
Consulteer
InCyber
wallarm

Shifting Sands

Risk and Change in the API Landscape

Consulteer InCyber

Short Introduction

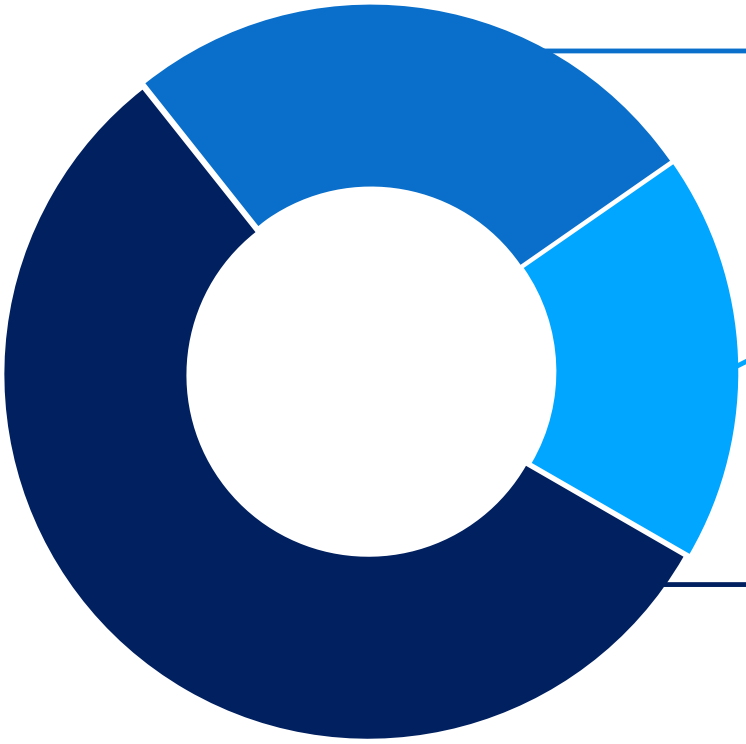
JULIAN RICHTER
Senior Cybersecurity Engineer
Consulteer InCyber

JAMES SHERLOW
Global VP of Sales Engineering
Wallarm

The API Threat Landscape

Number of APIs and Apps skyrocket

1.7 billion active APIs in 2030*



26%

Partners (shared with integration partners)

18%

Public (accessible on the Internet)

56%

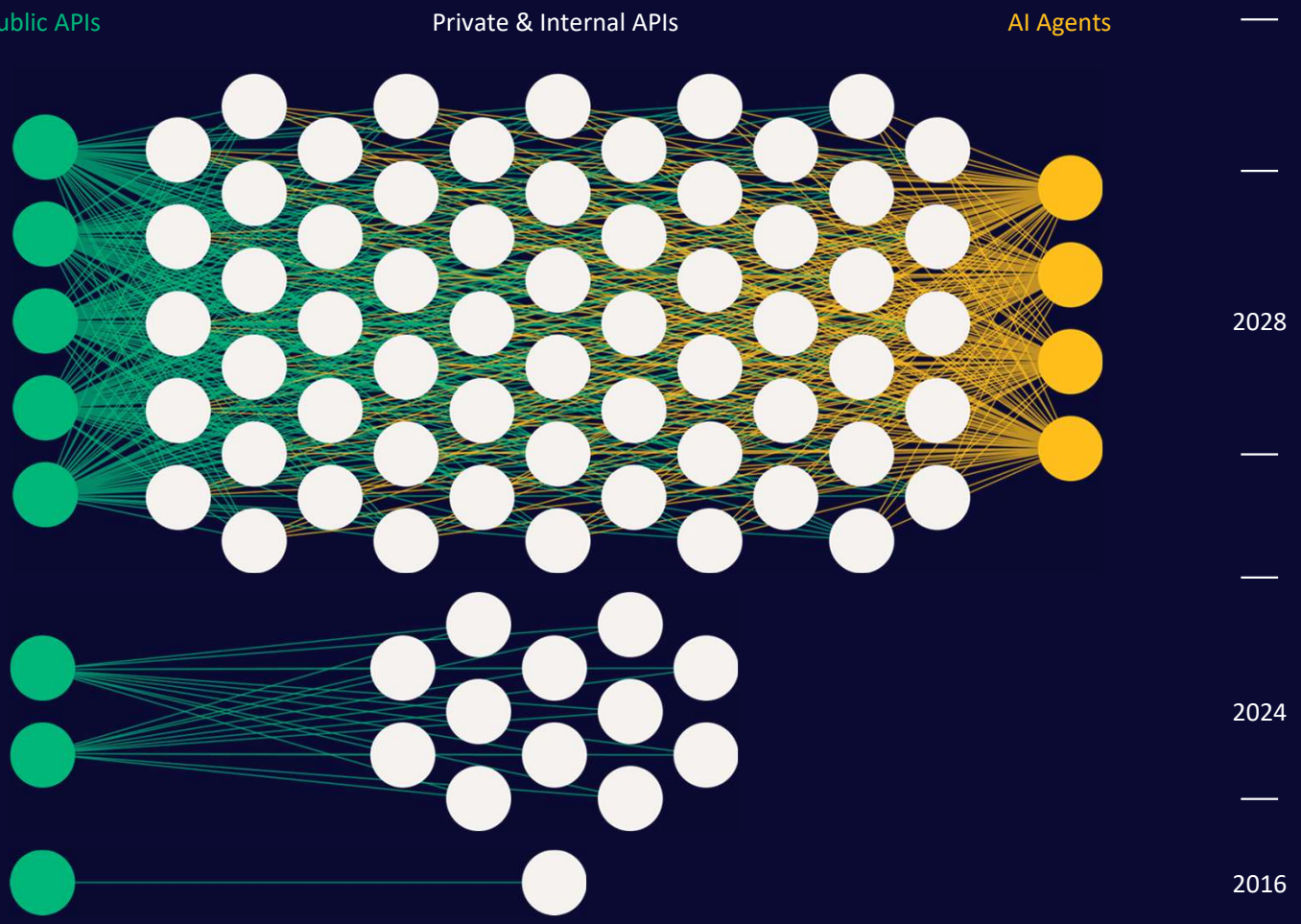
Private (used only within the company or team)

Consulteer InCyber

* Postman 2024 State of API Report

AI is driving the API market explosion

APIs are the new wires that connect data. GenAI and Agentic AI deployments are just getting started,all connected by APIs.



Consulteer InCyber

The OWASP Business Logic Top 10

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 againts checkout, refinds, 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.

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

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.

Consulteer InCyber

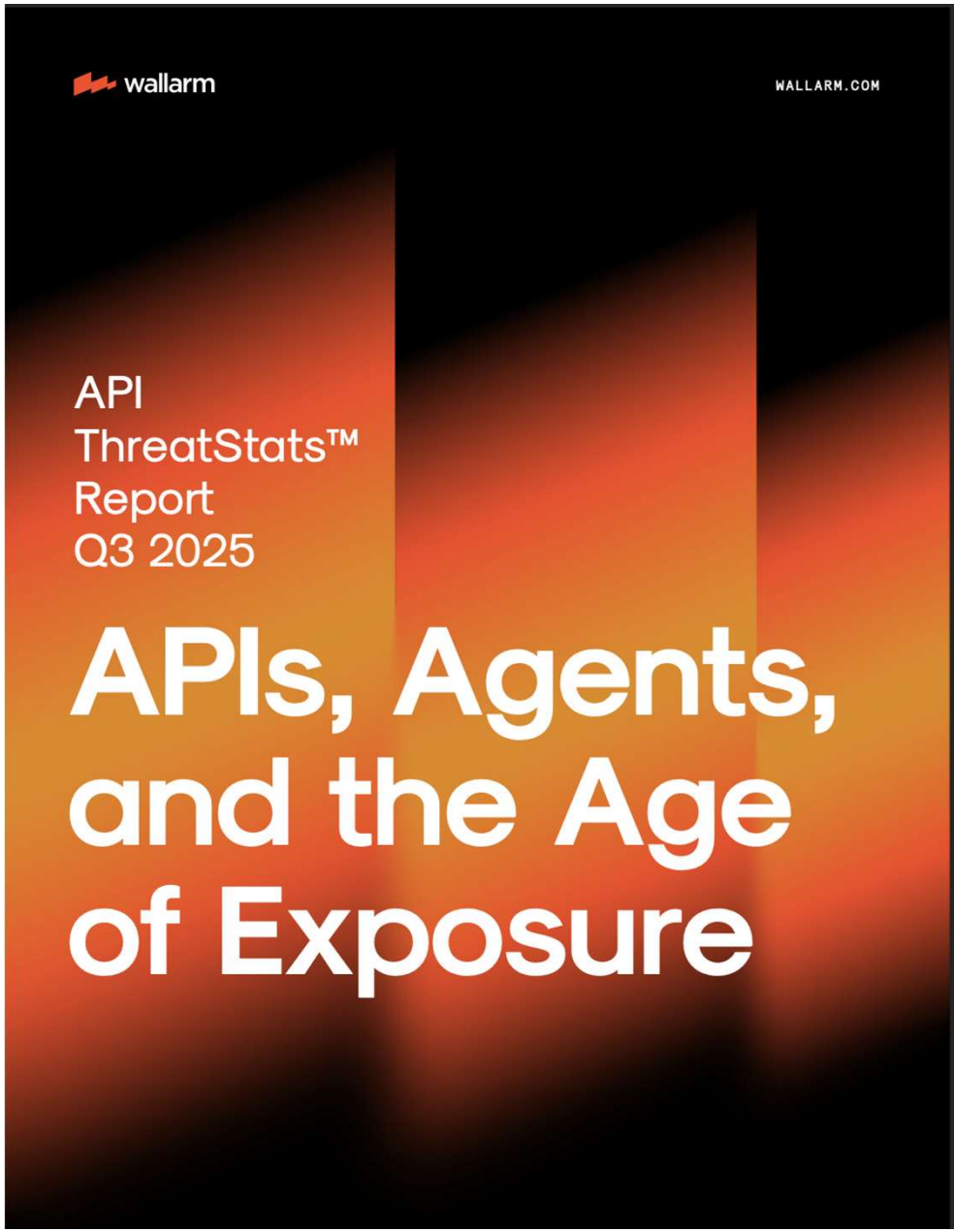
Wallarm
API ThreatStats Report

API, Agents, and the Age of Exposure

From vulnerability trends and exploit activity to real-world breaches, the Q3 2025 API ThreatStats Report shows why APIs are a critical attack surface that demand a strong security strategy.

https://www.wallarm.com/reports/q3-2025-wallarm-api-threatstats-report

Consulteer InCyber



Vulnerability Trends

API Vulnerabilities Increase

Q2	1,341*
Q3	1,602*

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%

Category	Q3 Count
Security Misconfiguration	605
Broken Function Level Authorization	287
Broken Authentication	207
Broken Object Level Authorization	169
Unrestricted Resource Consumption	136
Server Side Request Forgery	74
Unsafe Consumption of APIs	54
Broken Object Property Level Authorization	49
Unrestricted Access to Sensitive Business Flows	11
Other/Minor Categories	9

Consulteer InCyber

* API-related vulnerabilities in Q2/Q3 2025

AI API Vulnerability Breakdown

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

Category	Q2 Count	Q3 Count	% Change (Q2 → Q3)
MCP	10	37	+270%
Agentic AI	3	5	+67%
Other AI	64	79	+23%
Total AI-API Vulnerabilities	77	121	+57%

Exploit Trends

API Exploits in Q3

+59 New entries total in Q2 — API-related **13**

+51 New entries total in Q3 — API-related **8**

New CISA KEV entries

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-2025-59689

Libraesva ESG

Command injection via API endpoint.

Breach Trends

API Breaches in Q3

Rank	Vendor	What happened	Impact
1	Salesloft.	OAuth tokens abused to access Salesforce APIs across multiple enterprises.	Multi-company exposure; 4 major firms affected (Cloudflare, Zscaler, Palo Alto, Google)
2	rbi restaurant brands international	Drive-thru and ordering APIs exploited using BOLA and logic flaws.	Operational disruption; exposure of live audio and order data (thousands of stores).
3	SwissBorg	Fintech API abuse enabled fraudulent transfers from crypto wallets.	$41 million stolen.
4	PARADOX A Workday Company	Internal chatbot APIs leaked sensitive applicant and HR data for McDonald's.	Millions of applicant records exposed.
5	Flexypay	Partner integration APIs exploited to trigger unauthorized payouts.	$168,000 stolen via fraudulent API transactions.

Consulteer InCyber

Key Takeaways

Key Takeaways

01 API risk is outpacing traditional application security programs.

02 Integration and trust chains amplify impact.

03 Business logic abuse is emerging as a leading threat.

04 AI and agent-backed APIs are already being exploited.

What can be done?

Customer API Security Initiatives

Lack of API Security Posture Management

- Inventory: What APIs and apps do I have?
- Sensitive data: What information is transferred?
- Risks: What risks are my APIs exposed to?

Lack of API Runtime Security

- Remediation: How do I fix the existing risks?
- Mitigation: How do I reduce the impact of API security risks?
- Prevention: How do I block API attacks in real time?

Lack of Resources

- Operation: Who will monitor the API security tools?
- Threats: How can I recognise and investigate them?
- Incident response: How can I understand what happened?

What comes next?

Consulteer InCyber

Consulteer InCyber AG
Riedweg 6
CH-6045 Meggen
+41 41 377 22 66
consulteer-incyber.com