wallarm

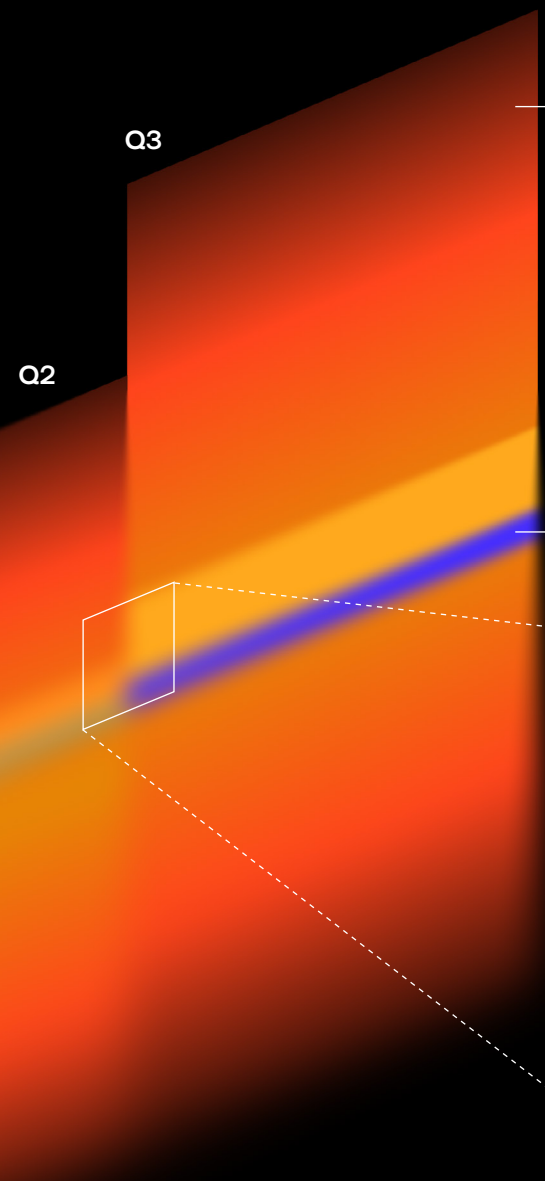
WALLARM.COM

API
ThreatStats™
Report
Q3 2025

APIs, Agents, and the Age of Exposure

wallarm

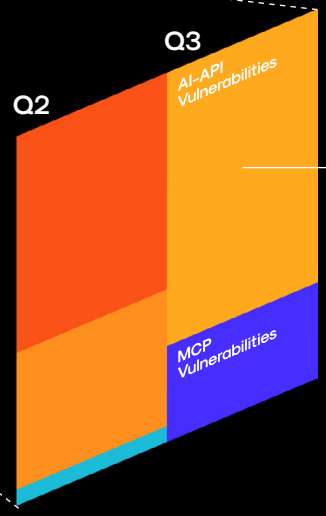
Contents



1,602
API-related vulnerabilities were disclosed in Q3

↑20%
increase in API related vulnerabilities from Q2 to Q3

↑270%
increase in MCP vulnerabilities from Q2 to Q3



↑57%
increase in AI-API vulnerabilities from Q2 to Q3

+51
new actively exploited API vulnerabilities in Q3

Executive Summary

The Q3 2025 API ThreatStats™ Report reinforces that APIs remain at the center of both vulnerability disclosures and real-world breaches. This quarter's findings confirm that API security has evolved from a purely technical challenge into a systemic business risk. Attackers are exploiting everything from misconfigured enterprise APIs to AI inference interfaces and partner integrations at scale. As in prior quarters, the analysis focuses on three dimensions: vulnerability trends, exploit activity, and real-world breaches.

Vulnerability Trends

The data shows a steep increase in API vulnerabilities. 1,602 API-related vulnerabilities were disclosed in Q3 2025, up nearly 20% from 1,341 in Q2. The average CVSS score remained stable at 7.4, indicating continued high severity across most advisories. Security Misconfiguration (API8) dominated with 605 cases, followed by Broken Authorization issues (API5, API1, API2). AI-related APIs saw a 25% increase, growing from 77 to 96 vulnerabilities, with most mapped to Security Misconfiguration and Broken Function Level Authorization. MCP vulnerabilities were the stand out data point with 270% growth quarter over quarter.

Exploit Trends

CISA's Known Exploited Vulnerabilities (KEV) catalog added 51 new entries in Q3, of which 8 (16%) were API-related. While the absolute count declined from Q2, APIs continue to represent a stable share of exploited vulnerabilities. The most common exploit vectors aligned with the OWASP API Top 10, particularly Broken Authorization (API1, API5), Security Misconfiguration (API8), and Unsafe Consumption of APIs (API10) through deserialization flaws.

> In Q3, **16%** of KEVs and 8 major breaches were API-related — misconfigs, auth failures, and AI integrations drove the risk.

Breach Trends

8 major API-related breaches were confirmed in Q3, compared to 10 in Q2. The Salesloft Drift incident stood out for its multi-enterprise impact through OAuth token abuse in Salesforce APIs. Other top breaches included Restaurant Brands International (drive-thru APIs), SwissBorg ($41M loss through fintech API abuse), Paradox.ai (chatbot exposure of HR data), and Flexypay Solutions (fraudulent payouts via partner APIs).

Overall, the Q3 data underscores that API risk is outpacing traditional AppSec coverage. Misconfigurations and authorization failures continue to dominate, while Business Logic Abuse has emerged as a leading threat vector. The expanding presence of AI-APIs adds new layers of integration complexity and risk. For CISOs, the takeaway is clear: treat APIs as a first-class attack surface, invest in discovery and runtime protection, and extend governance to cover AI and agentic systems before attackers do.

> **$41M lost**, HR data leaked, OAuth abused — Q3 breaches show APIs are the fastest path to compromise.

ThreatStats™ Spotlight

Business Logic Abuse (BLA)

Business Logic Abuse (BLA) targets flaws in how an application actually works, rather than exploiting flaws in code, such as more traditional injections or remote code execution. Instead of smuggling payloads (e.g., SQLi, XSS), attackers manipulate workflows, states, roles, quotas, and lifecycles to get privileged outcomes: skipping steps, repeating one-time actions, or harvesting sensitive system signals. That is why BLA often evades traditional controls (WAF signatures, SAST/DAST) and requires stateful, behavior-aware defenses.

While BLA isn't a new problem, the massive growth in API and AI applications has correspondingly increased the available business logic attack surface. According to the Postman State of the API report for 2025, 82% of organizations categorize themselves as API first[1]. Furthermore, it's reasonable to consider that generative AI applications are simply distilled business logic. We've chosen to spotlight Business Logic Abuse in this quarter's report because of the evident trend in incidents and vulnerabilities.

> BLA doesn't break code — it breaks logic. And with **82%** of orgs now API-first, the attack surface keeps growing.

Case Studies

CASE---------- #1

rbi restaurant brands international

RBI ranked in our top five breaches this quarter. Attackers took advantage of weaknesses in the drive-thru/ordering APIs, specifically BOLA and missing checks between steps (transition validation), to carry out business-logic abuse.

CASE---------- #2

stripe

Earlier in the year, Stripe experienced a complex incident involving skimming credit card numbers. The incident also involved a legacy API being abused for card validation, which amounts to shadow function abuse.

CASE---------- #3

ticketmaster®

In an ongoing case, Key Investment Group used multi-account automation to bypass Ticketmaster's purchase limits, resulting in a resource quota violation.

1 State of the API Report 2025

The OWASP Business Logic Abuse Top 10 '25

BLA1---------- ALO

Action Limit Overrun

Re-using "one-time" actions, like coupons or refunds, again and again because the system doesn't lock them after the first use.

BLA2--------- CWOB

Concurrent Workflow Order Bypass

Skipping ahead in a multi-step process (e.g., finishing before the required earlier steps complete) by sending requests out of order.

BLA3---------- OSM

Object State Manipulations

Object State Manipulations (OSM) - Sending sneaky values so the app quietly flips hidden settings, like roles or status, that it shouldn't let you change.

BLA4---------- MLL

Malicious Logic Loop

Triggering a process that never properly stops or repeats too much to chew up time, money, or system resources.

BLA5---------- ALE

Artifact Lifetime Exploitation

Using "short-lived" things such as tokens, sessions, or temporary files, after they should have expired because the app didn't actually retire them.

BLA6---------- MTV

Missing Transition Validation

Calling later workflow steps directly because the app doesn't re-check that you satisfied the earlier requirements.

BLA7---------- RQV

Resource Quota Violation

Hammering a feature too fast or too often, with vote spamming, heavy tasks, etc., to get an edge or degrade the service.

BLA8---------- ISD

Internal State Disclosure

Error messages, codes, or timing differences leak what's happening inside, helping attackers plan targeted abuse.

BLA9---------- BAC

Broken Access Control

The app doesn't properly check permissions in key business actions, so people do things they're not allowed to do.

BLA10--------- SFA

Shadow Function Abuse

Abusing forgotten or hidden functions, such as test utilities or internal endpoints, left available in production.

To address the growing trend of Business Logic Abuse, Wallarm initiated and led a community effort to develop the new OWASP Business Logic Abuse Top 10[2]. The objective is to provide a technology-agnostic industry standard for describing business logic abuse. Unlike many of the other OWASP Top 10 lists, the BLA Top 10 isn't restricted to a specific technology, like APIs, Mobile, or Docker; it's universally applicable, which makes it useful even as technology changes.

2 OWASP Top 10 for Business Logic Abuse

Outlook for Business Logic Abuse

Where are we headed with Business Logic Abuse?

1 **AI-ASSISTED WORKFLOW ABUSE**
Agentic tools now make it easier than ever to discover edge-state transitions and orchestrate multi-step exploits at scale; expect more CWOB and ALO against checkout, refunds, and coupon logic.

2 **SIGNAL HARVESTING AND DATA DISCLOSURE**
Error codes, timing differences, and partial successes will be mined as ISD to plan precision fraud.

3 **SHADOW ENDPOINTS AND INTEGRATIONS**
Legacy, mobile-only, and internal APIs remain prime entry points. The AI-driven velocity of development will only make this problem worse over time.

4 **QUOTA ECONOMICS**
As consumption-priced APIs expand, attackers will directly target RQV. Consumption pricing will become an attack vector whereby attackers can directly impact the victims' bottom line.

> BLA is evolving fast — AI agents, shadow endpoints, and quota abuse are turning logic into leverage.

API Vulnerability Trends

As in previous API ThreatStats reports, we've analyzed the published vulnerability data, but this quarter we've employed a higher fidelity methodology. Previous ThreatStats reports relied primarily on keyword analysis to categorize the vulnerability advisories and CVEs. This quarter, we've adopted a more sophisticated analysis that not only identifies whether a vulnerability is API related, but also which API protocol is involved.

Q2	1,341	API-RELATED VULNERABILITIES
Q3	1,602	

Since we've adjusted our methodology, we've re-run the analysis for Q2 data as well, in order to provide meaningful comparisons. This updated analysis reveals a clear upward trend in API-related vulnerabilities from Q2 to Q3 2025. A total of 1,341 API-related vulnerabilities were identified in Q2, rising to 1,602 in Q3, an increase of nearly 20 percent quarter over quarter. The average CVSS score remained steady at approximately 7.4, indicating that most vulnerabilities continue to fall in the High severity range; a pattern that's been consistent throughout our ThreatStats reports.

This growth reflects continued expansion of API usage across ecosystems and recurring security weaknesses in configuration and authorization logic. OWASP API Top 10 mapping confirms that the majority of API vulnerabilities remain concentrated in Security Misconfiguration (API8) and Broken Authorization categories (API5, API1, API2).

> API vulnerabilities rose **20%** from Q2 to Q3 — misconfigs and auth flaws still lead the trend.

OWASP API Top 10 Mapping

CATEGORY	Q3 COUNT
API8:2023 Security Misconfiguration	605
API5:2023 Broken Function Level Authorization	287
API2:2023 Broken Authentication	207
API1:2023 Broken Object Level Authorization	169
API4:2023 Unrestricted Resource Consumption	136
API7:2023 Server Side Request Forgery	74
API10:2023 Unsafe Consumption of APIs	54
API3:2023 Broken Object Property Level Authorization	49
API6:2023 Unrestricted Access to Sensitive Business Flows	11
Other / Minor Categories	9

Key Observations

1 Security Misconfiguration (API8) continues to dominate API risk, increasing from 456 in Q2 to 605 in Q3 (+33%). Misconfigurations now account for nearly 38% of all API-related vulnerabilities.

2 Authorization issues (API5, API1) remain the second-largest class of API flaws, representing about 28% of all API vulnerabilities.

3 Broken Authentication (API2) showed a notable rise, climbing from 155 to 207, driven primarily by weak or missing credential enforcement in REST and SOAP APIs.

4 Unsafe Consumption of APIs (API10) and Server Side Request Forgery (API7) remain persistent but less common patterns.

> API misconfigurations surged last quarter, now driving over a third of all reported API flaws.

API Protocol Distribution

The improved analysis gives us greater visibility into the breakdown of API protocols across vulnerabilities.

PROTOCOL	# OF ADVISORIES	% API VULNERABILITIES
REST	1,333	83.21%
AI-API	121	7.55%
SOAP	43	2.68%
WebSocket	34	2.12%
GraphQL	30	1.87%
gRPC	26	1.62%
XMLRPC	12	0.75%
MQTT	6	0.37%

> REST accounts for **83%** of API vulnerabilities — but AI-APIs already rank **#2**, revealing a fast-emerging risk surface.

Unsurprisingly, REST dominates the vulnerability landscape, but the presence of AI-APIs (admittedly, not really a protocol) is noteworthy. The fact that SOAP, arguably a legacy protocol, follows in the third spot speaks to the fact that even legacy API technologies remain a significant security issue. Careful readers might note, however, that for most intents and purposes, SOAP, Websocket, GraphQL, and gRPC are all about the same distribution.

Q3 Dominant Themes

1. Security misconfiguration remains the most prevalent API weakness, underscoring gaps in secure deployment, hardening, and access control across exposed endpoints.
2. The steady volume of high-severity CVSS scores highlights the potential for direct exploitation, particularly in production APIs handling sensitive data or authentication flows.
3. Authorization complexity continues to challenge development teams, with both function-level and object-level access control errors contributing to systemic risk.
4. The expansion from Q2 to Q3 reflects both the growing visibility of APIs in security advisories and ongoing weaknesses in API governance and testing.

> Misconfigurations, high-severity CVEs, and auth complexity continue to dominate — Q3 shows progress in visibility, not in control.

Overall, Q3 confirms that while awareness of API security risks is rising, consistent secure design and runtime enforcement remain elusive across industries.

AI-Related API Vulnerability Trends

Given the connection between AI and APIs, it's important to pay attention to the AI vulnerability trends in our API data set as well. The data reveals a continued increase in vulnerabilities specifically involving AI-related APIs. In Q2 2025, 77 vulnerabilities were identified as AI-API related, increasing to 121 in Q3 2025, marking a 57% rise. This growth mirrors the broader expansion of AI integration across applications and highlights the growing attack surface of model-serving and inference APIs.

OWASP Mapping for AI-Related API Vulnerabilities

CATEGORY		Q2 COUNT	Q3 COUNT
API8:2023	Security Misconfiguration	31	39
API5:2023	Broken Function Level Authorization	15	21
API2:2023	Broken Authentication	10	13
API10:2023	Unsafe Consumption of APIs	8	10
API1:2023	Broken Object Level Authorization	7	8
Other / Miscellaneous		6	5

> AI-related API vulnerabilities jumped **57%** in Q3 — integration flaws and misconfigurations continue to expose model-serving APIs.

When compared with the overall API vulnerability landscape, AI-API issues show similar weaknesses but differ in emphasis. Security Misconfiguration (API8) leads both groups, indicating that deployment and access control remain the weakest points for traditional and AI-driven APIs alike. However, AI-API vulnerabilities demonstrate proportionally higher rates of Broken Function Level Authorization (API5) and Unsafe Consumption of APIs (API10), suggesting that integration and orchestration flaws are more common in AI ecosystems where multiple components share data and execution context.

A quick breakdown of the AI-API vulnerabilities into sub-categories is very revealing. When broken down into MCP, Agentic, and Other AI categories, the data looks like this:

CATEGORY	Q2 COUNT	Q3 COUNT	% CHANGE (Q2 → Q3)
MCP	10	37	+270.0%
Agentic AI	3	5	+67%
Other AI	64	79	+23%
Total AI-API Vulnerabilities	77	121	+57%

The increase in specifically agentic AI vulnerabilities is notable percentage-wise (67%), but small in number. The increase in MCP vulnerabilities is huge as a percentage (270%) and also significant as a pure number. It's clear that MCP risks are increasing rapidly.

The trend toward increased AI-API vulnerabilities, and specifically MCP vulnerabilities, underscores the importance of applying traditional API security controls, such as authorization, authentication, and configuration hardening, to AI model-serving and inference endpoints. The preventative controls must be paired with effective discovery, as well as detection and blocking of attacks. As AI capabilities become more deeply embedded in enterprise architectures, the overlap between AI security and API security will continue to grow.

> MCP-related API vulnerabilities surged **270%** in Q3 — model-serving endpoints are becoming prime attack targets.

API Exploit Trends

In order to understand what vulnerabilities are being actively exploited for a given quarter, we look at the CISA Known Exploited Vulnerabilities (KEV) catalog. While the nature of exploit activity challenges any analysis to be comprehensive, the KEV represents an accurate cross-section of known exploit activity.

+59 NEW ENTRIES TOTAL IN Q2 — API-RELATED **13**

+51 NEW ENTRY TOTAL IN Q3 — API-RELATED **8**

NEW CISA KEV ENTRIES

In Q3 2025, the CISA KEV catalog added 51 new entries, compared to 59 in the previous quarter. Of these, 8 were API-related (16%), while 13 (22%) API-related in Q2.

API-Related KEVs in Q3 2025

CVE-2025-20337
CVE-2025-20281

Cisco ISE or ISE-PIC

API request manipulation allowed remote code execution.

CVE-2025-48927

TeleMessage TM SGNL

Exposed Spring Boot Actuator heapdump API endpoint.

CVE-2025-32463

Sudo

Functionality exposure exploitable via management-like API interface.

CVE-2025-10035

Fortra GoAnywhere MFT

Deserialization of untrusted data via API.

CVE-2025-5086

Dassault Systemes DELMIA Apriso

Deserialization flaw via API.

CVE-2025-21311

Adminer

SSRF through API interface.

CVE-2025-59689

Libraesva ESG

Command injection via API endpoint.

These API exploits primarily fall into three OWASP-aligned categories:

API---------- 1&5

Broken Object and Function Level Authorization

Several exploits (for example, Cisco ISE and TeleMessage) stemmed from missing or improperly enforced access controls on API endpoints.

API---------- 8

Security Misconfiguration

Exposed management and diagnostic interfaces such as Spring Boot Actuator endpoints were a recurring vector.

API---------- 10

Unsafe Consumption of APIs

Vulnerabilities involving deserialization of untrusted data (e.g., Fortra GoAnywhere, DELMIA Apriso) exemplify insecure consumption patterns that allow code execution through external API calls.

Exploit Analysis and Insights

What conclusions can we draw from this quarter's CISA KEV data? APIs make up a significant percentage of the exploited vulnerabilities, and do so consistently, quarter over quarter. We see some common exploit types: authorization issues, exposed interfaces, and unsafe consumption of APIs. There is clear continuity with the vulnerability analysis here, and, as we'll see in the next section, these patterns map directly to risks seen in real-world breaches, showing continuity between CVE exploitation and operational compromise.

API Breaches

In addition to analyzing vulnerabilities and exploits, we also looked at API breaches reported in the news. This quarter saw significant breaches spanning fintech, hospitality, crypto, and SaaS.

Breach analysis provides real-world examples of how attackers are targeting APIs in production environments, completing the analysis trifecta of vulnerabilities, exploits, and actual incidents. While the total number of incidents in Q3 (8 breaches) was slightly lower than Q2 (10 breaches), the breadth and depth of API exploitation remained significant. And as we'll see, the numbers aren't quite that simple.

Salesloft Drift Incident

The most impactful API breach of Q3 was the Salesloft Drift incident. In August, attackers used stolen OAuth tokens to gain unauthorized access to Salesforce APIs across multiple enterprises, including Cloudflare, Zscaler, Palo Alto Networks, and Google. There's unconfirmed speculation, given the number of impacted organizations, that the token(s) used were improperly scoped or root OAuth tokens. While we counted this as a single incident in the 8 this quarter, it had multiple victims and could be counted as multiple breaches impacting at least a dozen organizations. It's the breadth of this impact that makes this incident the number 1 for Q3 2025.

> One OAuth breach hit a dozen enterprises — Salesloft Drift shows how a single API token can ripple across ecosystems.

Top 5 API Breaches Q3 2025

RANK	VENDOR	WHAT HAPPENED	IMPACT
1	Salesloft / Drift	OAuth tokens abused to access Salesforce APIs across multiple enterprises.[1]	Multi-company exposure; 4 major firms affected (Cloudflare, Zscaler, Palo Alto, Google).
2	Restaurant Brands International	Drive-thru and ordering APIs exploited using BOLA and logic flaws.[2]	Operational disruption; exposure of live audio and order data (thousands of stores).
3	SwissBorg	Fintech API abuse enabled fraudulent transfers from crypto wallets.[3]	$41 million stolen.
4	McDonald's via Paradox.ai	Internal chatbot APIs leaked sensitive applicant and HR data for McDonald's.[4]	Millions of applicant records exposed.
5	Flexypay Solutions	Partner integration APIs exploited to trigger unauthorized payouts.[5]	$168,000 stolen via fraudulent API transactions.

1 Salesloft Drift Breach - Track the Salesforce Incident

2 Burger King hacked - ethical hackers crack fast food security, and find it's as fragile as a French fry

3 SwissBorg's $41M Exploit: Key Insights

4 McDonald's AI Breach Reveals The Dark Side Of Automated Recruitment

5 ₹1.39 Crore Vanishes: Hyderabad Tech Firm Hit by Sophisticated Server Breach

HONORABLE MENTION

Sapphos (Technology)[1]

In this incident, attackers discovered and repeatedly called unprotected API endpoints that exposed user and configuration data without enforcing proper authorization checks. The lack of object-level access control (a BOLA vulnerability) allowed unauthorized retrieval of sensitive records belonging to other users. Once the exposure was identified, the company was forced to take the affected application offline to contain the breach and prevent further exploitation. Although only about 17,000 user records were impacted, the incident is a textbook example of BOLA, and provides a reminder of the possible impact of missing authorization controls, earning it an honorable mention.

> **17,000 records** exposed via unprotected endpoints — a textbook BOLA breach that forced a full takedown.

Breach Analysis and Trends

Whereas the Q3 KEV entries showed a concentration of authorization issues, exposed interfaces, and unsafe consumption of APIs, the breach data reveals how those same weaknesses manifest in real-world workflows and integrations.

1 **INTEGRATION OR API TRUST CHAINS**
The Salesloft Drift OAuth, SwissBorg, and Flexpay incidents show how API integration with a single partner can result in significant compromise.

2 **BUSINESS LOGIC ABUSE**
RBI's drive-thru or ordering flows were exploited with Business Logic Abuse techniques such as BOLA and missing transition validation, demonstrating that attackers increasingly target the workflow, not just the code.

3 **AI OR AGENT APIS**
McDonald's (Paradox.ai) highlights exposure in LLM or agent-backed interfaces, where internal APIs and data flows may not be protected with the same rigor as public endpoints.

1 Brazil lesbian dating app shuts down after security flaw exposes sensitive user data.

4 **DIRECT MONETIZATION**
Both SwissBorg ($41M) and Flexpay ($168K) underscores how API abuse in fintech can lead to immediate financial loss, not just data exposure.

5 **AUTHORIZATION ISSUES**
Sapphos is a textbook case of an API vulnerable to BOLA, where a lack of granular authorization led to the application being taken offline.

Compared to Q2 (10 breaches), Q3 featured 8 total incidents; fewer incidents overall, but broader industry spread, and a stronger emphasis on integration abuse. Taken together with the KEV analysis showing that 16 percent of new exploited vulnerabilities in Q3 were API-related, the data demonstrates that APIs remain a consistent and critical vector across both confirmed exploits and real-world breaches.

> From OAuth abuse to direct monetization, Q3 breaches prove APIs are not just entry points — they are business-critical risk surfaces.

Key Takeaways

It's clear from the Q3 data that APIs remain a primary vector for attacks, and that API security must be a priority, but we can do better than AI-generated platitudes. Here are the specific takeaways from this quarter's analysis.

1

API RISK IS OUTPACING TRADITIONAL APPSEC PROGRAMS

CISA KEV and breach data show APIs are consistently exploited, yet most programs still address them in the same category as web applications. The disjunction here is amplified by Q3 breaches exploiting hidden endpoints (drive-thru ordering systems, debug APIs, partner APIs). Now that APIs have far outpaced web development, it's time for API security to ride shotgun instead of in the back seat. For CISOs that means that budgeting, staffing, and metrics must explicitly account for API security.

2

INTEGRATION AND TRUST CHAINS AMPLIFY IMPACT

The Salesloft Drift incident cascaded across enterprises; the SwissBorg and Fi-expay breaches showed that direct fintech API abuse can cause immediate financial loss. CISOs must treat API integrations as high-risk trust boundaries, enforce least-privilege, and continuously monitor token and trust use.

3

BUSINESS LOGIC ABUSE IS EMERGING AS A LEADING THREAT

Incidents like Restaurant Brands International, Stripe, and Ticketmaster show attackers exploiting workflows and state transitions, not just code flaws. Traditional defenses cannot catch these abuses. Behavioral and context-aware protection is required for API security programs and tools.

4

AI AND AGENT-BACKED APIS ARE ALREADY BEING EXPLOITED

Two points make a line, and we need to draw one between AI vulnerabilities and breaches like McDonald's (Paradox.ai). LLM or agent APIs are already being targeted. AI or agent exposure is a real risk today and requires the same, if not more, rigor as traditional API security.

API Security Guidance

The data points to expanding risk surfaces, persistent misconfigurations, and the growing convergence of AI and API threats. Below are three key moves for CISOs to lead strategically and three tactical plays for practitioners to execute immediately.

Guidance for CISOs

1 **MAKE API SECURITY A BOARD-LEVEL METRIC**
If APIs are now your primary attack surface, their security posture deserves visibility equal to patch rates or MFA adoption. Establish API security KPIs, such as API inventory coverage, authorization testing rates, and mean time to detect API misuse, and report them quarterly to leadership.

2 **COLLAPSE THE APPSEC / API DIVIDE**
Most AppSec programs still treat APIs as an afterthought. Unify your web, mobile, and API risk models. Build a joint governance framework that spans development, architecture, and operations so every new API is born secure, not retrofitted later.

3 **FUND AI-AWARE DEFENSES NOW**
AI-APIs grew 25% this quarter, and governance will lag adoption. Allocate budget for tools that can monitor AI inference, model exposure, and API trust chains. Make AI risk part of your enterprise security posture today, before regulators make it mandatory.

Guidance for Practitioners

1 **HUNT THE SHADOW APIS**
Don't just discover APIs, hunt them. Use active scanning, traffic analysis, and inventory comparison to uncover hidden endpoints in staging and production. Every untracked API is a potential breach vector.

2 **BREAK YOUR OWN AUTHORIZATION**
Test critical APIs for Business Logic Abuse, BOLA, and BFLA before attackers do. Automate these checks in CI/CD pipelines and verify role boundaries on every code release.

3 **PUT AI ENDPOINTS UNDER THE MICROSCOPE**
Treat AI-APIs like privileged systems: instrument them, log every request, and analyze behavior for anomalies. Use anomaly detection tools tuned for inference and integration traffic. If your AI systems talk to partners, audit those connections quarterly.

wallarm

Book a Demo

About Wallarm

Wallarm is the leading API security company, purpose-built to protect modern cloud-native and AI-driven architectures from today's most advanced threats. Our platform delivers complete visibility, intelligent threat detection, and real-time protection for all types of APIs like REST, GraphQL, gRPC, and increasingly, AI and Agent-based APIs.

As organizations adopt LLMs and autonomous agents, Wallarm helps secure the unique risks these interfaces introduce, including prompt injection, token abuse, and logic manipulation. By combining continuous API discovery, behavior-based analysis, and runtime policy enforcement, Wallarm enables security teams to protect complex API ecosystems including those powering AI without slowing innovation.

Learn more --------wallarm.com
Follow us----------Blog X LinkedIn YouTube
Explore product----tour.playground.wallarm.com

Secure APIs.
Stop breaches.

>

#EOF