact of disruptions to highly visible services, commerce, media, and financial services have been prime targets for Layer 7 DDoS attacks in EMEA and LATAM over the past two years. See the Industry trends section for a detailed discussion of the drivers and methods behind the high level of activity against the commerce and financial services industries.

Compliance

Global and North America perspective

The global cybersecurity landscape in 2025 is characterized by unprecedented complexity and volatility. Geopolitical tensions, particularly the ongoing conflicts in Ukraine and the Middle East, have intensified cyberthreats and state-sponsored attacks. The rise of hacktivism, especially from pro-Russian groups targeting Western nations, has further complicated the threat landscape. Economically, the rapid digital transformation across industries has expanded the attack surface, with cybercriminals increasingly targeting critical infrastructure and leveraging advanced technologies like AI to enhance their capabilities.

These factors, combined with the global economic pressures and political shifts in key countries, have created a perfect storm for cybersecurity professionals worldwide. Protecting web applications and APIs is an essential challenge for organizations. Efforts by ethical hackers, cybersecurity professionals, and organizations such as Akamai to address the imperative of securing these entry points complement rising compliance considerations.

Regulatory bodies around the world are implementing more stringent cybersecurity compliance requirements for applications. In North America, the focus has shifted toward comprehensive risk management strategies and mandatory incident reporting. The Cyber Incident Reporting for Critical Infrastructure Act in the United States, which is expected to go into effect in 2026, mandates that critical infrastructure organizations inventory their information systems, categorize cyber risks, and assess their cybersecurity posture at least annually. This act emphasizes the need for robust security measures in applications, particularly those used in critical sectors such as energy, chemical manufacturing, and information technology.

Similarly, Canada and Mexico are aligning their regulations with international standards, focusing on data protection and critical infrastructure security. While specific regulations vary, the global trend is toward more rigorous security requirements for applications, including enhanced input validation, secure development practices, and regular security audits.

The API security landscape is experiencing parallel challenges, with APIs becoming prime targets for cybercriminals because of their critical role in enabling service integration and data exchange. Regulatory bodies worldwide are responding by introducing more stringent regulations that require organizations to implement robust API security measures.

These include mandatory continuous API discovery, monitoring, and protection against evolving threats. In North America, the focus is on thorough risk assessments of API ecosystems, emphasizing secure development practices, robust authentication mechanisms, and real-time threat detection capabilities. The rapid adoption of AI-driven SaaS tools, often integrated via APIs, has significantly expanded the attack surface, prompting regulators to demand more sophisticated security approaches.

As the complexity of API environments grows, particularly with the rise of AI and machine learning applications, compliance requirements are evolving to mitigate risks associated with data breaches, unauthorized access, and service disruptions. While regions like APJ, LATAM, and EMEA are developing their own specific regulations, the global trend is toward harmonization of API security standards to address the interconnected nature of modern digital architecture.

APJ perspective

The APJ region is experiencing a significant shift in its regulatory landscape, with new compliance mandates that are impacting organizations across various sectors. In Singapore, recent amendments to its cybersecurity bill have expanded the scope to include both physical and virtual critical information infrastructure systems, including those hosted on cloud platforms and located overseas. Japan has updated its National Center of Incident Readiness and Strategy for Cybersecurity laws, while India has overhauled its IT Act with the passing of the Digital Personal Data Protection Bill. Australia has introduced its 2023–2030 Cyber Security Strategy, further emphasizing the region's focus on strengthening cybersecurity measures. As part of that strategy, amendments were made during late 2024 to the Australian Security of Critical Infrastructure Act and a new Cyber Security Act 2024 became law; enforcement will now include secondary assets like IoT devices, applications, and APIs that process sensitive data. These regulatory changes are compelling organizations to reassess and enhance their web application security practices, with a particular emphasis on protecting critical infrastructure and sensitive data.

The PCI DSS v4.0.1 is set to have a significant impact on organizations that handle payment card data; the compliance deadline was March 31, 2025. This new version introduces more stringent requirements for web applications, including the implementation of controls for all payment page scripts executed in consumers' browsers and the use of automated technical solutions to continually detect and prevent web-based attacks. Organizations in the APJ region must now conduct thorough gap analyses, update their security policies, and implement necessary technical changes to meet these enhanced security standards for their web applications.

In terms of APIs, the APJ region is witnessing a growing emphasis on API security, partly driven by the increasing adoption of open banking initiatives. Although the region has not yet fully embraced open banking regulations to the extent seen in EMEA, there is an opportunity for APJ countries to proactively address API security concerns. An August 2024 survey of API security insights from this region highlights that internal APIs are the most commonly used, but external user access remains the primary concern for API access control. This indicates a need for organizations to implement robust API security measures, including strong authentication and authorization protocols, data encryption, and continuous API discovery and monitoring. As the region moves toward open banking directives, organizations will need to prioritize API security to ensure compliance with evolving regulations and protect against emerging threats.

EMEA perspective

The cybersecurity landscape in EMEA is undergoing significant transformation, driven by a complex interplay of geopolitical tensions, technological advancements, and regulatory shifts. The region faces unique challenges, with ongoing conflicts in Ukraine and the Middle East intensifying cyberthreats and state-sponsored attacks. Additionally, the rise of hacktivism, particularly from pro-Russian groups that are targeting European countries, has made the region a prime focus for politically motivated cyber operations.

The API landscape within EMEA is experiencing parallel challenges. APIs have become prime targets for cybercriminals because of their critical role in enabling service integration and data exchange. And the rapid adoption of AI-driven SaaS tools, often integrated via APIs, has significantly expanded the attack surface.

In response to these escalating threats, the European Union has introduced a suite of comprehensive cybersecurity regulations. The updated Network and Information Systems (NIS2) Directive, effective from January 2025, significantly expands its scope to include 18 critical sectors, mandating stringent cybersecurity measures for medium and large entities.

For the financial sector, the Digital Operational Resilience Act (DORA), enforced from January 17, 2025, supersedes NIS2, requiring robust information and communication technology risk management frameworks, incident reporting mechanisms, and digital operational resilience testing programs for applications used in financial services. In addition, the PCI DSS v4.0.1, which became mandatory on March 31, 2025, introduces new compliance requirements centered on evolving security needs, continuous security processes, flexible methodologies, and enhanced validation procedures. The upcoming revised EU Payment Services Directive (PSD3) aims to address shortcomings in PSD2 by tightening data-sharing mechanisms, reinforcing security requirements, and enhancing oversight in the financial services sector.

The Cyber Resilience Act (CRA). which entered into force on December 10, 2024, introduces mandatory cybersecurity standards for products with digital elements sold in the European Union, requiring manufacturers to implement security measures throughout a connected product's lifecycle. For application developers and users, the CRA encompasses smartphones and tablets as significant risk vectors. This inclusion necessitates that organizations treat mobile terminals as fundamental components of their overall cybersecurity strategy, implementing rigorous security measures throughout the application lifecycle.

In the United Kingdom, the upcoming Cyber Security and Resilience Bill will improve U.K. cyber defenses and protect essential public services. The bill's crucial updates to the legacy regulatory framework will expand the scope to protect more digital services and supply chains, strengthen enforcement, and increase reporting requirements.

LATAM perspective

The cybersecurity landscape in LATAM is rapidly evolving, shaped both by global technological trends and by economic and political challenges unique to the region. In this context, the rapid digital transformation across LATAM countries, coupled with the vulnerabilities of increasingly interconnected systems, has made the region an attractive target for cybercriminals and state-sponsored actors alike. The commerce and financial services sectors have emerged as prime targets for cyberattacks. Online retailers, payment processors, banks, insurance companies, fintech startups, and cryptocurrency exchanges are particularly vulnerable to threats that target their digital infrastructure, especially their web applications and APIs.

LATAM countries recognize these challenges and are making significant strides in developing and implementing cybersecurity regulations, with a growing focus on web application and API security. Brazil has taken a leading role with the implementation of the Lei Geral de Proteção de Dados Pessoais (LGPD), which came into effect with stringent requirements for data protection and security. Although it does not specifically address web applications or APIs, the LGPD has driven organizations to enhance their overall cybersecurity posture, including the security of their digital interfaces.

Similarly, Chile has enacted its Framework Law on Cybersecurity, which came into force on January 1, 2025. This law establishes the National Cybersecurity Agency and outlines comprehensive measures to prevent, report, and resolve cybersecurity incidents across various sectors, including those heavily reliant on web applications and APIs. Also in January 2025, Argentina published its Federal Plan for the Prevention of Cybercrime and Strategic Management of Cybersecurity (2025–2027).

There are promising developments in the realm of API-specific regulations. Mexico, for instance, has implemented legislation focusing on the financial sector, including fintech, with detailed requirements for credit bureaus and clearinghouses to develop secure APIs. This approach reflects a growing recognition of the critical role APIs play in modern digital ecosystems and the need for targeted security measures. Additionally, the Federal Law on the Protection of Personal Data Held by Private Parties in Mexico regulates the processing of personal data and establishes obligations for companies and organizations.

Colombia has also been advancing its regulatory framework, expanding its legal scope by releasing public policy on cybersecurity for public institutions, and creating a digital security risk management system with different levels of incident response reporting. While not exclusively focused on APIs, these measures will inevitably impact API security practices within organizations.

Across the region, there is a growing trend toward adopting industry-specific initiatives, such as open finance frameworks, which set API security standards to protect consumer data. These frameworks are particularly relevant in the financial sector, where the security of APIs is crucial for maintaining the integrity of financial transactions and protecting sensitive customer information. As LATAM countries continue to prioritize security advancements and align their cybersecurity regulations with international standards, we can expect to see more comprehensive and specific guidelines emerge for web application and API security.

Mitigation

In an evolving threat landscape with more sophisticated attack techniques on the rise, protecting web applications and APIs is an essential challenge for organizations. Some of the safeguarding and mitigation techniques we recommend include:

- **Establish a comprehensive API security plan:** Implement a shift-left and DevSecOps approach, integrating security from API design through post-production. Ensure continuous discovery and visibility to understand the full attack surface, including hidden APIs (shadow, legacy, and zombie APIs). Strengthen security with strict authentication and authorization (OAuth 2.0, mTLS, role-based access control/attribute-based access control), rate limiting, and bot mitigation to prevent abuse. Implement real-time threat detection, anomaly monitoring, and runtime protection to identify and stop attacks as they happen. Ensure compliance with regulations like DORA, GDPR, HIPAA, NIS2, and PCI DSS while enforcing API governance policies to maintain security at scale.
- **Implement robust cybersecurity measures:** Use an adaptive security engine that continuously monitors and responds to threats in real time and provides threat intelligence and runtime protection. Also use API testing tools like dynamic application security testing (DAST) to help ensure that security requirements — including secure access, encryption, and authentication — are met.
- **Take a proactive defense against threats:** Use specialized DDoS protection tools, configure rate limiting and CDN caching, and implement measures like patch management, access control policies, and network segmentation. Also protect DNS infrastructure with continuous traffic monitoring and hybrid platforms.
- **Mitigate API vulnerabilities:** Follow established security guidelines, such as those provided by OWASP, to ensure robust API security and address the risks of poor coding practices and misconfigurations in API architecture, which can create exploitable vulnerabilities that allow hackers to gain unauthorized access or manipulate data.

- **Defend against ransomware threats:** Use a layered approach to combat ransomware. Implement Zero Trust solutions to block malicious traffic, use microsegmentation for detailed visibility and precise access control, and leverage the MITRE ATT&CK framework to understand attack patterns and enhance response strategies.
- **Be prepared for AI:** Employ a comprehensive defense strategy that includes bot defense solutions, AI-powered security tools, specialized firewalls, and proactive measures like continuous assessments and Zero Trust models to address the new security risks introduced by the increasing use of AI. Secure AI systems with a multifaceted approach: Address specific threats, such as prompt injection and data poisoning, through awareness of models and datasets; perform proactive vulnerability testing; and use robust defenses like behavioral monitoring, content validation, and automated attack responses that are integrated across both development and runtime environments.

Methodology

Web application and Layer 7 DDoS attacks

This data describes application-layer alerts on traffic seen through our web application firewall (WAF). The web application attack alerts are triggered when we detect 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 a high level of customization, we collected the data presented here in a manner that 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.

This data covered the 24-month period from January 1, 2023, through December 31, 2024.

API security attack data

Akamai's integration of Noname Security has enhanced our API threat research and reporting capabilities. This dataset is still in the early stages of integration and analysis. For this report, we took a 30-day data sample from Q1 2025 to analyze the breakdown of API security alerts according to their corresponding security frameworks and compliance standards. This dataset will continue to progress and provide an expanded view of API security issues in the future.

Credits

Research director

Mitch Mayne

Editorial and writing

Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Maria Vlasak

Review and subject matter contribution

Tom Emmons
Reuben Koh
Richard Meeus
Stas Neyman
Steve Winterfeld

Data analysis

Chelsea Tuttle

Promotional materials

Barney Beal
Ashley Linares

Marketing and publishing

Georgina Morales Hampe
Emily Spinks

State of the Internet/Security

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

Akamai threat research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research. akamai.com/security-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.com/sotidata

Akamai security research

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

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, formerly known as Twitter, and LinkedIn. Published 04/25.