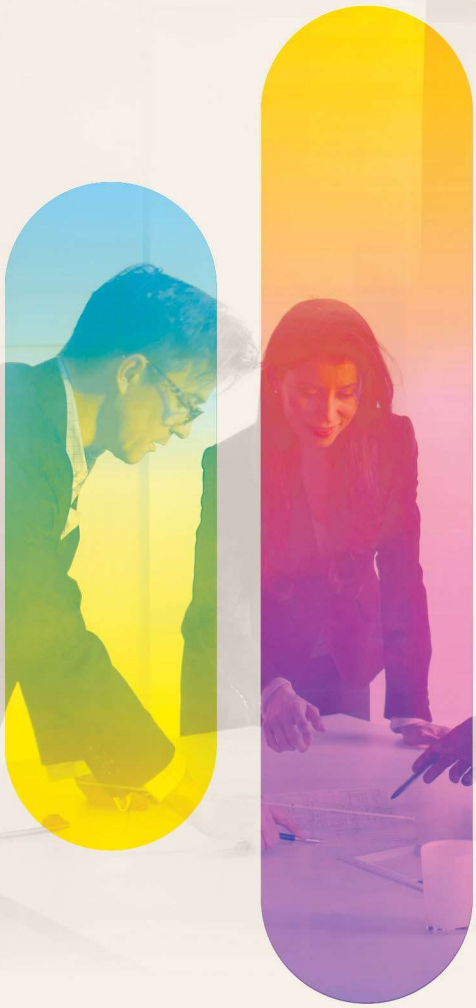
datos INSIGHTS

October 2025

Securing Financial Services in the Age of Risk: Protecting Multicloud Environments

Jane Ginn



This report provided compliments of:

f5®

October 2025

Securing Financial Services in the Age of Risk: Protecting Multicloud Environments

Jane Ginn

Table of Contents

List of Figures

List of Tables

Summary and Key Findings

The transformation of financial services through open banking and digital innovation has created an unprecedented expansion in attack surfaces at financial institutions, insurance carriers, and other financial services firms. Explosive growth has outpaced security teams' ability to maintain adequate protection. Traditional perimeter security models, designed for monolithic applications within clearly defined network boundaries, have become obsolete in today's hybrid multicloud environments. A shift from unauthenticated, perimeter-based cyberattacks to authenticated-user cyberattacks is a significant development in threat vectors with fundamental implications for how organizations must approach security defenses.

In response to these challenges, the web application and API protection (WAAP) security services market has experienced substantial growth, expanding from US$10 billion in 2025 toward a projected US$25 billion by 2033. Modern WAAP solutions have evolved beyond reactive security measures to incorporate sophisticated artificial intelligence (AI)-powered capabilities.

Several emerging trends will shape the future of application and API security:

- The AI race continues to escalate. Attackers and defenders are leveraging AI for increasingly sophisticated operations.
- Moving-target defense is a paradigm shift in security strategy.
- Advanced WAAP platforms now incorporate machine-learning (ML) models that continuously update their understanding of normal behavior patterns, enabling them to detect previously unknown attack vectors for web apps and APIs.

Organizations that embrace these emerging capabilities early will be better positioned to defend against evolving threats while maintaining the agility and innovation required to compete in digital markets. The ultimate objective is to anticipate and prevent threats to web applications and APIs, creating security architectures that enable rather than constrain business innovation.

Introduction

The financial services industry is at a critical inflection point: Open banking and digital transformation imperatives are colliding with an expanding threat landscape. Fifty-seven percent of organizations responding to a Q3 2025 Datos Insights' survey reported experiencing API-related breaches in the past two years. Interestingly, many of these respondents operate in multicloud environments, where they depend on their providers to provide basic security. This strategy has failed them.

A comprehensive WAAP strategy has become important for meeting operational and security objectives and addressing this issue proactively. WAAP services are designed to address the contingencies of managing multicloud environments, providing a single dashboard for managing the security of web applications and API configurations.

The many vulnerabilities in the APIs that financial services companies use are a fundamental risk to business continuity in the event of an undetected intrusion leading to a data breach. Customer trust in a business's ability to protect their data becomes a fundamental business imperative. The increasingly interconnected financial ecosystem needs comprehensive protection for the entire digital estate throughout the API lifecycle.

This report provides an overview of WAAP security requirements specifically tailored to the sector's unique operational and regulatory environment. The analysis encompasses three critical dimensions:

- The evolving threat landscape specific to financial services
- Emerging trends, including advanced AI implementations used by threat actors to harvest data from their victims
- The technical features of modern WAAP solutions and their integration with existing multicloud security infrastructures

The scope of this analysis extends beyond traditional web application security to encompass the full spectrum of API protection requirements, from discovery and inventory management through runtime protection and post-incident forensics. Special attention is devoted to the emerging standards driving API security and the evolving landscape of open banking mandates.

Methodology

The research methodology for this study employed a multifaceted approach to analyze the regulatory landscape and technological solutions in the financial services sector. Desk studies were conducted by this analyst, encompassing a review of government agency threat intelligence data, regulatory agency rules, legal mandates, the FDX API standard, vendor product briefs, and previous Datos Insights market analyses. This documentary research provided a solid foundation for understanding the current market environment and the available security solutions in the API and WAAP markets.

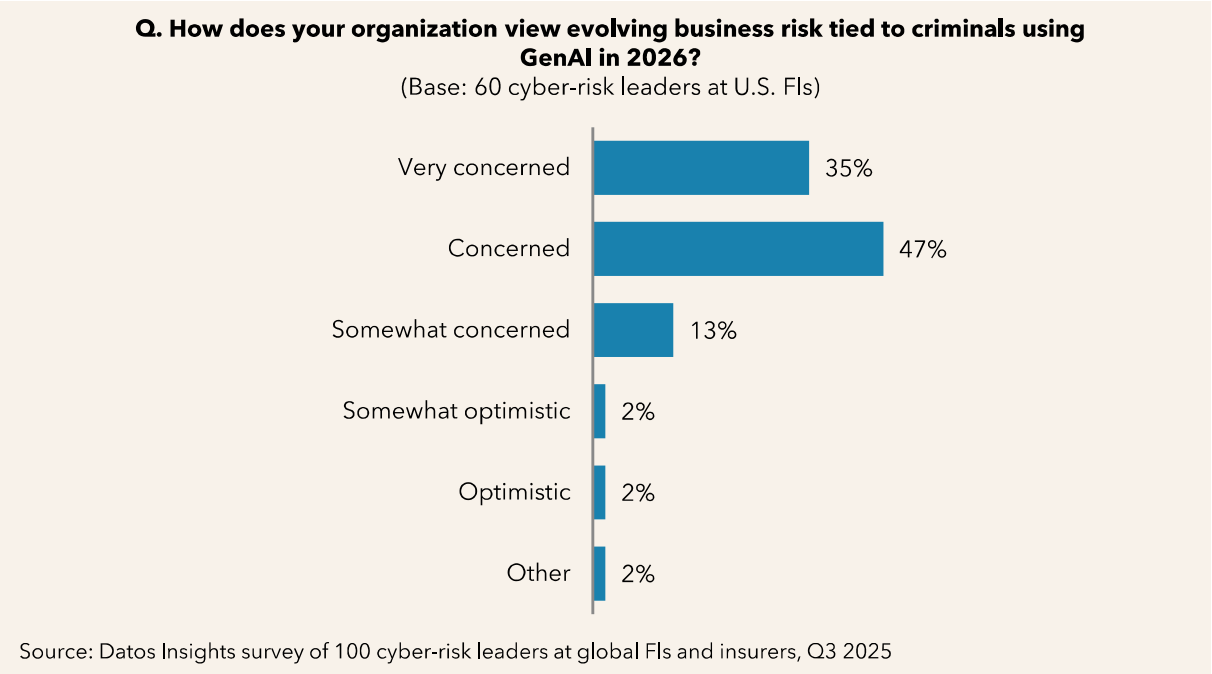
To complement the theoretical framework, Datos Insights designed and implemented a survey for CISOs, CTOs, and program owners within the financial services sector. The survey, which garnered responses from over 60 CISOs and cyber-risk leaders at North American financial institutions (FIs), aimed to gauge their budgeting priorities for 2026. The findings offer valuable insights into the strategic focus areas and practical challenges that industry leaders will face in 2026. Given the size and structure of the sample, the survey results in this report are considered a directional indication of market conditions.

Datos Insights' combination of research and primary data collection enabled a robust analysis of the intersection between technological innovations and financial services industry priorities within the context of open banking/open finance, as well as digital transformation for insurance carriers.

Emerging Trends

The most significant emerging trend in API security is the bidirectional evolution of AI in cybersecurity. According to Datos Insights' Q3 2025 survey of 60 U.S. risk leaders, 35% are very concerned about criminal use of generative AI (GenAI), and another 47% are concerned (Figure 1).

Figure 1: Sentiment on Business Risk Tied to Criminals Using AI



Source: Datos Insights survey of 100 cyber-risk leaders at global FIs and insurers, Q3 2025

This sentiment has accelerated investment in AI-powered defense mechanisms that can match the sophistication of AI-enabled attacks.

The AI Arms Race: Attack and Defense Evolution

Advanced WAAP platforms are now incorporating ML models that continuously evolve their understanding of normal behavior patterns, enabling the detection of previously unknown attack vectors. These systems leverage behavioral analytics not just for anomaly detection, but for predictive threat modeling that can anticipate attack patterns before they fully manifest.

The integration of large language models (LLMs) into security operations enables the creation of natural language policies, democratizing advanced security capabilities across organizations with varying technical expertise. Automated threat analysis can be

significantly enhanced by leveraging linked data analysis, which is built on various global open-access databases, such as the MITRE ATT&CK framework, for active analysis and defense. A specific example of how this is accomplished is provided later in this report.

The following analysis of trends, based on data from the Key Exploited Vulnerabilities (KEV) database and the Common Vulnerabilities and Exposures (CVE) database from DHS/CISA, shows alarming developments over time (Table A).

Table A: Four-Year Trend in the Growth of Attacks Against APIs

Year	Total CVEs	Year-over-year change	Percentage critical/ high severity	Key observations
2021	53	-	32%	• Baseline year
2022	642	+1,111%	72%	• Massive 3.7-times quarterly growth in Q2 • APIs became the primary attack surface
2023	1,090	+70%	56%	• Volume peaked • Severity remained consistently high
2024	674	-38%	61%	• Decreased total as threat actors shifted to AI vulnerabilities • Increased severity

Source: CVE database, KEV database

The following are other notable insights:

- **Q1 2025 projection**: Eight CVEs recorded, with a projection of 32 for the full year; 63% critical or high severity.
- **Time-to-exploit acceleration:** By Q4 2022, exploits were being published an average of three days before CVE assignment (negative time-to-exploit).
- **Trend analysis:** The data shows a clear evolution from rapid volume growth (2022) to quality/severity focus (2024).

Datos Insights also found that AI-related vulnerabilities emerged as a major new threat vector. This data will be provided in a subsequent section of this report.

Moving-Target Defense: Dynamic Security Architectures

Moving-target defense is a paradigm shift from static security postures toward dynamic, adaptive protection mechanisms. Advanced WAAP implementations now incorporate dynamic endpoint rotation, API schema randomization, and adaptive authentication mechanisms that continuously alter the attack surface. These systems can automatically adjust security policies, modify API endpoints, and reconfigure protection mechanisms based on threat intelligence and attack patterns. Moving-target defense makes targeted campaigns by threat actors significantly more difficult to execute and maintain.

Advanced Threat Intelligence Integration

Modern WAAP solutions are evolving beyond reactive security measures toward proactive threat hunting capabilities powered by integrated threat intelligence platforms. These systems correlate internal security events with global threat intelligence feeds, enabling the identification of emerging attack patterns and the proactive adjustment of policies. The integration extends to automated threat attribution and campaign tracking, enabling security teams to understand not just individual attacks but coordinated campaign activities.

This capability is essential for defending against sophisticated threat actors who employ multi-vector attacks spanning extended time frames, as demonstrated by advanced persistent threat groups operating in the financial services sector. For example, North Korean hackers have become the most significant state-sponsored threat to the financial services sector, devoting a substantial portion of their cyber resources to exploiting the global financial market, with a growing focus on cryptocurrency. Their activities serve to generate revenue for the regime and circumvent international sanctions.

They are matched in sophistication by cybercriminal enterprises that deploy Ransomware-as-a-Service platforms and global affiliate networks. For example, the platform of a threat actor known as Dragonforce was made easily configurable for the development of language-specific phishing campaigns, ransomware demands, links to cryptocurrency wallets, and other features.

Platform Consolidation

The convergence of these emerging trends suggests a future WAAP market characterized by intelligent, adaptive security platforms that provide comprehensive protection across the application ecosystem. The most successful solutions will combine advanced AI capabilities with human expertise, providing automated protection against known threats while enabling security teams to focus on strategic threat hunting and incident response activities.

One of the questions in the Q3 2025 survey focused on the top two cybersecurity investments respondents planned to make in 2026. The top priority, improving data and cloud security defenses (35%), indicates that organizations recognize the inadequacy of perimeter-based security models in protecting distributed cloud environments and sensitive data assets (Figure 2).

Figure 2: Risk Managers' 2026 Priorities

Source: Datos Insights survey of 100 cyber-risk leaders at global FIs and insurers, Q3 2025

These 2026 cyber investment priorities reveal a strategic shift toward addressing the expanded attack surface created by cloud adoption, AI integration, and complex supply chains. The significant focus on third-party vendor risk management (25%) highlights a growing awareness of supply chain vulnerabilities, likely influenced by recent high-profile breaches resulting from vendor compromises.

The emergence of WAAP-enabled bot defenses and agentic AI security (23%) as a major investment area signals preparation for the next wave of automated threats, including AI-powered attacks and the need to secure nonhuman identities that are proliferating across digital ecosystems. While API security ranks fifth at 18%, this still represents a substantial investment.

Emerging Privacy and Data Protection Capabilities

As privacy regulations continue to evolve globally, WAAP platforms are incorporating advanced data protection capabilities that extend beyond traditional security functions. These include automated data classification, privacy policy enforcement, and consent management integration that ensures compliance with emerging data protection requirements.

Advanced implementations offer granular data access controls, automated data loss prevention, and capabilities for assessing the privacy impact. These capabilities enable organizations to maintain comprehensive data protection while supporting business operations and regulatory compliance requirements.

Evolving Security Paradigm

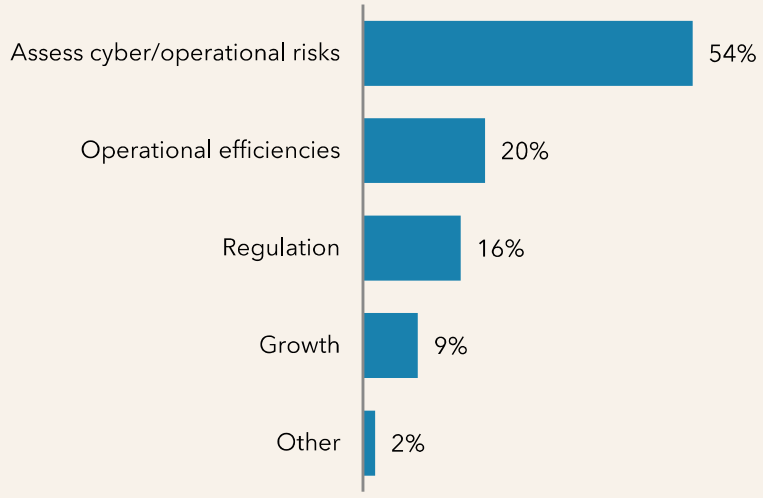
Traditional perimeter security models, predicated on clearly defined network boundaries, have become obsolete in the era of hybrid multicloud architecture. The shift toward open banking/open economy business models built on APIs and microservices architectures has fundamentally altered the attack surface. It has created "API sprawl," i.e., the proliferation of connected endpoints to third-party services that expand faster than security teams can manually protect.

This transformation is particularly pronounced in financial services, where customer demand for real-time payments has accelerated the adoption of APIs. Over 85% of banks have adopted open banking APIs, allowing third-party access to customer data for improved services. The average API call volume in financial services doubled from 2023 to 2024, reaching over 2 billion daily requests.

Cyber-risk leaders selected reducing risk and achieving operational efficiencies as the top drivers for improving web application firewall (WAF), WAAP, and API security solutions in 2026 (Figure 3).

Figure 3: Top Drivers for Improvements to WAF/WAAP/API Security

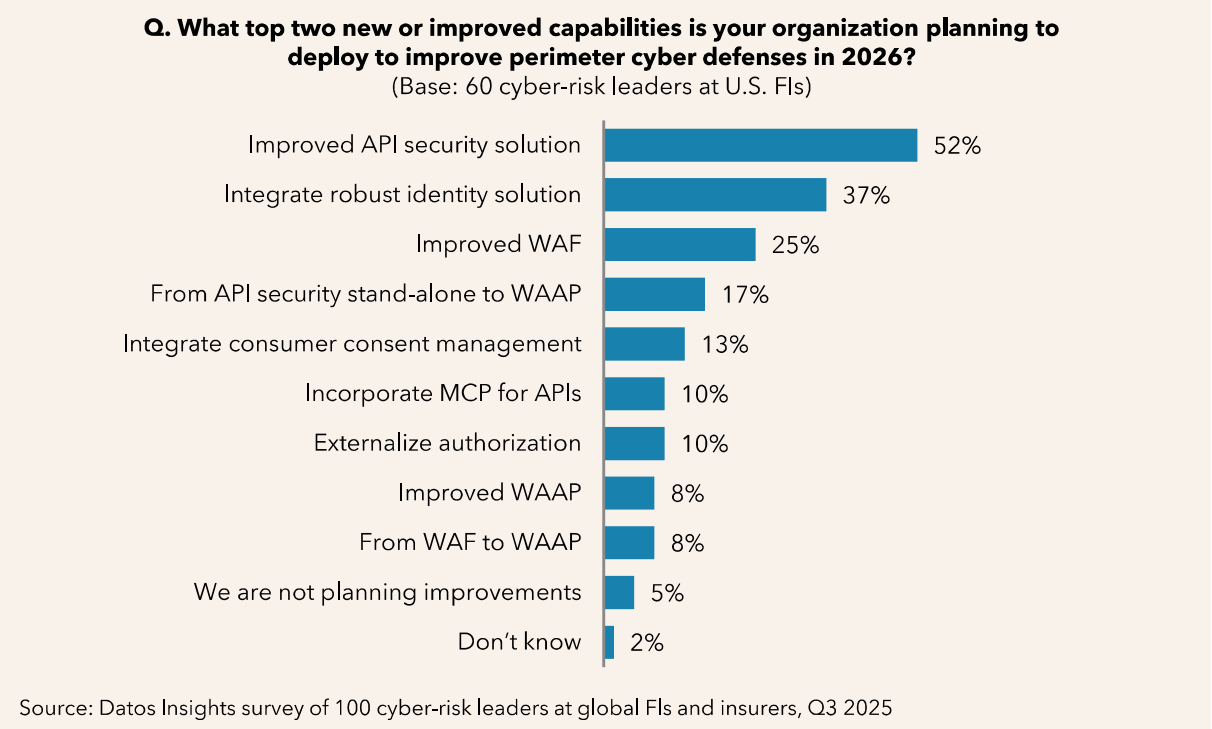
Q. What is your top driver for improving WAF/WAAP/API security solutions in 2026?
(Base: 56 cyber-risk leaders at U.S. FIs planning to improve perimeter cyber defenses)



Source: Datos Insights survey of 100 cyber-risk leaders at global FIs and insurers, Q3 2025

The sophistication of attacks has evolved in parallel with the larger attack surface that open banking has enabled. The shift from perimeter-based to authenticated-user attacks represents a fundamental change in threat vectors, requiring correspondingly sophisticated defense strategies. Given this threat environment, cyber-risk indicated that improving API protection was at the top of their lists for 2026 (Figure 4).

Figure 4: API Protection, Improved WAF, and Move to WAAP Are Top Priorities for 2026



Source: Datos Insights survey of 100 cyber-risk leaders at global FIs and insurers, Q3 2025

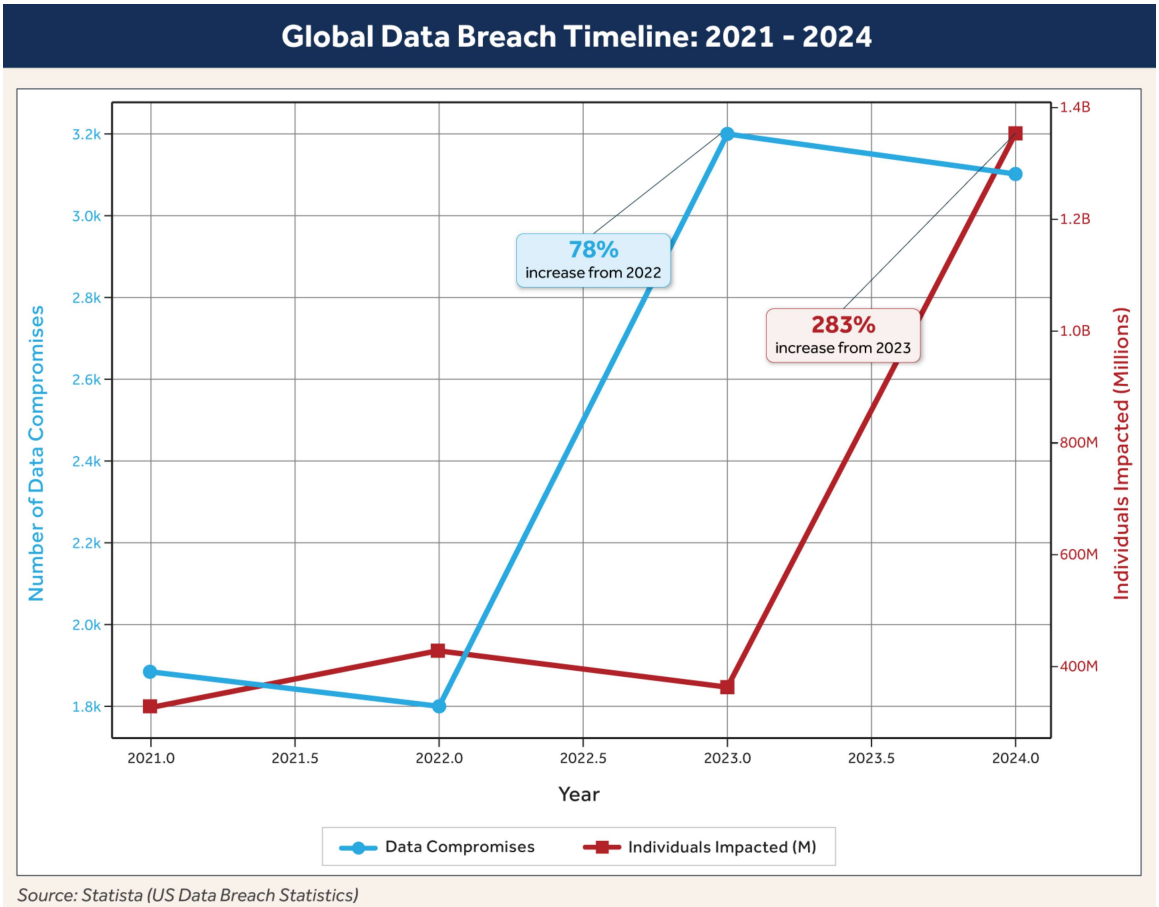
These findings reveal a significant shift in how organizations are approaching perimeter cyber defenses for 2026, with API security emerging as the dominant priority. The relatively lower emphasis on traditional WAF improvements (25%) suggests that organizations view legacy web application protection as insufficient for today's API-centric threat landscape.

This distribution of 2026 priorities demonstrates a clear market consensus: The perimeter has shifted from traditional web applications to APIs, and security strategies must evolve accordingly to protect these now-critical business assets. The rapid adoption of API calls to external services has created a security gap that threat actors are exploiting with increasing frequency. These realities have given rise to a very robust market for API security and WAAP products. The Threat Intelligence Imperative

Contemporary threat analysis reveals trends in attack sophistication and frequency. The financial impact extends beyond direct losses to encompass operational disruptions, regulatory penalties, and reputational damage that can persist for years. The sector is constantly targeted, as are the APIs that create a robust open banking system.

The introduction of LLMs, ML algorithms, and domain-specific agents has had a significant impact on the threat landscape. Datos Insights reviewed trends from 2021 to 2024, finding a surprising increase in the number of companies reporting data breaches and an increase in the number of individual records that have been harvested. Many of these records are encrypted using current cryptographic methods (e.g., RSA 2048, ECC) that have been effective for decades in classical computing for data at rest. This threat vector is referred to as the "harvest now, decrypt later" attack. According to aggregate data, these breaches affected 1.35 billion individuals in 2024—the highest on record (Figure 5).

Figure 5: Global Data Breach Timeline, 2021 to 2024



Source: Statista (US Data Breach Statistics)

The Figure 5 data were compiled from the annual Verizon Data Breach Investigation Reports, the FBI's Internet Crime Complaint Center, the Privacy Rights Clearinghouse, and Statista.

The FBI's Internet Crime Complaint Center, in affiliation with the NSA, CISA, and others, finds that state-sponsored cyber actors from the People's Republic of China are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the U.S. The joint advisory was released in collaboration with agencies from the Five Eyes alliance countries and other U.S. government partners.[1]

The following are key elements of the warning:

- **Persistent access:** U.S. authoring agencies have recently observed indications that Volt Typhoon actors have maintained access and footholds within some victim IT environments for at least five years. This finding demonstrates the threat actor's commitment to long-term, undetected persistence within critical infrastructure networks.[2]
- **"Living off the land" techniques:** These are a hallmark of Volt Typhoon actors' malicious cyber activity when targeting critical infrastructure. The group also relies on valid accounts and leverages strong operational security; combined, these enable long-term undiscovered persistence. This approach allows them to blend in with normal system behavior and avoid detection.[3]

AI-Powered Attacks Combined With Social Engineering

The emergence of AI-powered attack methodologies has introduced additional complexity to the threat landscape. Threat actors increasingly leverage AI for reconnaissance, vulnerability discovery, and attack automation. At the same time,

---

1 "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System," Internet Crime Complaint Center, September 2025, accessed September 23, 2025, https://www.ic3.gov/CSA/2025/250827.pdf.

2 "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," Cybersecurity and Infrastructure Security Agency, February 7, 2024, accessed September 23, 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

3 "People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection," Cybersecurity and Infrastructure Security Agency, May 24, 2023, accessed September 23, 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a.

defenders must protect against these advanced techniques while securing their AI-driven applications and services.

In a recent development to the risk landscape, a threat actor group with exceptional English language skills and a questionable moral compass has emerged. Characterized as Scattered Spider, these young miscreants have targeted multiple high-profile targets, including several financial services companies.

Their modus operandi depends on social engineering help desk personnel for initial access. They then exploit APIs in the victim's architecture to move laterally and gain access to an organization's crown jewels: customer data. These data are then exfiltrated and used as a basis for demanding a ransom payment to avoid public release.

Attack Pattern of Scattered Spider

A 2025 campaign by this threat group, as documented by Datos Insights, shows that it weaponized a single-sign-on (SSO) API for initial entry. It then used a Windows-based exploit of the Sender Message Block tool, which system administrators use for network-wide visibility and maintenance.

A well-designed and configured WAAP would have provided the security team with visibility into the intrusion by dynamically detecting the rogue SSO API, enabling the team to circumvent subsequent lateral movement and data exfiltration by the threat actor within the organization's network.

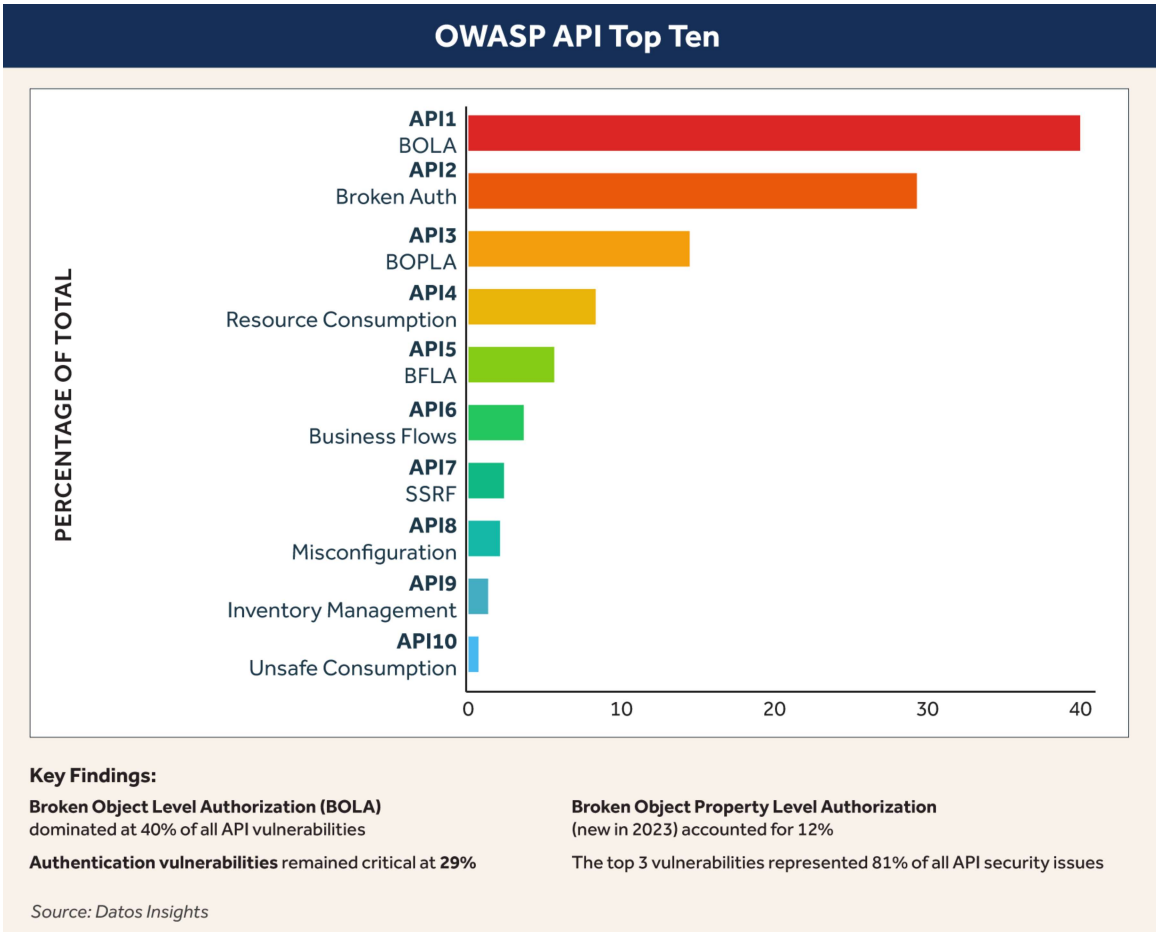
Calling on Community Resources to Support Threat Intelligence Trends

On the defender side, the Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve software security through community-led open-source projects. OWASP is best known for its Top 10 lists that identify the most critical security risks to web applications, including the OWASP API Security Top 10. The API attack patterns are fully described at the OWASP website.[4]

The frequency of attack patterns is useful for understanding the growing threat. The key attack vectors for API vulnerabilities are broken object-level authentication, shown below as "BOLA," at 40% and broken authentication at almost 30% (Figure 6)

[4] "OSWAP Top 10 API Security Risks – 2023," OSWAP, 2023, accessed September 23, 2025, https://owasp.org/API-Security/editions/2023/en/0x11-t10/.

Figure 6: OWASP API Security Top 10 Attack Patterns in 2023



Broken object property level authorization (shown as BOPLA) ranks third, accounting for over 10% of the attacks. These top three vulnerabilities represented 81% of all API security issues. Cybersecurity development teams should focus on getting these configurations right.

Importantly, WAAP solutions are evolving beyond reactive security measures toward proactive threat hunting capabilities powered by integrated threat intelligence platforms. These systems correlate internal security events with global threat intelligence feeds, enabling the identification of emerging attack patterns and the proactive adjustment of policies.

Recognizing the three key elements of modern API security—multicloud environments, open banking imperatives, and the expanded attack surface—is the first step in assessing the true value of a WAAP solution.

Jane Ginn, Cybersecurity Fellow

This integration also requires a well-designed and responsive architectural transformation that integrates security information and event management platforms, threat intelligence platforms, and security orchestration, automation, and response platforms. Coupled with WAAP, these tools provide security teams with the visibility they need to respond to threats left of boom and execute playbooks for rapid response if an intrusion is detected.

Architectural Transformation

The transition to hybrid multicloud environments has fundamentally altered the security architecture requirements for financial services organizations. Legacy security models, designed for monolithic applications within well-defined network perimeters, have proven inadequate for protecting distributed microservices architectures spanning multiple cloud providers and on-premises infrastructure.

WAAP solutions integrate several critical security components to provide layered defense for digital assets. This integration combines WAF capabilities, bot management systems, and distributed denial-of-service (DDoS) protection into a unified security framework that encompasses web application and API security. A typical WAAP filters requests through a rigid sequence to ensure each signal is properly interpreted.

The HTTP journey begins with client requests (from mobile devices or computers) passing through the internet to an API gateway; this is the first line of defense. Here, the next-generation firewall performs initial request validation, checking if requests are properly formed and authorized. If requests pass basic validation, the system checks cache status to optimize performance while maintaining security.

For the more technical readers, the following lists typical events in the WAAP sequence:

- For noncached or expired content, back-end validation occurs before returning successful responses (2xx codes).
- WAF functionality appears in the request validation process, examining requests for malformation (returning 400 errors) and invalid parameters (returning 422 errors), thereby protecting against injection attacks and malicious inputs, such as cross-site scripting.
- Suspicious bot traffic patterns or automated behaviors trigger specialized scrutiny. This traffic is separated into legitimate users and potential automated threats.
- Rate limiting protects against DDoS attacks by preventing request flooding or API abuse that could overwhelm systems.
- Error handling pathways (5xx errors) provide a mechanism whereby the system maintains availability during temporary issues, a critical component of DDoS mitigation.

This stepwise integration ensures that legitimate traffic flows smoothly through caching and validation processes. At the same time, suspicious or malicious requests are identified and blocked at the appropriate security layer, creating defense-in-depth that protects applications and APIs from increasingly sophisticated threats.

Future-Ready Architecture

State-of-the-art WAAP solutions are designed with architectural flexibility to accommodate emerging threats and evolving compliance requirements. This includes support for zero-trust security models, integration with identity and access management systems, and the ability to provide consistent protection across hybrid multicloud environments.

The most advanced platforms also incorporate extensible policy engines that can adapt to new attack vectors and compliance requirements through configuration updates. This helps financial services firms avoid architectural changes, ensuring that organizations can maintain protection effectiveness as the threat landscape continues to evolve.

The WAAP Ecosystem

The traditional perimeter-based security model has proven inadequate for protecting modern distributed architectures in financial services operations. Datos Insights has identified 12 critical functions and categorized them according to high, medium, and low security requirements (Figure 7).

Figure 7: Financial Services Functions Using APIs By Security Level

Source: Datos Insights

Advanced Capabilities and API Security

Modern WAAP solutions leverage AI capabilities, including AI-powered behavioral analysis to detect anomalous authentication patterns, real-time bot detection for identifying automated credential stuffing attacks, and API schema learning to prevent unauthorized access patterns—to address contemporary threats. These capabilities are essential, as 84% of attacks against financial services originate from "authenticated" users who appeared legitimate but are actually malicious, AI-powered agents.

Instead of maintaining separate connectors for each AI data source, developers can now build against a standard protocol, the Model Context Protocol (MCP), eliminating the need for custom integrations and enabling seamless switching between different LLM providers while maintaining the same tool connections. Three additional factors should be considered when deploying MCP:

- **Agentic AI enablement:** MCP is used for building sophisticated AI agents that need real-time access to diverse data sources. MCP helps developers build agents and complex workflows on top of LLMs by providing secure, context-aware connections to databases, APIs, file systems, and business tools.
- **Enterprise adoption:** Major AI providers, including OpenAI and Google DeepMind, have adopted MCP, along with development platforms.
- **Futureproofing:** As the ecosystem matures, AI systems will maintain context as they move between different tools/datasets. MCP's open-source nature and growing ecosystem of prebuilt servers make it the standard for contextual AI integration.

MCP is a foundational shift from isolated AI models to connected, context-aware systems that can access and utilize real-world data securely in production settings. Modern WAAPs also incorporate discovery and inventory features for managing MCP interfaces.

Strategic Implementation Considerations

Organizations must evaluate WAAP solutions based on their ability to provide consistent security policies across heterogeneous environments while maintaining performance and scalability for real-time financial transactions. The objective is to implement a security architecture that enables innovation and agility while providing comprehensive protection against threats. A key element of doing so is the ability to generate meaningful metrics to measure key performance indicators (KPIs) of an API program. Figure 8 details six key KPIs for evaluating the effectiveness of a WAAP product.

Figure 8: Six KPIs for Evaluating the Effectiveness of a WAAP Product

Source: Datos Insights

The evolution toward comprehensive WAAP ecosystems requires organizations to move beyond reactive security measures toward proactive, intelligence-driven protection strategies. The integration of advanced threat detection capabilities with traditional web application firewalls creates a unified security framework that addresses the full spectrum of contemporary threats, from sophisticated API attacks to AI-powered reconnaissance activities.

State-of-the-Art in WAAP Security

The convergence of sophisticated threat actors, regulatory pressures, and the exponential growth of API attack surfaces is reshaping the state of the art in application security and API protection. Datos Insights' survey findings confirm that financial services and insurance companies have experienced API-related security issues in their production APIs over the past year. WAAP innovation in protection technologies has accelerated beyond traditional reactive security models toward predictive, AI-driven defense systems.

The threat landscape's sophistication has catalyzed breakthrough innovations in behavioral analytics and automated threat detection. Modern WAAP platforms now incorporate AI-powered behavioral analysis capable of detecting anomalous authentication patterns that traditional signature-based systems miss entirely. This evolution addresses the issue of attacks against financial services originating from authenticated users who appeared legitimate, requiring security systems that can distinguish between genuine user behavior and sophisticated impersonation attempts.

Real-time bot detection capabilities have evolved beyond simple rate limiting to incorporate ML models that analyze request patterns, device fingerprinting, and behavioral biometrics. These advanced systems can identify automated credential stuffing attacks and API abuse in real time, responding to the reality that threat actors increasingly leverage AI for reconnaissance and attack automation.

Advanced API Schema Learning and Runtime Protection

The proliferation of API endpoints has driven innovation in API schema learning technologies. State-of-the-art WAAP solutions now employ dynamic API discovery and learning algorithms that automatically map API endpoints, understand expected behavior patterns, and detect deviations that indicate potential attacks or misuse. An open-source

tool provides a good example of how this works: a CVE SQL injection into a REST API shows how WAAPs can use machine-readable threat intelligence (MRTI) for ML in real time.

Take, for example, an open-source tool called KubeClarity, which manages software bills of materials and vulnerabilities in cloud container images and file systems.[5] Using the vulnerability CVE-2024-39909 as an example, this open-source tool can quickly link the CVE to the common weaknesses and exposures (CWEs) and common attack pattern enumeration and classification (CAPECs) developed by MITRE.[6] These can then be linked to the MITRE ATT&CK tactics and techniques, which can then be linked to the D3FEND framework developed by the Center for Threat Informed Defense.[7]

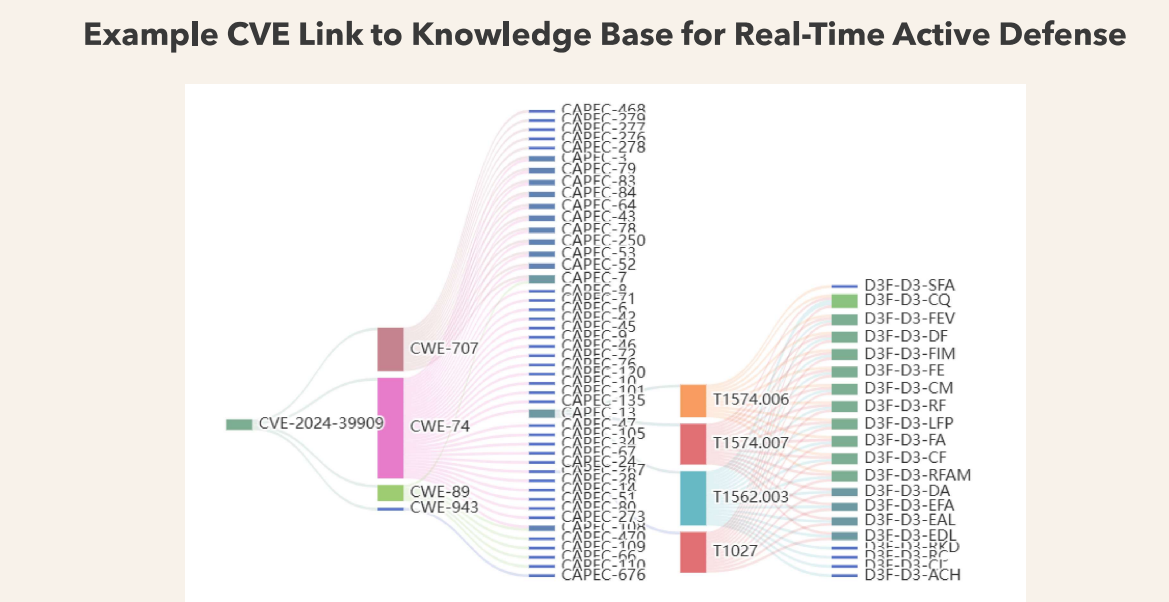
The MRTI for CWEs, CAPECs, ATT&CK, and D3FEND can be linked in milliseconds to the subject CVE. This high-speed response is what is needed to respond to attacks in real time. Figure 9 shows an example of a CVE and its respective linkages. This sequence is possible with the use of multiple knowledge graph databases linked by semantic technology. Advanced WAAPs also use such technologies.

5 "CVE-2024-39909," CVE, accessed September 24, 2025, https://www.cve.org/CVERecord?id=CVE-2024-39909.

6 "Galeax/CVE2CAPEC," GitHub, accessed September 24, 2025, https://github.com/Galeax/CVE2CAPEC.

7 D3FEND is a knowledge graph of cybersecurity countermeasures that complements MITRE's ATT&CK framework. While ATT&CK focuses on adversary behaviors and tactics, D3FEND provides a corresponding framework for defensive techniques and technologies, helping organizations understand what defensive capabilities can counter specific attack techniques.

Figure 9: Example CVE Link to Knowledge Base for Real-Time Active Defense



Source: Datos Insights

Protocol-Specific Security Innovations

Innovation in API protection has become highly protocol-aware, recognizing that different API architectures require tailored security approaches. Modern WAAP solutions must address this architectural complexity by providing consistent security policies across heterogeneous environments while maintaining the performance and scalability necessary for real-time financial transactions. The security considerations vary significantly across API protocols:

- The highly secure gRPC with built-in HTTP/2, mandatory transport layer security, and strong typing via Protocol Buffers
- Financial-grade APIs (FAPI 2.0) as developed by the OpenID Foundation in response to regulatory challenges posed by Europe's Second Payment Services Directive (PSD2)
- A RESTful implementation with OAuth 2.0 and OpenID Connect (OIDC) that provides token-based authentication with scoped permissions.

Each of these API protocols offers high-grade protection. When coupled with a single-pane dashboard as provided by a WAAP product, the security team can gain full visibility into network operations, including DDoS activity and network intrusion attempts.

Table B lists five of the key protocols FIs use, as well as those that are not recommended for financial services implementations.

Table B: Key Protocols Used by Financial Services Companies

API protocols	Security summary
gRPC	• Built on HTTP/2 with mandatory transport layer security • Strong typing via Protocol Buffers reduces injection attacks • Seamless OAuth 2.0 integration • Binary format minimizes parsing vulnerabilities
GraphQL with Apollo	• Query complexity analysis prevents DoS attacks • Persisted queries reduce the attack surface • Authorization directives for access control • Still vulnerable to over-fetching if improperly implemented
REST with OAuth 2.0/OIDC	• Token-based authentication with scoped permissions • Standardized flows for different client types • Well-established security patterns • Vulnerabilities in token management if implemented poorly
SOAP with web services security	• XML encryption and digital signatures • SAML assertions for identity • Message-level security • Complexity creates a larger attack surface
REST with API keys	• Simple authentication model • Limited authorization capabilities • Key management challenges • Transport-dependent security
Lower-rated protocols	• Basic GraphQL, JSON-RPC, basic REST, and XML-RPC (Ratings 1 to 2) lack built-in security features and rely entirely on external protection

Source: Datos Insights

The next section outlines the practical implications for rolling out a WAAP program.

Practical Implications

Platform consolidation continues to accelerate as organizations seek unified security ecosystems rather than disparate point solutions. This trend drives innovation in unified management interfaces, correlated analytics, and integrated incident response workflows. Advanced implementations provide seamless integration with identity management systems, cloud security posture management tools, and security orchestration platforms.

Organizations that embrace these emerging trends early will be better positioned to defend against the evolving threat landscape while maintaining the agility and innovation required to compete in digital markets.

The scope of this analysis extended beyond traditional web application security to encompass the full spectrum of API protection requirements, from discovery and inventory management through runtime protection and post-incident forensics.

The recommendations provided have been designed to enable financial services organizations to develop comprehensive WAAP strategies that address immediate security requirements while building the flexibility and scalability necessary to adapt to future threat evolution and regulatory changes. This forward-looking approach recognizes that effective security architecture must anticipate rather than merely respond to emerging challenges.

Through the use of a case study, specifically one strategy of the Scattered Spider group, this paper demonstrated how advanced WAAP implementations can provide effective protection against contemporary threat methodologies while maintaining the performance and availability requirements essential for financial services operations.

The ultimate objective has been to equip security leaders, architects, and implementers with the strategic and technical insights necessary to identify a vendor product and then deploy and operate the WAAP solution that effectively protects their organizations' digital assets while enabling the innovation and agility required to compete in an increasingly digital financial services marketplace.

Conclusion

CISOs and cyber-risk executives serving FIs, insurers, and other financial services firms:

- **Prioritize API security investment:** 52% of financial services organizations plan to improve API security, and 57% report API-related breaches. Immediate action is required to address this critical vulnerability.
- **Migrate to integrated WAAP solutions:** For most financial services firms, moving beyond stand-alone security tools to comprehensive WAAP platforms will yield optimal visibility and defenses for web applications and APIs in multicloud environments.
- **Implement AI-powered defense mechanisms:** Deploy behavioral analytics and ML capabilities to detect authenticated-user attacks.
- **Adopt protocol-specific security:** Implement secure API protocols like OAUTH 2.0 with ODIC and FAPI 2.0 for financial-grade protection and track the six key KPIs outlined in this report.
- **Integrate threat intelligence:** Leverage MRTI and frameworks such as MITRE ATT&CK and D3FEND for real-time threat response.

Market security providers and vendors:

- **Invest in AI/ML capabilities:** Build advanced behavioral analytics that can distinguish between legitimate users and sophisticated impersonation attempts in real time.
- **Enable protocol-aware security:** Provide tailored security approaches for different API architectures with protocol-specific protections.
- **Integrate MCP:** Prepare for AI agent security by supporting MCP for secure connections between LLMs and enterprise data sources.
- **Provide actionable metrics:** Deliver comprehensive dashboards that track discovery rates, security effectiveness, runtime coverage, and vulnerability response times to demonstrate a return on investment.

About Datos Insights

Datos Insights is the leading research and advisory partner to the banking, insurance, securities, and payments industries—both the financial services firms and the technology providers that serve them.

In an era of rapid change, we empower firms across the financial services ecosystem to make high-stakes decisions with confidence and speed. Our distinctive combination of proprietary data, analytics, and deep practitioner expertise provides actionable insights that enable clients to accelerate critical initiatives, inspire decisive action, and de-risk strategic investments to achieve faster, bolder transformation.

Contact

Research, consulting, and events:
sales@datos-insights.com

Press inquiries:
pr@datos-insights.com

All other inquiries:
info@datos-insights.com

Global headquarters:
6 Liberty Square #2779
Boston, MA 02109
www.datos-insights.com

Author information

Jane Ginn
jginn@datos-insights.com