Prophaze
The New Phase of Security

Application Threat Landscape

Analysis Report

Q1 2026

January · February · March

Table Of Contents

01 Foreword

Overview of the report purpose and key themes ---------- 01

02 · Executive Summary

Q1 highlights, key metrics, and major findings ---------- 02

03 · OWASP Threat Distribution And Patterns

Threat distribution, dominant risks, and exposure signals ---------- 03

04 · Threat Activity & Trends

Monthly patterns, industry attack behavior, and attack density analysis ---------- 05

05 · Industry Intelligence

Industry- wise OWASP profiles and key insights ---------- 08

06 · Addressing The Findings, Key Insights & Decisions

Critical findings and security implications ---------- 19

07 · Q4 2025 vs Q1 2026 Comparison & Q2 2026 Outlook

Comparative analysis and forward-looking trends ---------- 20

08 · Conclusion

Final takeaways, strategic direction & Limitations ---------- 22

09 · Prophaze Platform Overview

Solutions, capabilities, and differentiators ---------- 23

About Prophaze

Prophaze is a fully managed, **AI-powered Web Application and API Protection (WAAP)** platform delivering 360° application security. Combining adaptive WAF, API security, bot mitigation, and DDoS protection, Prophaze enables organizations to secure modern applications with real-time behavioral intelligence and 24×7 expert monitoring.

FOREWORD

Application-layer threats are no longer occasional ,they are continuous, targeted, and embedded in modern systems. However, most threat intelligence is too broad to reflect the specific risks organisations face daily.

This report addresses that gap using real Q1 2026 telemetry from applications across 11 industries and hundreds of domains, turning observed attacks into actionable insights for security and risk teams

This quarter highlights a convergence of OWASP API and Web Application threats, notably in Finance where API2:2023 (Broken Authentication) fueled a massive surge in authentication-layer attacks. Across other sectors, Injection (A03) remains the primary threat, while Component Vulnerabilities (A06) and Healthcare's Insecure Design (A04) persist due to upgrade constraints and legacy design debt.

All insights are based on observed data. Even threats marked as 0% indicate low but present activity ,often early signals of future escalation, as seen in the Finance API trend.

This report begins an ongoing quarterly analysis aimed at helping organisations prioritise protection with precise, data-driven intelligence.

About This Report

This is Prophaze's inaugural Application Threat Landscape report , the first in a quarterly series built from live telemetry across our monitored estate.

Coverage

Q1 2026 · January–March

Industries

11 sectors · Education, Healthcare, Government, Manufacturing, IT & Software, Finance, Energy, Legal, Real Estate, Business, Non-Profit

Monitored Domains

Approximately 569 domains

Methodology

OWASP threat percentages weighted against deduplicated monthly attack totals per industry and averaged across Q1. Threats at 0% are confirmed but negligible , not absent.

First Report Finding

First confirmed OWASP API Security Top 10 threat in Prophaze telemetry , API2:2023 Broken Authentication in Finance & Banking at 99% of March activity.

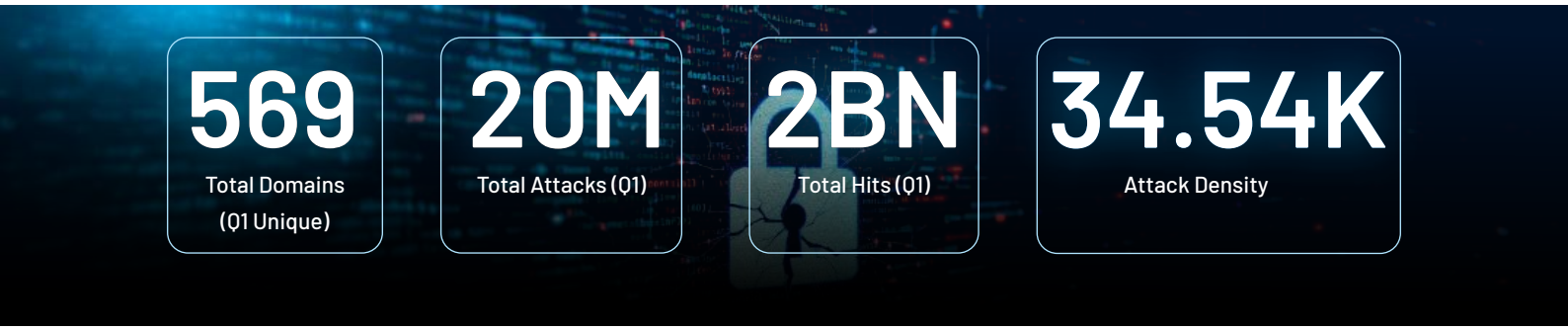
Next Edition

Q2 2026 Application Threat Landscape , Prophaze Technologies · July 2026

01 EXECUTIVE SUMMARY

At a Glance

Prophaze's Q1 2026 Application Threat Landscape report covers Q1 2026 telemetry across 11 industries and approximately 569 monitored domains. The first quarter of 2026 confirmed that application-layer threats are structural and persistent across every sector we monitor. Finance recorded a March attack surge driven entirely by API-layer authentication abuse , the first confirmed OWASP API Security Top 10 pattern observed in Prophaze telemetry.



The metric mentioned above define the scope and intensity of Q1 2026 application-layer threat activity across the Prophaze-monitored estate. They establish the baseline against which every industry finding in this report is measured.

1 in 100 requests was an attack

20 million attack events were detected within 2 billion total Q1 HTTP requests a 1% attack-to-traffic ratio across the monitored estate. The 99% of legitimate traffic surrounding every attack is why rule-based and volume-based detection generates unacceptable false positive rates at this scale. Behavioral baselining learning what normal looks like per endpoint is the only detection model that operates accurately within this signal-to-noise environment.

KEY INSIGHT The Q1 API Signal

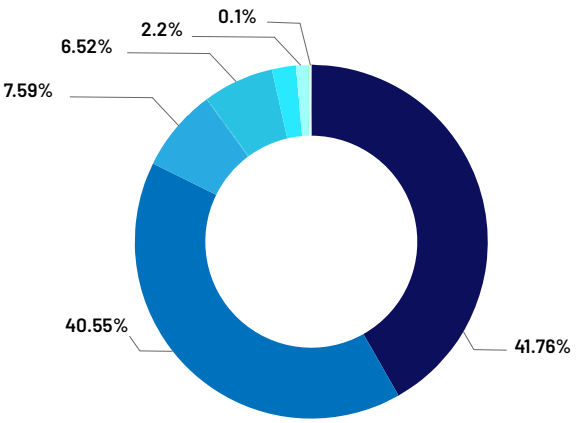
Finance & Banking is the only industry in Q1 2026 telemetry to surface confirmed OWASP API Security Top 10 threats alongside OWASP Top 10. API2:2023 Broken Authentication accounted for 99% of March activity , 1.27 million attack requests in a single month. This is not a statistical anomaly. It marks a structural expansion of the attack surface from web application vulnerabilities into the API authentication layer itself.

Three structural conditions define the Q1 2026 threat environment beyond the Finance API finding. A06 and A03 together account for over 82% of all attacks eliminating these two structural weaknesses would resolve the majority of adversarial exposure for most industries. Attack patterns are increasingly sector-specific: Legal saw a 25-fold volume increase across the quarter; Non-Profit a 1,000-fold surge in a single month. And monitoring gaps are active: Government's 139,000-attack February reconnaissance operated below existing detection thresholds. Q2 is not a story of rising volume across the board, it is one of precise, targeted adversarial activity operating within visibility gaps that volume-based controls will not surface.

OWASP Threat Distribution Across Total Attacks in Q1 In Different Industries

All-Industry OWASP Distribution

This chart shows how Q1 2026's 20 million total attack events are distributed across OWASP threat categories when all 11 monitored industries are combined. Each segment represents that category's share of overall attack frequency , not a severity score or a count of successful breaches, but a measure of where adversarial effort was concentrated across the quarter. It answers a single question: when adversaries targeted applications in this monitored estate, which vulnerability class were they probing most often?



Note: *This chart breaks down Q1 2026's 20 million total attacks by OWASP threat category across all 11 monitored industries. Each slice represents that category's share of the overall attack volume not a severity score, but a frequency distribution showing where adversarial effort was concentrated during the quarter.*

Two categories dominate the chart to a degree that leaves little ambiguity. Vulnerable and Outdated Components (A06) accounts for 41.76% and Injection (A03) accounts for 40.55% . Together they represent over majority of all observed attack activity in Q1. This is not a coincidence of methodology; two consecutive quarters of Prophaze telemetry now confirm that A06 and A03 are the permanent structural dominant threats across the monitored estate, not the result of a single campaign or a single industry's elevated volume.

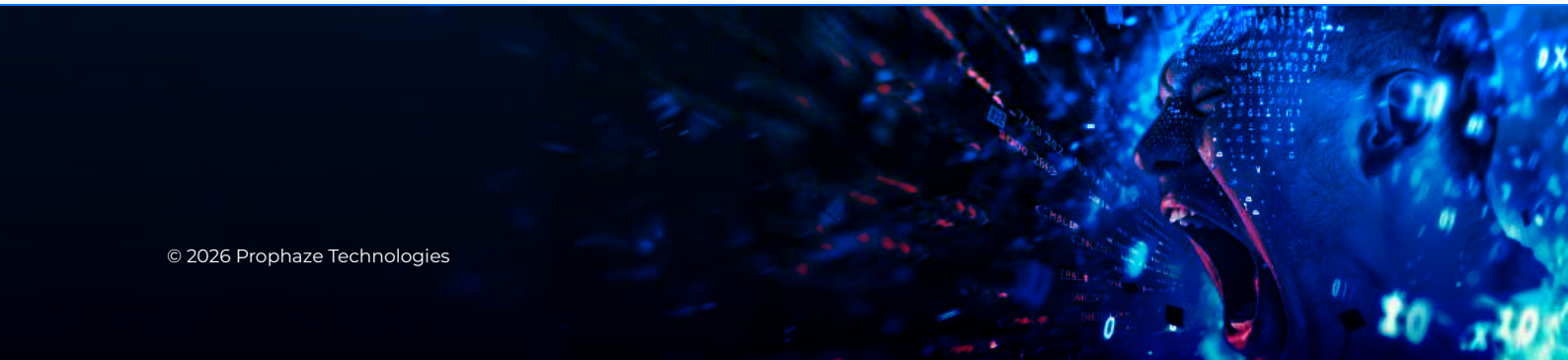
The remaining 18% of attack volume is distributed across nine further OWASP categories. Insecure Design (A04) accounts for 7.59% elevated in Healthcare and Government where architectural decisions made years before modern API consumption patterns existed cannot be retroactively patched. Broken Authentication (A07) sits at 6.52%, driven primarily by Finance's March API2:2023 surge which reached 99% of that industry's single-month activity. Security Misconfiguration (A05) at 2.20% reflects cloud-native sprawl and exposed admin interfaces across Finance, Energy, and Non-Profit environments. All remaining categories sit below 1.2%, though none are absent each represents a confirmed, active attack vector.

Improper Inventory Management and Unrestricted Resource Consumption both register at 0.00% in the all-industry total. This does not mean these attack vectors are absent. Both are confirmed present at negligible rates fewer than 10 events per 100,000 requests and both appear as trace-level signals in Finance's Q1 API telemetry. API4:2023 Unrestricted Resource Consumption in Finance is precisely the kind of near-zero signal that preceded the API2:2023 surge observed in March. Near-zero categories in this chart warrant monitoring, not dismissal.

Q1 2026 OWASP Threat Reference

The table below maps each OWASP category observed in Q1 2026 telemetry to its root cause and the decision it forces. All categories appearing at 0% in specific industries represent confirmed but negligible activity, not absence.

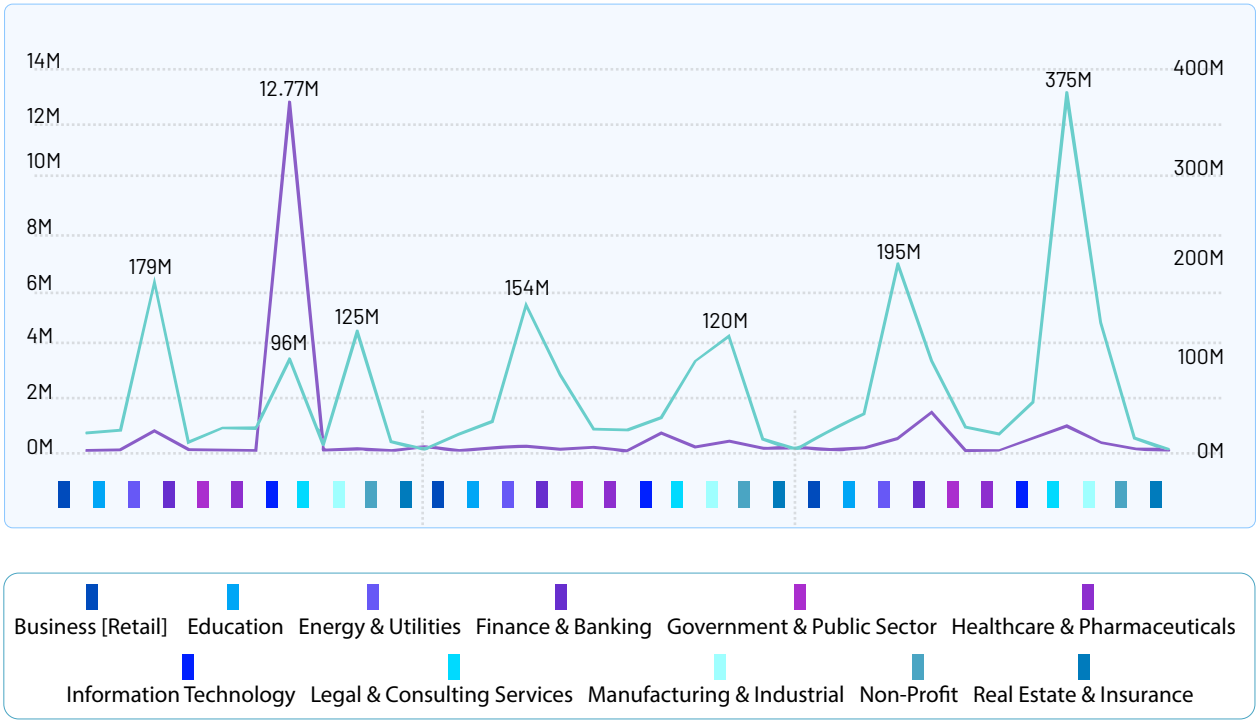
Code	Q1 Industries	Root Cause & Decision Required
A03:2021	Education, Govt, Legal, IT, Non-Profit	Widespread input probing across parameters; consistent cross-industry baseline threat
A04:2021	Healthcare (dominant), Manufacturing, Govt	Architectural weaknesses exposed at runtime; not patch-fixable
A06:2021	Energy (q1 avg 58.15%), Real Estate (q1 avg 96.44%), Business, Legal, Manufacturing	Dominant structural risk driven by legacy/unpatched components
A07:2021	Manufacturing, Finance, Healthcare	Credential stuffing and login abuse patterns observed
A05:2021	Finance, Energy, Non-Profit, Education	Misconfigured or exposed endpoints exploited
A02:2021	Finance, Real Estate, Energy	Legacy encryption usage at low but persistent levels
A09:2021	Government, Energy	Detection gaps allow low-visibility probing
A10:2021	Multiple (low)	Low-frequency SSRF probing observed across industries, indicating early-stage reconnaissance of internal resource access paths.
A01:2021	Energy, Finance, Legal	Low-rate but consistent access bypass attempts
API2:2023	Finance, Q1 Avg 98 % March	High-volume API authentication abuse defining sector risk
API4:2023	Finance (trace)	Low-volume signals of resource exhaustion attempts, indicating early-stage testing for API rate limits and abuse thresholds.
API8:2023	Finance (trace)	Trace-level probing of API configurations, suggesting reconnaissance of exposed endpoints and misconfigured API behaviors.



02 THREAT ACTIVITY & TRENDS

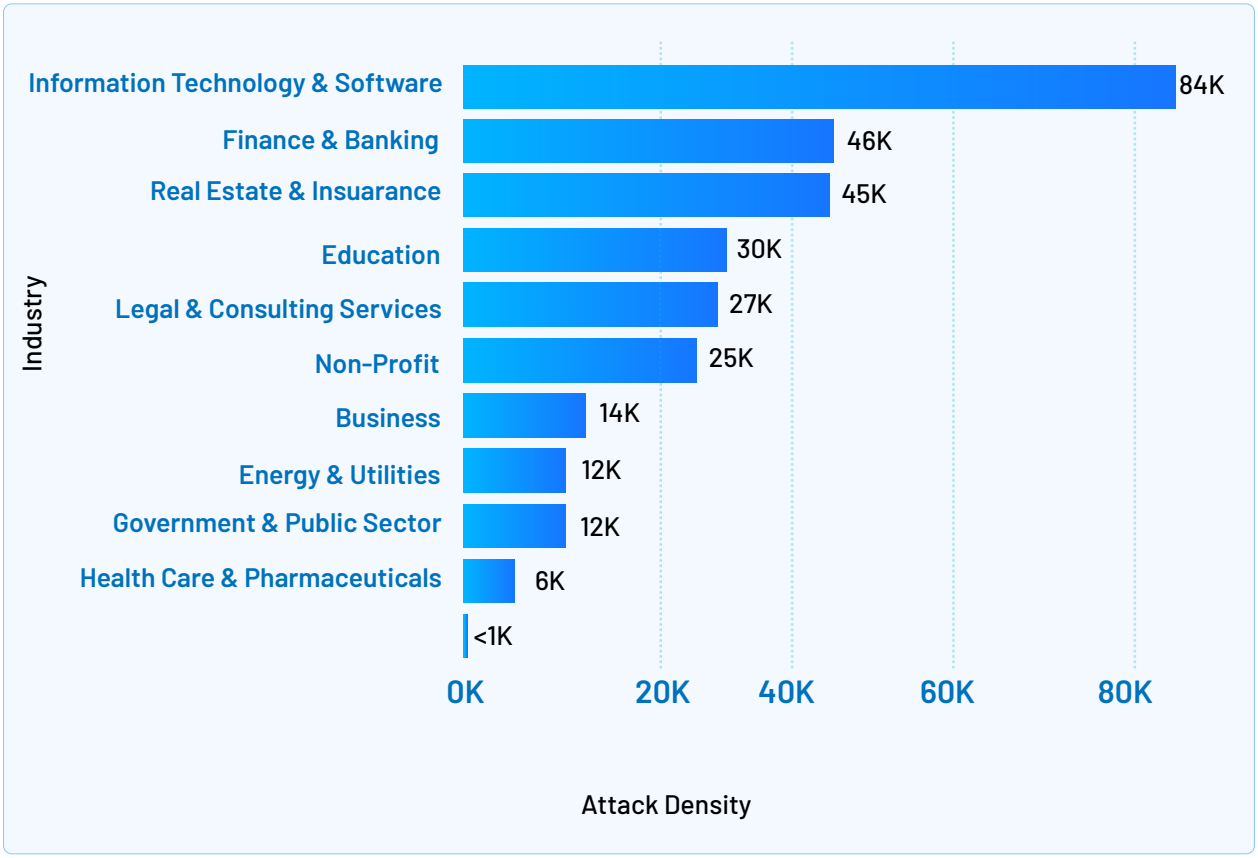
Month-over-Month Attack Activity

Q1 2026 attack volumes show divergent patterns across industries, unlike Q4 2025's consistent escalation. Q1 is characterised by industry-specific surges. Finance dominated March with 1.27M attacks driven by API authentication abuse. IT & Software recorded 11.8M attacks in January alone before normalising. Government showed the inverse, declining from 139K in February to 15.6K in March, consistent with a sustained-presence-then-withdraw reconnaissance pattern.



Note: This chart shows month-over-month trends of total attacks and total traffic across industries. The measures aggregate data at a domain–month level to avoid duplication, providing a clear view of real activity. Gaps between traffic and attacks highlight targeted attack spikes independent of normal usage.

Industry	January	February	March	Pattern
IT & Software	11,808,039	547,564	228,762	Jan spike then normalised , sustained broad-surface probing
Finance & Banking	38,037	24,116	1,274,431	March API surge , API2:2023 at 99% drives explosive growth
Energy & Utilities	412,359	161,512	446,689	Consistent high volume , A06 dominant throughout
Legal & Consulting	24,962	142,259	615,657	Escalating , March 25× January volume
Manufacturing	53,039	183,501	99,201	Feb peak then partial retreat , crawler reconnaissance pattern
Real Estate & Insurance	155,635	130,388	22,878	Declining , high Jan/Feb, lower March
Education	24,559	97,623	89,630	Feb/Mar surge , 4× January
Government	32,858	139,462	15,639	Feb peak then sharp drop , sustained-presence-withdraw pattern
Non-Profit	87	95,915	76,949	Massive Feb/Mar increase from near-zero January
Business	13,243	8,416	41,692	Gradual escalation , low absolute volume
Healthcare	7,765	2,175	3,294	Consistently low , structural risk not reflected in volume



Note : *IT & Software leads at 84K attacks per domain, driven by its January 11.8M spike across 165 domains. Finance and Real Estate & Insurance both sit near 46K, despite very different footprints Finance across 33 domains, Real Estate across just 7. This convergence illustrates the core insight: high-value data targets attract concentrated adversarial attention regardless of estate size. Healthcare, despite its near-zero density (0K on this scale), carries the highest structural risk per compromise a low attack rate should not be read as low threat.*

Raw attack volume is an incomplete risk signal. An industry with 500 monitored domains will accumulate far more total attacks than one with 7, even if the smaller sector is under far more intense adversarial pressure per asset. Attack density corrects for this by dividing each industry's total Q1 attack count by the number of unique monitored domains it contains, producing a like-for-like comparison of targeting intensity across sectors of very different sizes. A high density figure means each domain in that industry is absorbing a disproportionate volume of attack traffic and by extension, that a single undetected compromise carries a concentrated risk.

IT & Software leads at 84K attacks per domain, driven by a January spike of 11.8 million attacks across its 165-domain estate consistent with automated broad-surface CVE scanning and injection probing at scale. Finance and Real Estate & Insurance converge near 46K and 45K respectively, despite having very different footprints: Finance spans 33 domains, Real Estate just 7. This convergence is not accidental both sectors hold high-value financial data that motivates concentrated, targeted adversarial attention regardless of how many assets are exposed. Education at 30K reflects semester-driven surges that are predictable and seasonal. Energy and Government both sit at 12K, yet their structural risk profiles differ significantly: Energy's density is distributed across 113 domains, Government's across just 16.

84K
IT & Software - Highest Density

46K
Finance - 33 domains

45K
Real Estate - 7 domains

< 1K
Healthcare - low volume, high structural risk

03 OWASP INTELLIGENCE

Top Q1 Weighted Threat by Industry

This view highlights the dominant OWASP threat patterns across industries in Q1 2026 using weighted attack distribution. Percentages represent the average share of each OWASP category within total attacks, calculated at a domain–month level to prevent duplication and ensure accuracy.

The data shows clear structural concentration: A06 (Vulnerable & Outdated Components) and A03 (Injection) dominate most industries, while Finance & Banking stands apart, with API2:2023 Broken Authentication accounting for the overwhelming majority of activity. This confirms a shift from traditional web vulnerabilities toward API-layer risk in high-value sectors.

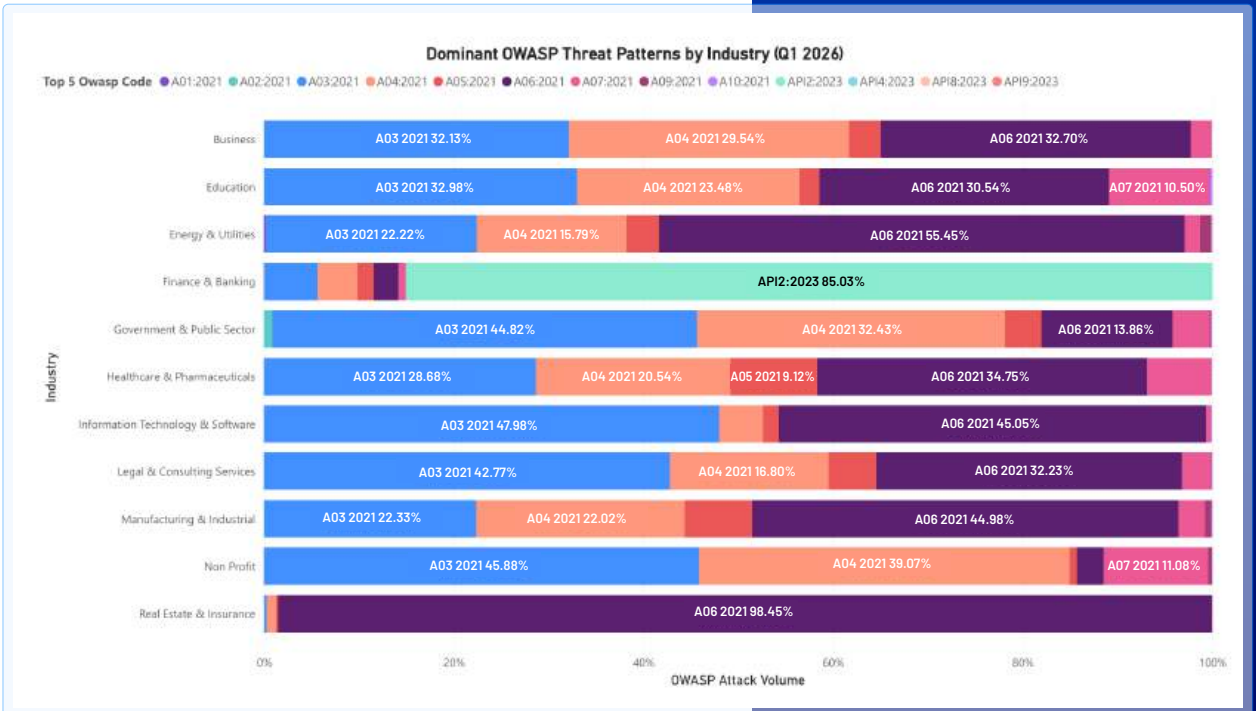
Attack composition varies significantly by industry. Some sectors (e.g., Real Estate, Energy) are heavily concentrated in a single weakness, while others (e.g., Government, IT) show a more distributed attack surface—indicating broader exposure and testing behavior.

Industry Threat Composition: Q1 2026

Data Methodology: Average Q1 attack shares are weighted by volume to identify sustained adversarial trends across industry domains.

The API Pivot: A06 and A03 remain the global baseline, but Finance stands apart with a massive concentration in API Authentication abuse.

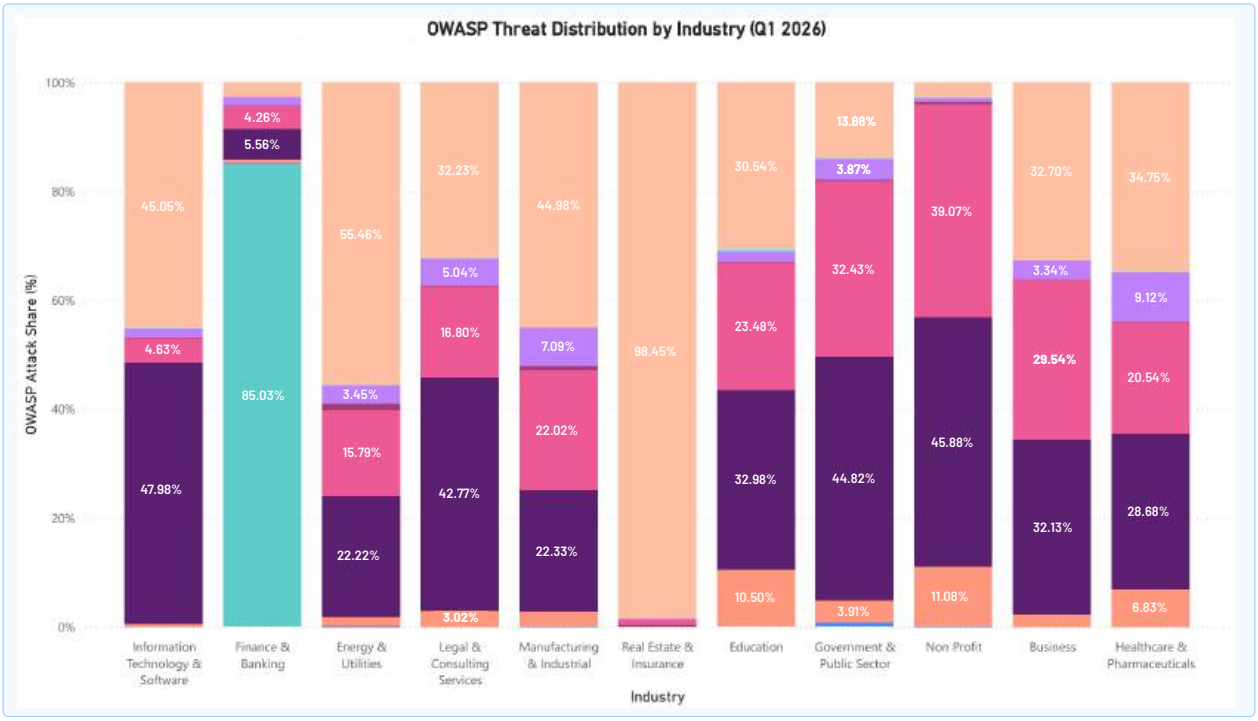
Exploitation vs Probing: Attack patterns vary from concentrated exploits in Real Estate to broad, multi-vector testing in Government and IT sectors.



04 INDUSTRY INTELLIGENCE

Industry Intelligence: Sector-Wise OWASP Threat Profiles (Q1 2026)

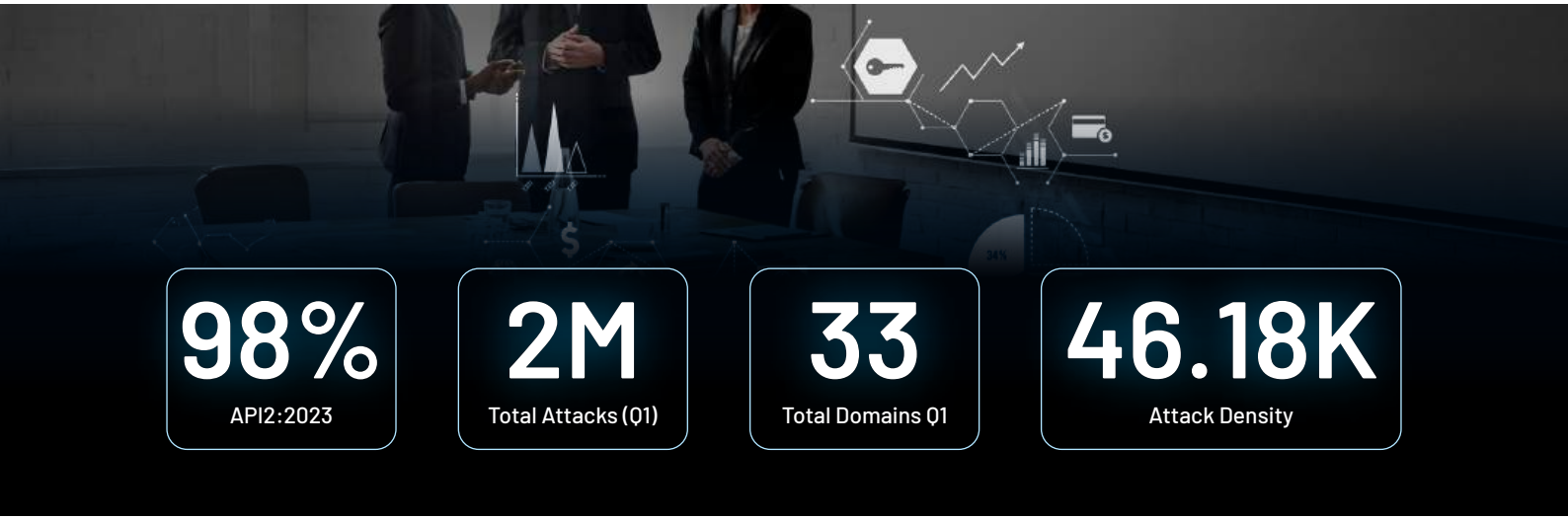
This section analyzes how OWASP Top 10 risks manifest across industries based on Q1 2026 telemetry. Each sector demonstrates distinct attack patterns driven by infrastructure maturity, application architecture, and operational constraints.



Note : Shows the proportional distribution of OWASP attack categories across industries, highlighting dominant threat classes within each sector.

Industry	Top OWASP Threats	Avg Q1 %	Defining Pattern
IT & Software	A03:2021 Injection	41.3%	Highest absolute attack volume · A03 leads over A06 · Multi-vector surface across 165 domains
Finance & Banking	API2:2023 Broken Authentication	97.97%	Only industry with confirmed API Security Top 10 · March 99% · 1.27M single-month surge
Energy & Utilities	A06:2021 Vulnerable Components	57.7%	Most extreme single-sector concentration in Q1 dataset
Legal & Consulting	A03:2021 Injection	42.8%	Highest injection rate in dataset · Document workflow vectors · March 25× January
Manufacturing	A06:2021Vulnerable Components	43.5%	OT-IT middleware on legacy cycles · Supply chain portal risk · A07 peaked 31% Jan
Real Estate & Insurance	A06:2021Vulnerable Components	95.7%	7 domains · Near-total component concentration · Second-highest density in dataset
Education	A03:2021 Injection	34.1%	LMS and SIS search interfaces · Feb semester surge 4× January · A07 42% in February

Finance & Banking



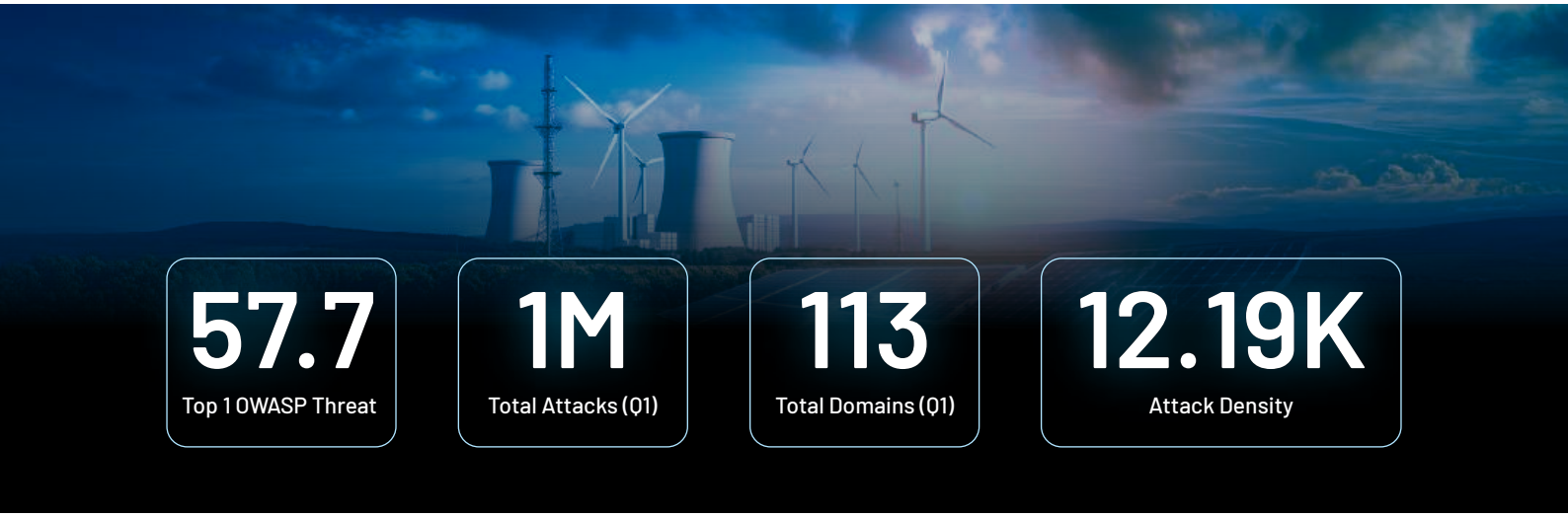
98%	2M	33	46.18K
API2:2023	Total Attacks (Q1)	Total Domains Q1	Attack Density

98% API2:2023 Broken Authentication	18.5 % A03:2021 Injection	15.7 % A04:2021 Insecure Design
❖ March attack surge, 1.27M requests targeting API authentication endpoints	❖ Legacy core banking APIs, SQL probing across payment gateway callbacks	❖ Authorisation logic gaps in multi-product banking interfaces
❖ Missing or improperly implemented token validation on financial APIs	❖ Parameter injection across loan and account management endpoints	❖ Parameter tampering against account and transaction APIs
❖ OAuth flow weaknesses and session token manipulation probed at scale	❖ Cross-service injection attempts exploiting inconsistent validation	❖ Trust boundary violations between customer-facing and internal systems

KEY INSIGHT Q1 2026 Pattern

Finance is the only industry in Q1 2026 telemetry to surface confirmed OWASP API Security Top 10 threats alongside OWASP Top 10. API2:2023 Broken Authentication at 99% for March specifically across 1.27 Million attack requests , is not noise. It represents automated toolkits systematically probing API authentication endpoints for missing token validation, weak session management, and bypassed authorisation checks. This is structurally different from web application attacks and requires API-layer protection, not just WAF rules.

Energy & Utilities



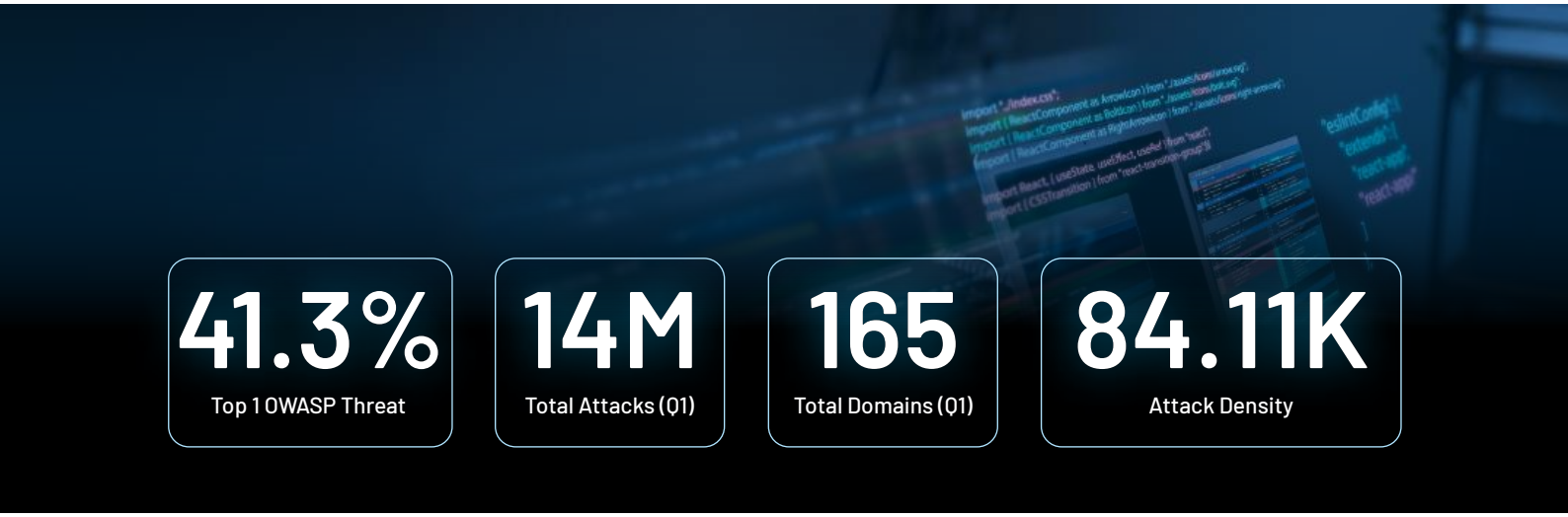
57.7	1M	113	12.19K
Top 1 OWASP Threat	Total Attacks (Q1)	Total Domains (Q1)	Attack Density

57.7% A06:2021 Vulnerable Components	15.9% A04:2021 Insecure Design	19.5% A03:2021 Injection
❖ Operational software on multi-year qualification and certification cycles	❖ APIs bridging customer-facing portals and operational domains without sufficient trust boundaries	❖ Customer portal search and query interfaces with legacy input handling
❖ Vendor platforms at end-of-support still running in production	❖ Design decisions in legacy billing systems create exploitable authorisation gaps	❖ Billing APIs accepting customer-supplied account parameters without uniform validation
❖ Geographic distribution creates inconsistent patch visibility across 100-domain estate		

KEY INSIGHT Q1 2026 Pattern

A06 at 57.7% across Q1 is the most extreme single-sector OWASP concentration in the dataset. This is not a patching failure , it is a structural governance problem unique to operational technology environments. Multi-year qualification and certification cycles mean component upgrades are constrained by operational continuity requirements, not negligence. The adversarial implication is that every known CVE against components in the energy estate remains an active, exploitable attack surface until compensating controls are in place at the application layer.

Information Technology & Software



41.3%	14M	165	84.11K
Top 1 OWASP Threat	Total Attacks (Q1)	Total Domains (Q1)	Attack Density

28.1% A06:2021 Vulnerable Components

- SaaS platforms integrating open-source libraries per product release
- CI/CD pipelines pulling dependencies without automated validation gating
- January spike of 11.8M attacks confirms automated CVE scanning at scale

41.3% A03:2021 Injection

- Customer-facing REST and GraphQL APIs with diverse input surfaces
- Multi-tenant platforms where one tenant's input can affect another's data
- SQL, command, and LDAP probing across every accessible API parameter

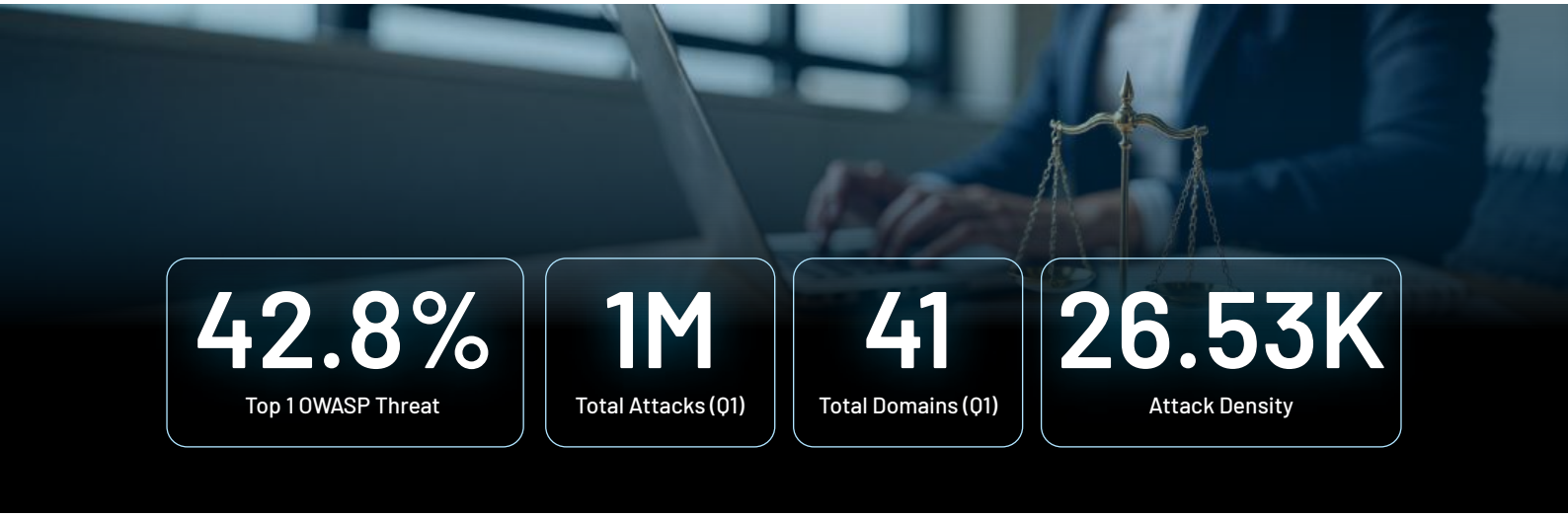
20.5% A04:2021 Insecure Design

- Security architecture review cannot pace microservice deployment velocity
- API versioning creates parallel attack surfaces with inconsistent controls
- Authorisation logic gaps accumulating as services scale independently

KEY INSIGHT Q1 2026 Pattern

IT & Software accounts for the highest absolute Q1 attack volume at 14 million requests , driven by a January spike of 11.8M that normalised through February and March. Three OWASP categories , A03 , A06 , A04 are at 41.3% , 28.1% and 20.5% for Q1 avg. This is the signature of a fully active, multi-vector attack surface where adversaries are simultaneously fingerprinting components, probing injection vectors, and testing design logic flaws across 103 domains.

Legal & Consulting Services



42.8%	1M	41	26.53K
Top 1 OWASP Threat	Total Attacks (Q1)	Total Domains (Q1)	Attack Density

42.8% A03:2021 Injection

- Document management workflows with legacy SQL construction in matter search
- Per-engagement portal customisation creates inconsistent input validation across deployments
- LDAP probing against client directory and matter management systems

35.8% A06:2021 Vulnerable Components

- Document management platforms on extended vendor upgrade cycles
- Matter-specific portal deployments using outdated framework versions
- Aggregated vulnerability exposure across 41 domains

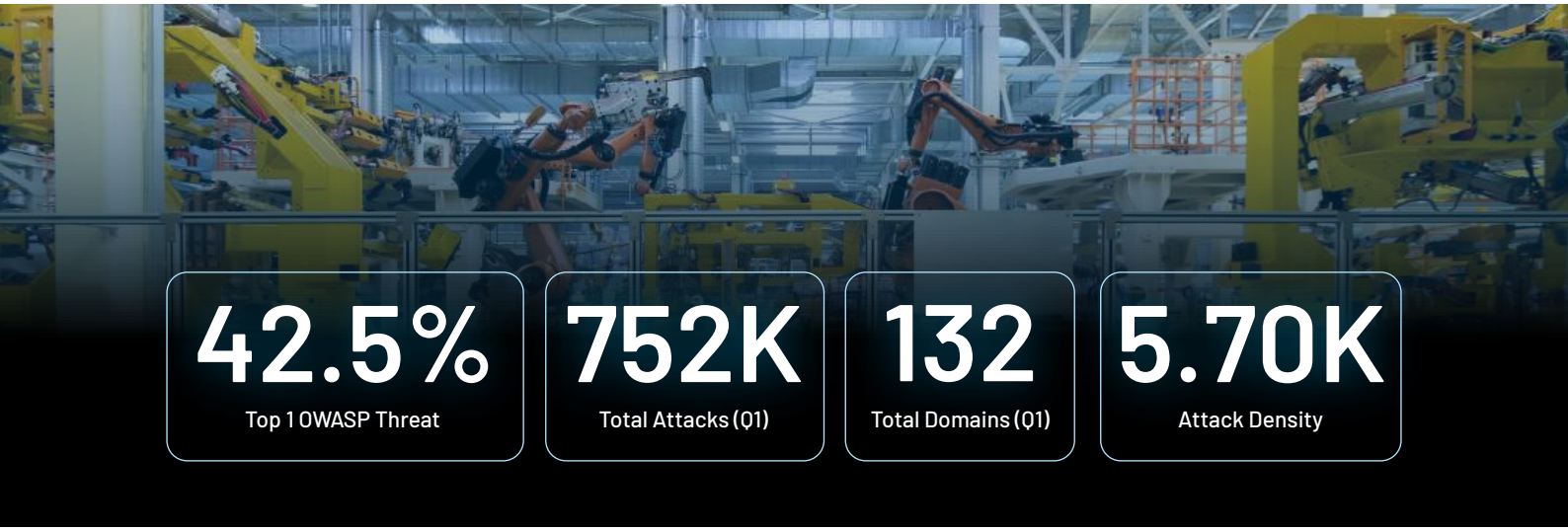
14.4% A04:2021 Insecure Design

- Authorisation logic inconsistently enforced across per-client portal customisations
- Cross-matter data access scenarios not covered by original access control design
- Trust boundaries not designed for modern API consumption of legacy case management systems

KEY INSIGHT Q1 2026 Pattern

Legal & Consulting's document management workflows create structural injection risk at 42.8% Q1 average. SQL-heavy matter search interfaces, LDAP-connected client directories, and per-engagement portal customisations each introduce localised input validation gaps characteristic of legal tech stacks. March attacks reached 615,657 , 25× January volume showing escalating adversarial attention on these case-sensitive systems as the quarter progressed.

Manufacturing & Industrial



42.5%	752K	132	5.70K
Top 1 OWASP Threat	Total Attacks (Q1)	Total Domains (Q1)	Attack Density

43.5% A06:2021 Vulnerable Components

- Industrial software and OT-IT integration middleware on extended operational lifecycles
- ERP and supply chain portal components operating beyond support windows
- February 183K attack peak consistent with automated CVE scanning phase

22.2% A04:2021 Insecure Design

- Supply chain portal APIs accepting diverse supplier input without consistent trust boundaries
- IT-OT integration pathways designed before modern API consumption patterns existed
- Authorisation gaps at the boundary between supplier portals and internal manufacturing systems

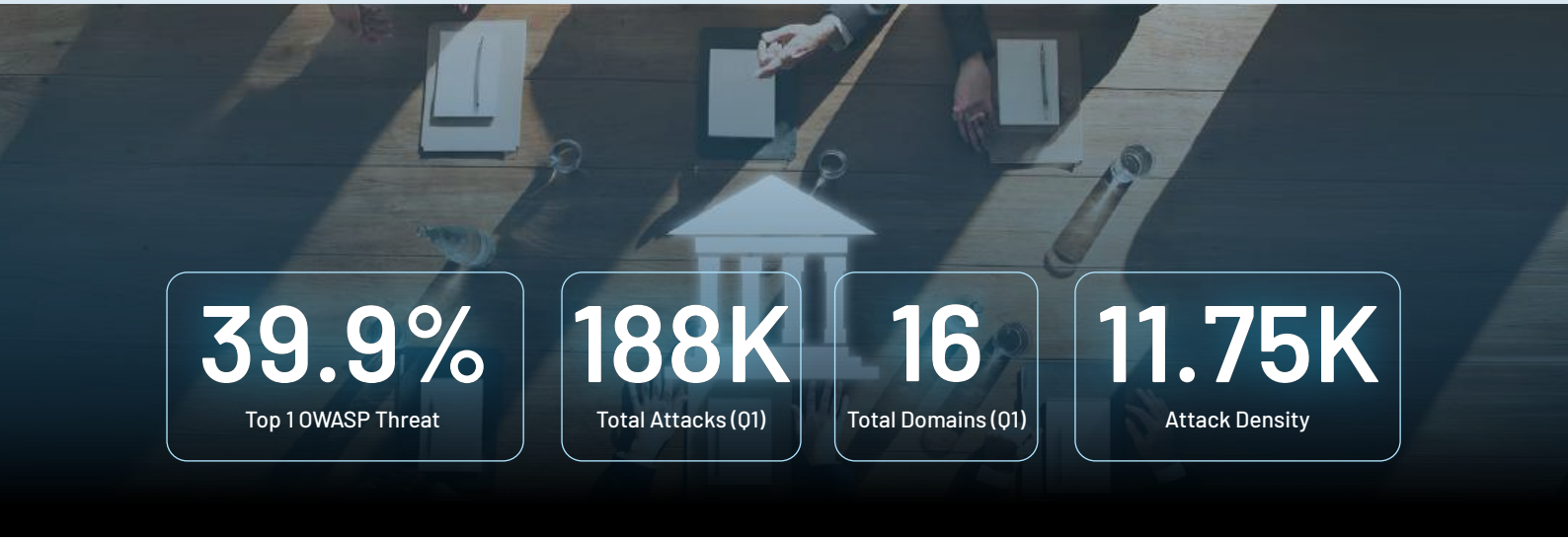
23.8% A03:2021 Injection

- Supply chain portal APIs accepting diverse supplier-provided input
- Production analytics dashboards with user-supplied query parameters
- SQL probing across logistics and inventory management interfaces

KEY INSIGHT Q1 2026 Pattern

Manufacturing's A07 Authentication Failures peaked at **31%** for January , while not the leading threat by percentage , carries the most consequential risk in the dataset. Automated credential attacks against supply chain portal authentication are not just account takeover attempts. Each supply chain portal represents a potential IT-OT entry pathway. A compromised supplier credential is a potential access route into operational technology networks, production systems, and industrial control infrastructure. This makes authentication failure in Manufacturing a board-level operational continuity question, not an IT security metric.

Government & Public Sector



39.9% A03:2021 Injection

- Legacy citizen service platforms with inconsistent form parameterisation
- Inter-agency APIs with procurement-managed inconsistent input validation
- February sustained presence at 139K attacks , full-month persistent probing

27.1% A04:2021 Insecure Design

- Multi-decade citizen platforms , threat models never updated
- Authorisation logic not designed for modern API consumption patterns
- Design debt accumulated across consecutive government IT procurement cycles

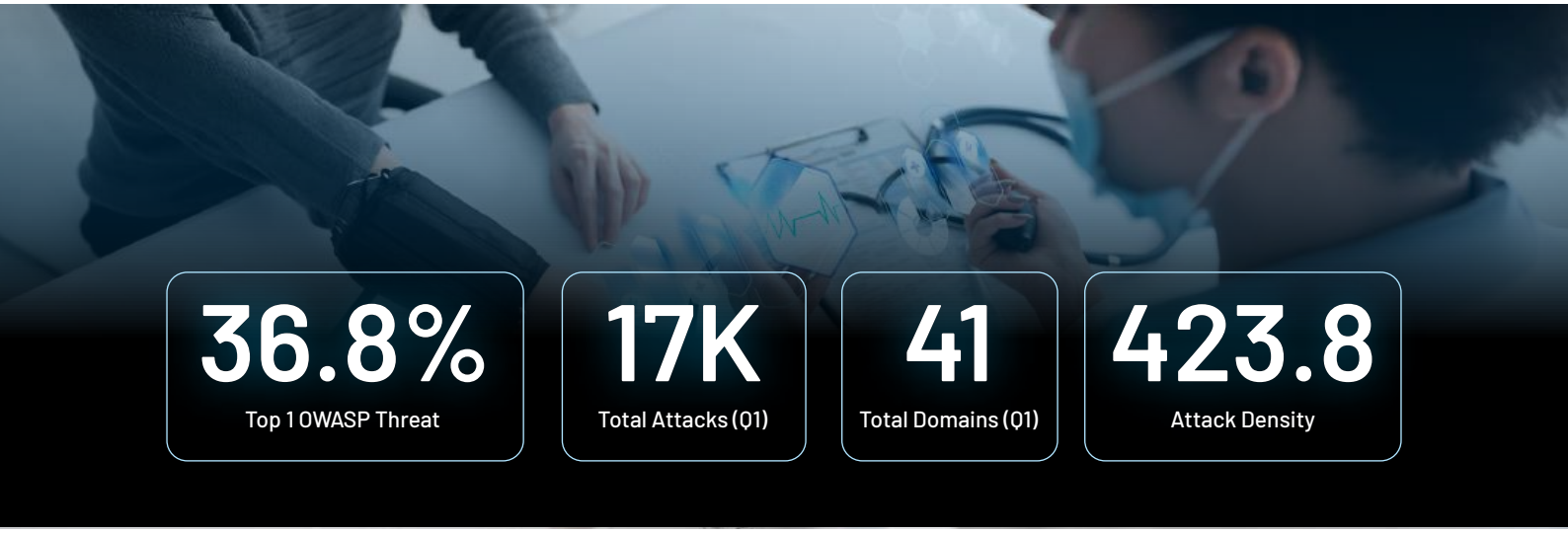
22.0% A06:2021 Vulnerable Components

- Legacy procurement: Multi-year contracts lock agencies into outdated vendor software
- Siloed palnter-agency systems with inconsistent update cadences
- PII breaches in citizen portals or service outages affect national security

KEY INSIGHT Q1 2026 Pattern

Government's Q1 pattern is structurally significant: **139K attacks** in February followed by a sharp decline to 15.6K in March. This is not a security improvement , it is a reconnaissance-then-withdraw pattern consistent with adversaries completing their intelligence-gathering phase before moving to targeted exploitation. A09 Logging and Monitoring Failures at 1.24% during March means the February probing operated largely below existing detection thresholds. The combination of sustained presence and monitoring gaps creates conditions for undetected persistent access that standard volume-based alerting will not surface

Healthcare & Pharmaceuticals



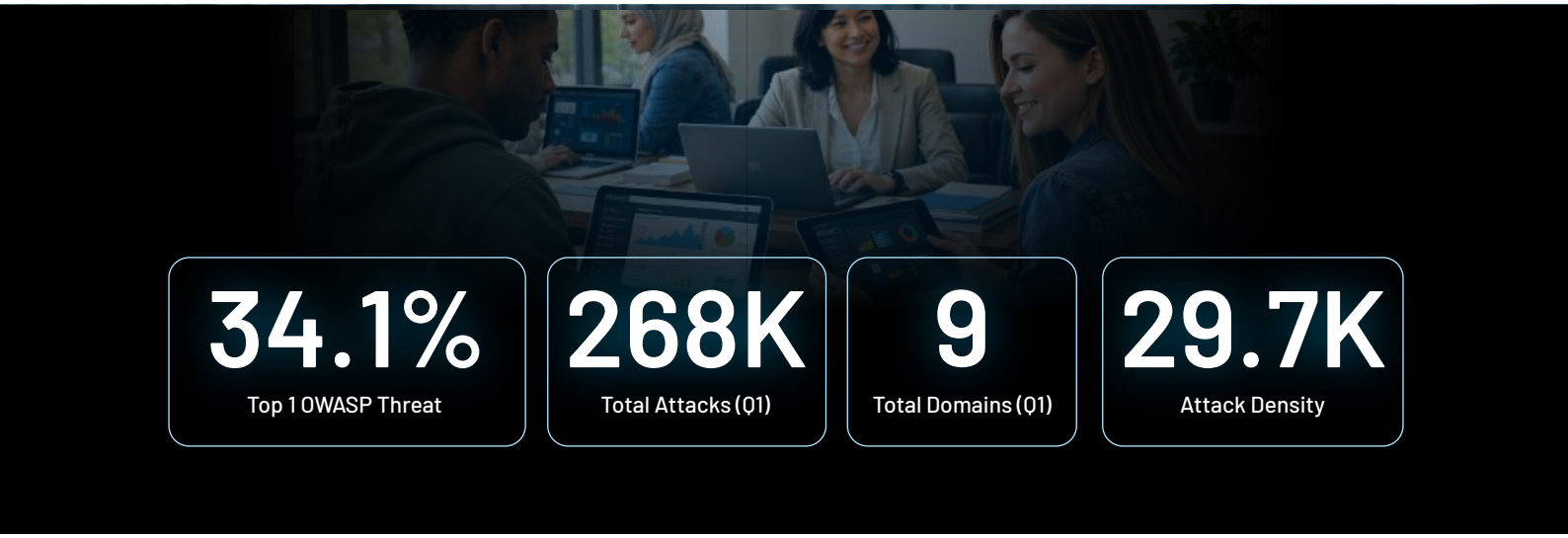
36.8%	17K	41	423.8
Top 1 OWASP Threat	Total Attacks (Q1)	Total Domains (Q1)	Attack Density

21.6% A04:2021 Insecure Design	36.8% A06:2021 Vulnerable Components	27.1% A03:2021 Injection
❖ Modern patient portals built atop legacy clinical backends , inconsistent trust boundaries	❖ Clinical platforms on extended certification cycles , remediation constrained by regulatory timelines	❖ Patient-facing EHR APIs with legacy input parameterisation
❖ Authorisation logic inconsistently enforced across patient and insurance APIs	❖ Third-party diagnostic integrations with vendor-controlled patch cadences	❖ SQL and LDAP probing against clinical directory and records systems
❖ Design decisions made for pre-API clinical architectures now exposed to modern consumption patterns	❖ Component vulnerability surface grows as certification cycles extend	❖ Insurance API endpoints without uniform input validation

KEY INSIGHT Q1 2026 Pattern

Healthcare shows A06 Vulnerable Components (36.8%) leading over A04 Insecure Design (21.6%). This is a patching-constrained problem amplified by regulatory certification cycles, not just design debt. Clinical platforms can't patch freely due to FDA/HIPAA timelines, making runtime behavioral monitoring essential to protect unpatchable component flaws.

Education



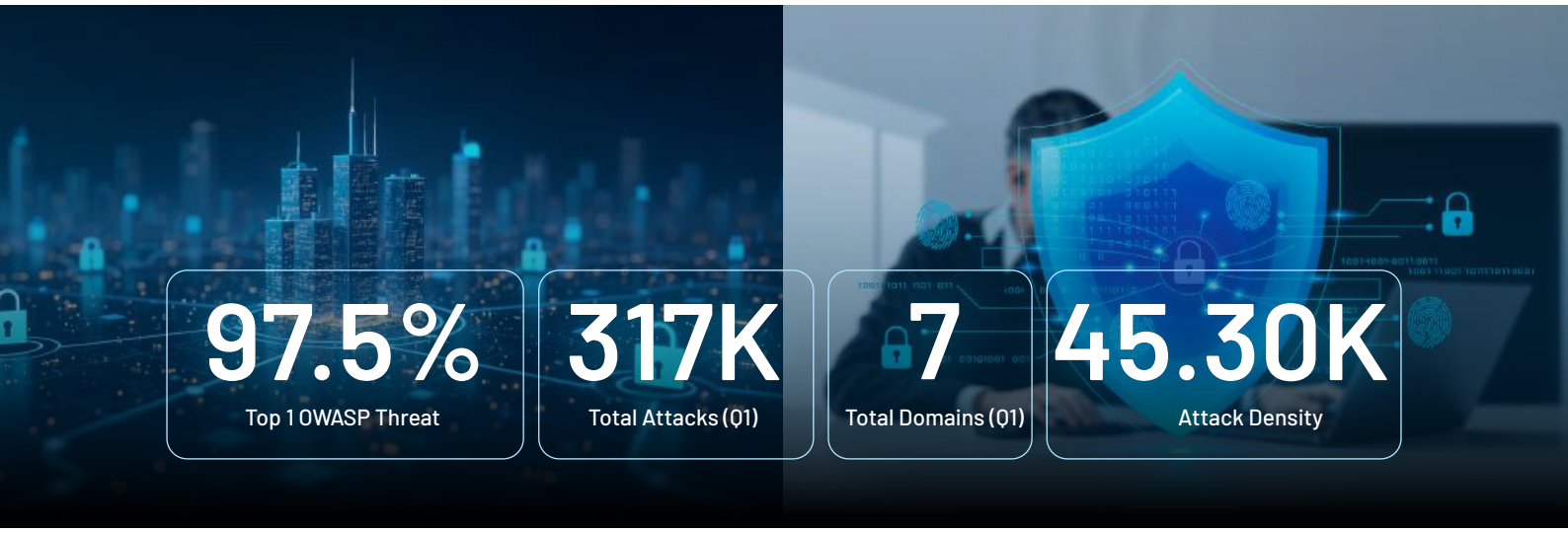
34.1%	268K	9	29.7K
Top 1 OWASP Threat	Total Attacks (Q1)	Total Domains (Q1)	Attack Density

34.1% A03:2021 Injection	29.9% A04:2021 Insecure Design	19.2% A06:2021 Vulnerable Components
❖ Database-driven LMS with diverse student-generated input channels	❖ Multi-year academic software licenses lock institutions into unpatched versions	❖ Applications built over institutional timescales without central security review
❖ SIS search interfaces with legacy SQL construction	❖ Decentralized departmental systems with inconsistent vendor patch management	❖ Decentralised departmental stacks with divergent security assumptions
❖ Research repositories without uniform input validation across departmental deployments	❖ Open-source learning tools with delayed security updates across campus deployments	❖ Authorisation not designed for modern cross-system student data access

KEY INSIGHT Q1 2026 Pattern

Education's February surge from 24K to 97K attacks , a 4× increase , aligns structurally with semester-start periods when student portal authentication traffic peaks and credential stuffing campaigns intensify. A07 Authentication Failures at **42.38% for February** is the second-highest in the dataset after Manufacturing, confirming that automated login attacks track academic calendars as reliably as they track commercial peak periods. Decentralised IT across departmental LMS and SIS deployments means injection vulnerabilities exist across multiple independently managed surfaces without central security visibility.

Real Estate & Insurance



43.5% A06:2021 Vulnerable Components

- Legacy insurance platform components at extended vendor upgrade cycles
- Smallest domain footprint in dataset , just 4 domains , yet second-highest attack density
- High personal financial data value drives concentrated adversarial targeting of known CVEs

23.8% A03:2021 Cryptographic Failures

- Legacy encryption in property/title databases and policy storage systems
- Weak key rotation practices across multi tenant real estate/insurance platforms
- Insecure PII transmission between agents, brokers, and centralized records

22.2% A04:2021 Insecure Design

- Authorisation logic in insurance APIs not designed for modern direct-to-consumer access
- Parameter tampering against policy and claim status interfaces
- Trust boundary weaknesses between customer-facing portals and core insurance systems

KEY INSIGHT Q1 2026 Pattern

Real Estate & Insurance has the second-highest attack density in the Q1 dataset despite having only 4 monitored domains. 308,901 attacks across 4 domains produces an attack density that vastly exceeds its footprint. The structural driver is data value , insurance platforms process personal financial data, policy information, and claims history that adversaries target specifically for their intelligence and fraud value. A06 at 95.7% means nearly every attack is targeting a known component vulnerability on platforms where upgrade cycles are constrained by insurance system certification requirements.

Business Services

39.1% A03:2021 Injection	34.1% A04:2021 Insecure Design	17.3% A06:2021 Vulnerable Components
❖ CMS-driven donation and contact interfaces with inconsistent input validation	❖ Applications built without dedicated security review on small-organisation timescales	❖ CMS plugin ecosystems with unmaintained or abandoned dependencies
❖ SQL probing across member management and fundraising database APIs	❖ Authorisation logic not designed for public-facing API access patterns	❖ Donation platform components operating beyond vendor support windows
❖ Injection attempts tracking seasonal campaign activity periods	❖ Trust boundary weaknesses in payment and donation processing workflows	

KEY INSIGHT Q1 2026 Pattern

Non-Profit recorded 87 attacks in January , then 95,915 in February and 76,949 in March. This is a greater than 1,000× increase. The February surge is not random. CMS-driven estates with unmaintained plugin ecosystems and publicly accessible donation and contact interfaces become targeted when adversaries identify the vulnerability profile through January reconnaissance. The low internal security resource typical of non-profits means this surge lands without the detection infrastructure to identify it until damage has occurred.

05 ADDRESSING THE FINDINGS

How Prophaze WAAP Closes These Gaps

The findings in this report are not theoretical. Every OWASP category, attack volume figure, and threat percentage reflects real probing activity observed in Q1 2026 telemetry. The structural conclusions, API authentication is a new primary attack surface, injection remains the cross-sector dominant threat, component vulnerabilities require runtime compensating controls, and monitoring gaps enable persistent access point to specific capability requirements.

Threat pattern	Evidence from Q1	Adaptive WAAP
Cross-sector injection probing across API parameters A03:2021	Education **34.1%** · Govt **39.9%** · Legal **42.8%** · IT **41.3%** · Non-Profit **39.1%**	ML-driven per-endpoint behavioral baselining detects SQL, LDAP, and command injection payloads , including novel variations , inline before they reach application logic. No static signature rules to bypass.
Threat pattern	**Evidence from Q1**	**Adaptive WAAP**
API authentication endpoint abuse at scale API2:2023	Finance · 99% of March activity · 1.27M requests	ML-driven per-endpoint behavioral baselining detects SQL, LDAP, and command injection payloads , including novel variations , inline before they reach application logic. No static signature rules to bypass.
Threat pattern	**Evidence from Q1**	**Virtual Patching**
Component CVE exploitation on constrained upgrade cycles A06:2021	Energy **57.7%** · Real Estate **95.7%** · Manufacturing **43.5%**	CVE exploitation intercepted at Layer 7 before reaching the vulnerable component. No code changes, no service interruption. The primary risk management option where operational or certification cycles prevent direct remediation.
Threat pattern	**Evidence from Q1**	**Runtime Behavioral Monitoring**
Insecure Design exploitation at runtime A04:2021	Healthcare **21.6%** Government **27.1%** Manufacturing **22.2%**	Authorisation bypass, parameter tampering, and trust boundary violations detected through deviation from learned behavioral baselines. Cannot be patched retroactively , only detectable at runtime.
Threat pattern	**Evidence from Q1**	**Bot Mitigation**
Automated credential stuffing at login endpoints A07:2021	Manufacturing supply chain portals · Finance · Healthcare	AI behavioral fingerprinting distinguishes automated credential-testing toolkits from legitimate users by analysing request cadence, session structure, and behavioral signatures , without CAPTCHA friction.
Threat pattern	**Evidence from Q1**	**SIEM / 24×7 Analysts**
Persistent probing below monitoring thresholds A09:2021	Government · Feb 139K attacks operated below detection thresholds	Native SIEM/SOAR integration feeds application-layer behavioral anomaly telemetry into existing SOC infrastructure. Prophaze's 24×7 human analysts surface persistent low-volume probing that volume-based alerting misses entirely.

06 Q4 2025 VS Q1 2026

Comparisons, Findings & Q2 2026 Outlook

Q1 2026 telemetry establishes baseline patterns that have direct implications for Q2. The Finance API2:2023 surge, the Legal escalation from 25K to 615K, and the Government reconnaissance-withdraw pattern are not isolated events , they are indicators of adversarial intent and capability that will carry forward.

Q4 2025 Vs Q1 2026 - What Changed, What Intensified, And What Emerged For The First Time

Dimension	Q4 2025	Q1 2026	Observation
Attack pattern	Consistent 10× escalation Oct - Dec across all sectors	Divergent, industry-specific surges , not uniform escalation	Q1 adversarial behaviour is more targeted and sector-specific than Q4's broad campaign wave
Top threat (all-industry)	A06 Vulnerable Components dominant at 32.9%	A06 Vulnerable Components dominant at 41.76% of total attacks	A06 concentration increased quarter-over-quarter. Component exploitation is deepening, not plateauing
Second threat (all-industry)	A03 Injection at 25.2%	A03 Injection at 40.55% of total attacks	Injection surged significantly in Q1. Now effectively tied with A06 as the primary structural threat
Highest attack volume	IT & Software , 91% of Q4 total volume	IT & Software , highest Q1 volume at 14M	IT & Software remains the dominant attack volume sector across both quarters
Fastest-escal ating sector	Government: 1.00 sustained presence score in December	Finance: March surge from 24K - 1.27M driven by API2:2023	Different sectors dominated each quarter , broad adversarial targeting rotation
New threat category	OWASP Web Application Top 10 only	OWASP API Security Top 10 confirmed , Finance API2:2023 at 99% March	First API Security Top 10 threat observed in Prophaze telemetry. Attack surface has expanded
Healthcare pattern	A06 43% · Low density · Dec presence 0.77	A06 36.8% leads · A04 21.6% · Consistent low volume	A06 reduced slightly. A04 Insecure Design growing as secondary structural risk in clinical platforms
Government pattern	December sustained presence 1.00 , full-month persistent probing	February surge 139K then sharp withdrawal to 15.6K in March	Shifted from sustained persistence in Q4 to reconnaissance and with draw model in Q1
Energy Sector Pattern	**A06 74% , most extreme Q4 concentration**	A06 57.7% , still most extreme Q1 concentration	A06 dominance reduced but remains the most concentrated sector. Structural governance problem persists
Legal & Consulting	Not in Q4 top-tier escalation sectors	March at 25× January volume , 615K attacks	Legal sector emerged as a new high-attention target in Q1 with no Q4 precedent in the dataset
Non-Profit	A06 96% , most extreme Q4 single-sector concentration	A03 39.1% leads with 1,000× Jan-to-Feb surge	Threat profile shifted from component-dominant to injection-dominant. Adversarial approach evolved

KEY COMPARISON FINDING **What Q4 and Q1 Together Confirm**

Two consecutive quarters of telemetry now establish a structural baseline: A06 Vulnerable Components and A03 Injection are not tactical campaign choices , they are the permanent dominant threat categories across the monitored estate. Every sector carries at least one of them as a leading threat. What changed between Q4 and Q1 is the method, not the target. Finance moved from TLS cipher probing to API authentication abuse. Non-Profit moved from component exploitation to injection. Government moved from sustained persistence to reconnaissance and withdraw. The structural weaknesses being exploited are the same. The adversarial toolkits are evolving

Q2 2026 Outlook — Directional Forecasts Based On Q1 2026 Telemetry Signals

Each forecast below is grounded in a specific Q1 data signal. The direction indicator reflects trajectory: escalating means a confirmed adversarial toolkit with no observed plateau; persistent means a structural condition unchanged between quarters; emerging means early-stage reconnaissance signals that a new threat category is entering the estate at scale.

	**Escalating** Finance API authentication attacks	API2:2023 at 99% of March is a confirmed adversarial toolkit. Q2 will see this technique deployed against Finance and other API-heavy industries. API4 and API8 traces in Q1 confirm broader API reconnaissance already underway.
	**Escalating** Legal sector attack volume	March at 25× January with no plateau. Adversarial attention to document management and matter data is intensifying. Legal's A03 at 42.8% is the highest injection rate in the Q1 dataset.
	**Emerging** API Security Top 10 expansion	Finance's API2, API4, API8 in Q1 , even at trace levels , confirms API-layer reconnaissance is underway across the broader monitored estate. Expect API threat categories to appear in additional industries in Q2.
	**Persistent** A06 component exploitation	Energy, Real Estate, and Manufacturing all carry structural upgrade constraints unchanged in Q2. Q4-to-Q1 showed A06 increasing from 32.9% to 41.76% of total attacks. Trajectory is upward.
	**Persistent** Government targeted probing	February's reconnaissance-withdraw pattern signals intelligence already gathered for Q2 exploitation. The A09 logging gap at 1.24% means Q2 exploitation may not surface through volume-based monitoring.
	**Persistent** Cross-sector injection campaigns	A03 dominant in five simultaneous industries in Q1, up from Q4's similar pattern. Two consecutive quarters confirm this is structural, not tactical.
	**Persistent** Healthcare structural risk	A06 36.8% and A04 21.6% reflect certification and design constraints that will not change in Q2. Low attack density should not be interpreted as low risk , structural exposure remains elevated.

07 CONCLUSION

The Single Most Important Q1 2026 Takeaway

Finance's API2:2023 at 99% of March activity marks the first confirmed API Security Top 10 pattern in Prophaze Q1 telemetry.

The attack surface has expanded beyond OWASP Web Application Top 10 into API-layer authentication. Injection remains the cross-sector dominant threat in five simultaneous industries. Component vulnerabilities require application-layer compensating controls where upgrade cycles cannot accelerate. These are structural conditions, not episodic incidents. They will persist in Q2 unless addressed at the runtime protection layer.

Q1 2026 confirms a structural shift in application threats attacks are now targeted, sector-specific, and aligned to architectural weaknesses.
The emergence of API2:2023 Broken Authentication (99% of Finance's March activity) marks a clear expansion of the attack surface into API authentication layers, beyond traditional web protection.

Across industries, two risks remain dominant:

- Injection (A03) as the primary cross-sector attack vector
- Vulnerable Components (A06) as the largest structural exposure

Attackers are operating with precision below detection thresholds, through targeted sector spikes, and across expanding API surfaces. What this means , Traditional approaches relying on signatures, volume thresholds, or periodic assessments are no longer sufficient.

What must change

- **Continuous application-layer visibility**
- **Behavioral, per-endpoint detection**
- **API-specific security controls**
- **Runtime protection for unpatchable risks**

Final takeaway

Q1 is a baseline. Organisations that adapt to these structural signals will reduce exposure; those that don't will face increasing blind spots.

Limitations

- Findings are based on Prophaze-monitored telemetry and represent directional insights, not industry-wide metrics.
- OWASP categories indicate attack intent, not confirmed breaches.
- Low or 0% values reflect trace-level activity, not absence of threat.

Prophaze™
The New Phase of Security

Fully Managed · 360° Web Application Security · That You Can Afford

AI-powered. Continuously monitored by 24×7 security analysts. Protecting applications from DDoS, malicious bots, API attacks, OWASP Top 10, and zero-day threats.

One Platform | Every Attack Vector | Any Environment.

WAAP Platform

- Unified ML-driven platform: WAF, API, Bot, DDoS, CDN in one
- Consistent protection across all deployment environments
- Rapid onboarding and simplified management at scale
- In-country support with always-on high availability

Adaptive WAF

- Auto-learns application behaviour, no manual rule tuning
- Near-zero false positives with performance-optimised rules
- Advanced response-side security controls
- Virtual patching, protection without code changes

API Security

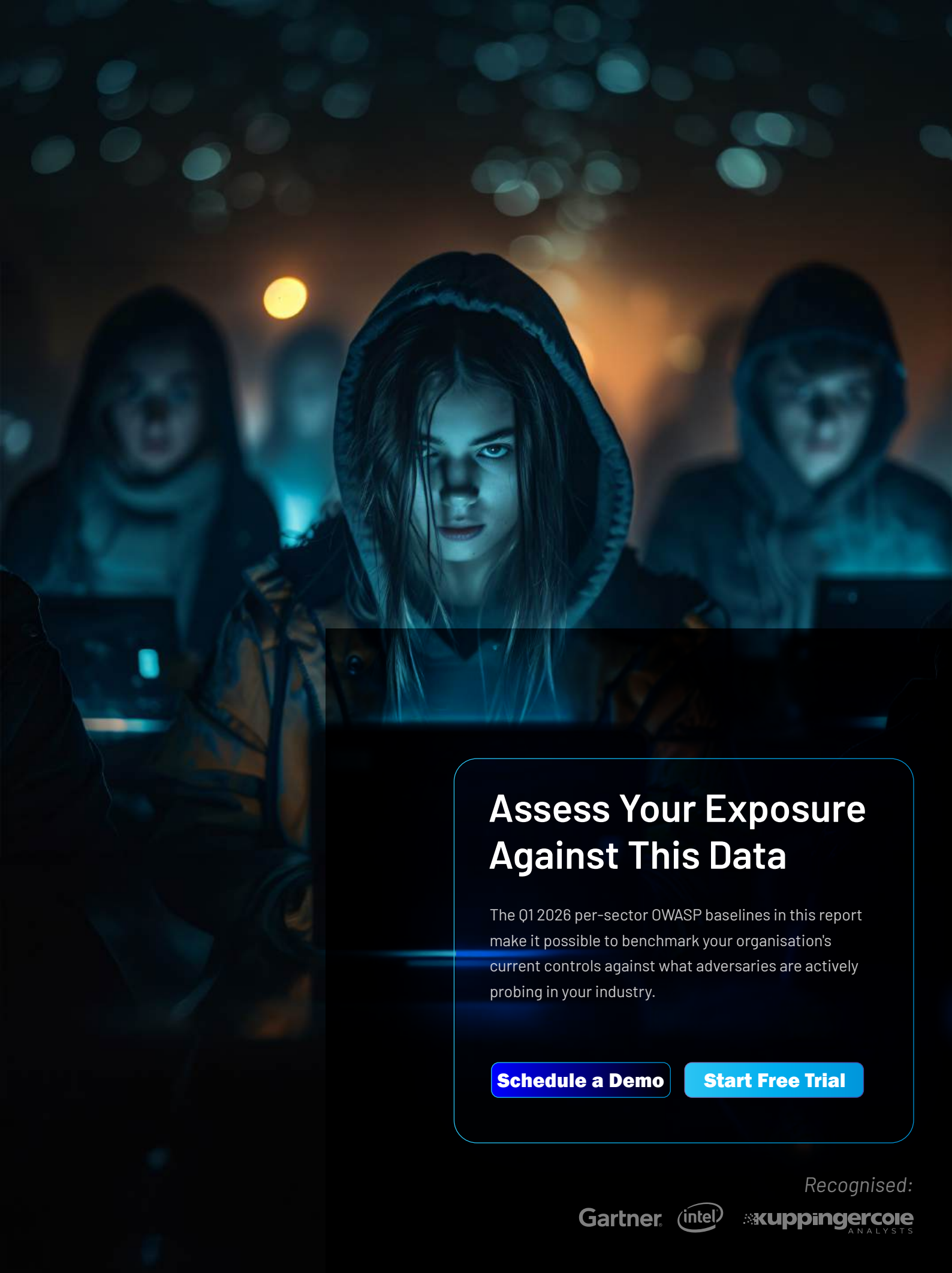
- Continuous API discovery, including shadow and undocumented APIs
- Deep behavioural analysis with real-time risk scoring
- Schema enforcement and zero-day API attack blocking
- Protects business logic and sensitive data at the API layer

Bot Mitigation

- Intent-based classification beyond traditional signature methods
- Advanced behavioural fingerprinting , no CAPTCHAs
- Invisible, low-friction challenges for legitimate users
- Stops credential stuffing, scraping, and account takeover

DDoS Protection

- Intelligent detection distinguishing real users from attack traffic
- Multi-layer behavioural analysis for accurate mitigation
- Ensures uninterrupted application availability
- Context-aware protection across all attack vectors



Assess Your Exposure Against This Data

The Q1 2026 per-sector OWASP baselines in this report make it possible to benchmark your organisation's current controls against what adversaries are actively probing in your industry.

Schedule a Demo **Start Free Trial**

Recognised:

Gartner intel kuppingercole ANALYSTS