Prophaze™
The New Phase of Security

Application Threat

# Analysis Report

Q2 2026

April · May · June

# Table Of Contents



## 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

# Q2 2026 at a Glance

Web applications and APIs now power every critical business function and as organizations become more cloud-native, the application layer continues to attract increasingly sophisticated attacks. Prophaze's State of Application's Threat Landscape Analysis Report provides a quarterly view of how that landscape is evolving, helping security leaders understand where risk is growing and where defenses should adapt.

This second edition analyzes Q2 2026 (April–June) telemetry collected across 11 monitored industries and approximately 581 monitored domains. The report examines attack volume, OWASP attack categories, and industry-specific trends to identify meaningful shifts from the previous quarter.

One of the defining findings confirms a pattern first observed in Q1: Finance & Banking once again experienced a surge in API2:2023 Broken Authentication attacks, indicating that authentication-focused abuse is becoming a recurring campaign rather than an isolated event. At the same time, Vulnerable and Outdated Components (A06:2021) remained the dominant attack category, accounting for nearly half of all observed attacks despite an overall decline in malicious traffic.

Every metric in this report is derived exclusively from Prophaze's Q2 2026 telemetry. External research from organizations such as Mandiant, Cisco Talos, Cloudflare, and NETSCOUT is referenced only to provide broader industry context. Our objective is simple: to help organizations move beyond raw attack counts and better understand the trends shaping application security today.

## Report Facts

- Coverage: Q2 2026 · April–June
- Industries: 11 sectors, unchanged from Q1
- Domains: 581 monitored
- Methodology: unchanged from Q1 , OWASP percentages weighted against deduplicated monthly attack totals per industry

## Next Edition

Q3 2026 Application Threat Landscape · October 2026

## 01 EXECUTIVE SUMMARY

Between April and June 2026, Prophaze watched over roughly 581 domains across 11 industries, covering approximately 2.33 billion requests and blocking 16.4 million attacks. Total attacks fell 18% from Q1's 20 million, even though traffic grew 17% but that headline number hides what actually happened. Seven of eleven industries saw attacks go up this quarter, four of them by more than 140%, and one thing we flagged in Q1 just happened again almost exactly the same way.


### Finance's Authentication Attacks Are Now Recurring

Finance & Banking repeated the same authentication attack pattern seen in Q1. Broken Authentication accounted for 92.4% of June attacks, following 99% in March, confirming a recurring campaign rather than a one-time spike.

### Healthcare Became a Fast-Rising Target

Healthcare & Pharmaceuticals surged from 13,234 attacks in Q1 to 828,054 in Q2 - a 62× increase. Multiple attack categories rose together, pointing to sustained, deliberate targeting rather than isolated activity.

### Unpatched Components Remain the Biggest Risk

Vulnerable and Outdated Components (A06:2021) grew to 48.2% of all attacks, up from 41.8% in Q1. It remained the dominant threat across industries, reaching 85.9% in Real Estate and 77.6% in Energy & Utilities.

### Four Industries Saw Triple-Digit Attack Growth

Manufacturing, Legal & Consulting, Energy & Utilities, and Government all recorded attack growth above 200%. Activity shifted from broad reconnaissance to more targeted attacks, suggesting adversaries refined their focus as the quarter progressed.

### Lower Attack Volume Didn't Mean Lower Risk

Attacks on IT & Software dropped 93.3% quarter-over-quarter, but the decline reflected the end of a large automated scanning campaign. Injection remained the leading threat, showing underlying risk persisted despite lower volumes.

### What security leaders should take away

- Expect Finance's login attacks to return. Continuous monitoring ,not periodic audits , is key to detecting recurring authentication campaigns.
- Treat Healthcare as a Q3 priority. A 62× increase suggests sustained targeting, not a one-off spike.
- Accelerate patching in Energy, Manufacturing, Real Estate & Insurance, and Business, where component risk remains highest or continues to grow.
- Watch for scan-first, strike-later activity. This pattern appeared across five industries and is likely to continue into Q3.

02 | OWASP THREAT LANDSCAPE

# Q2 2026 OWASP Distribution vs. Q1

## Two attack types made up 72% of everything we blocked

We weighted every attack category by how many attacks it actually represented, then added it all up across all 11 industries to see the full Q2 2026 picture. Outdated components (A06) led at 48.2%, up from 41.8% in Q1. Injection (A03) held second at 23.8%, about the same as Q1. Together, these two alone made up 72% of every attack we blocked this quarter.

**48.2%**
Outdated components , across all industries

**23.8%**
Injection , across all industries

**72%**
combined share of these two alone

Q2 2026 OWASP Threat Distribution - All Industries Combined

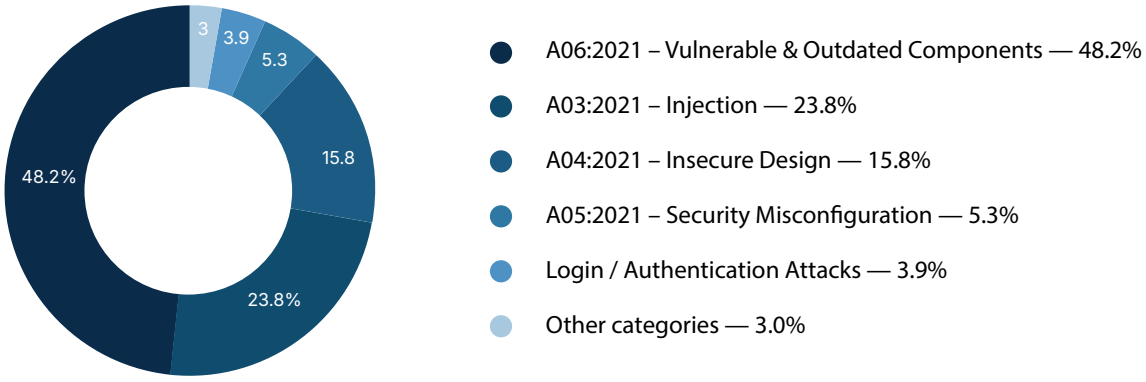



Figure 1. Q2 2026 attack types, weighted by volume across all monitored industries.

## These same two categories have now led two quarters running

Insecure design (15.8%) and misconfiguration (5.3%) round out the next tier, both picking up ground since Q1 as sectors like healthcare, manufacturing, and government saw design-related attacks grow alongside the two leaders. Login attacks made up just 3.9% of attacks across the board, an unremarkable number until you look at Finance & Banking alone, where they spiked to 92.4% of one month's attacks (June) after sitting near zero in April and May. That's the catch with averages: they can completely hide a serious, sector-specific pattern.

### Why does the outdated-components problem keep getting worse?

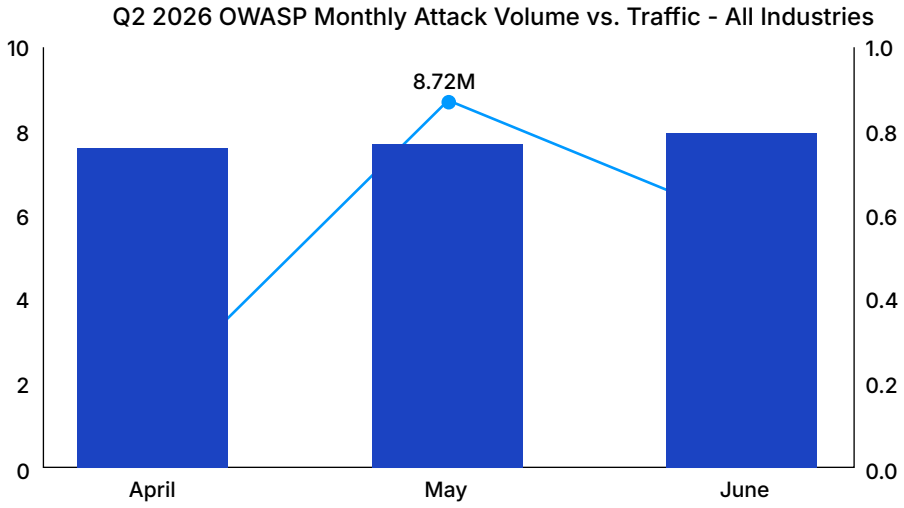
- Legacy platforms and third-party components extend the exposure window, delaying remediation of known vulnerabilities.
- Component exploitation has remained the dominant attack vector for two consecutive quarters, indicating a sustained trend rather than episodic activity.
- Virtual patching provides immediate risk reduction, but durable remediation still depends on patching or replacing vulnerable components.

03 | THREAT ACTIVITY & TRENDS

# Q2 2026 Attack Volume by Industry and Month

### May was the peak of the quarter, and two sectors drove most of it

Attacks didn't rise in a straight line this quarter. April started low, at 1.79 million attacks. May more than quadrupled that, to 8.72 million, the quarter's high point. June eased back to 5.90 million, still well above where April started. Traffic stayed roughly flat the whole time, so May's spike was a real jump in attacks, not just more everyday traffic to sift through.




**What drove it:** mainly Legal & Consulting Services, where May volume ran about 34 times April's before dropping sharply in June, and Finance & Banking, where May carried a wave of component scanning right before June's login-attack spike. Both look like short, focused campaigns rather than a slow climb across the board.

### Four industries drove most of this quarter's attacks

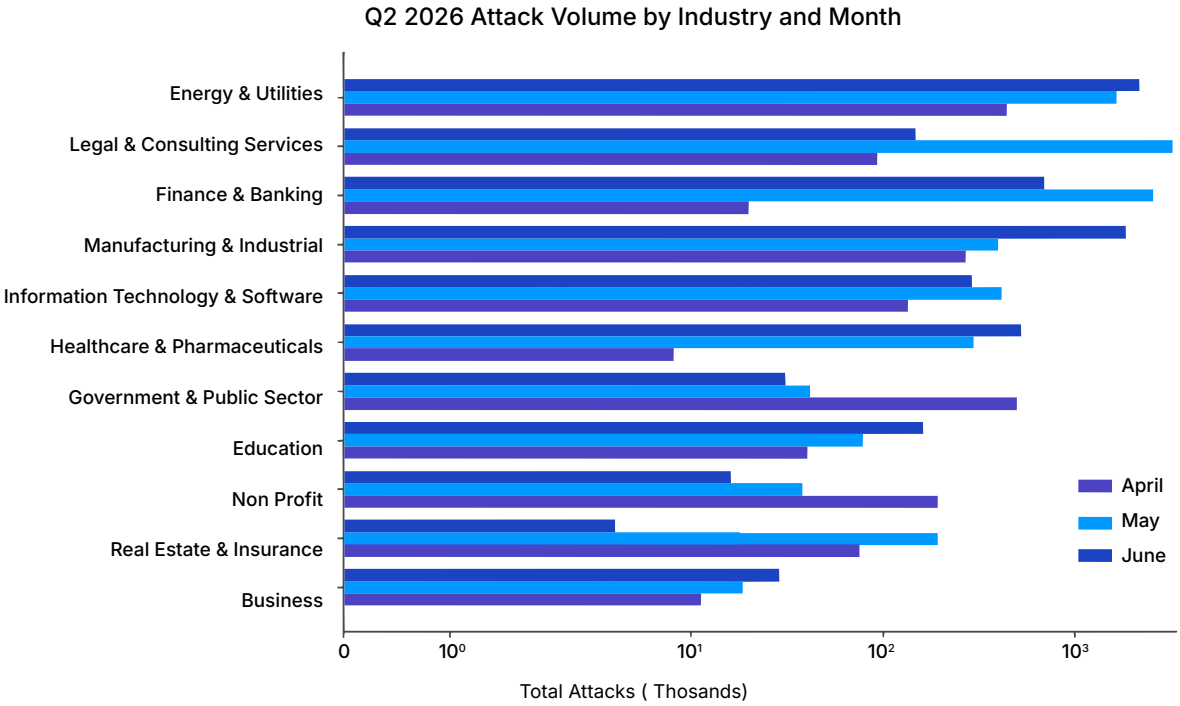



Figure 3. Monthly attack volume by industry (log scale).

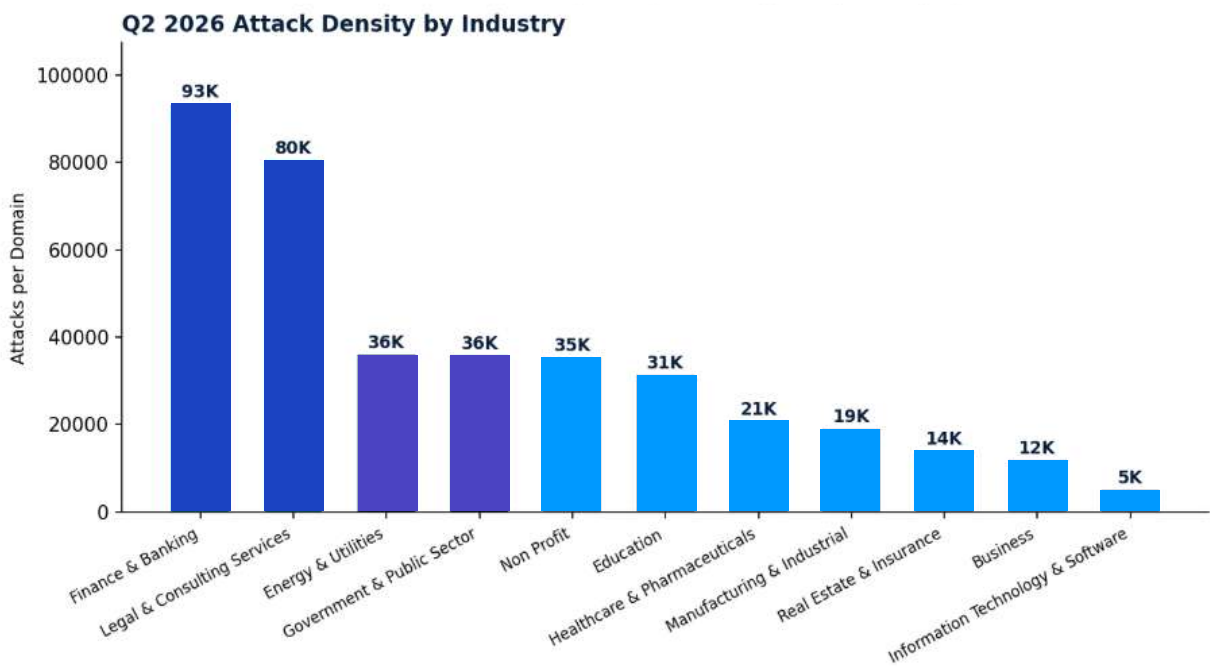
Energy & utilities, legal & consulting services, finance & banking, and manufacturing & industrial together accounted for the large majority of this quarter's attacks, each in the millions, while the other seven sectors combined stayed in the low hundreds of thousands. That doesn't mean those seven are safe, though, Real Estate & Insurance and IT & Software both had two of the quarter's biggest percentage drops, yet still show attack-rate peaks (3.95% and 1.08%) that point to real, concentrated risk hiding under the lower totals.

**93,246**
attacks per domain in Finance, highest of any sector

**4,963**
attacks per domain in IT & Software, lowest of any sector

### Raw totals don't tell the whole story - density does

Looking at attacks per domain instead of raw totals changes the picture. Finance & Banking sits at 93,246 attacks per domain the highest of any sector, and well ahead of Legal & Consulting Services, the next closest at 80,428. That means Finance's applications are hit harder per site than almost anywhere else in the report. IT & Software sits at the opposite end: its 169 monitored domains spread a comparatively modest attack volume very thin, producing the lowest density of any sector.




*Note : Finance (93K attacks/domain across 35 domains) and Legal (80K across 43 domains) show the highest concentration , both driven by their single-month May/June spikes rather than broad, estate-wide probing. For graph visual clarity some of the numbers have been rounded of for example 4.9k to 5k*

### A scan-first, strike-later pattern showed up in five unrelated sectors

The same pattern turned up in Energy, Manufacturing, Healthcare, IT & Software, and Government this quarter, even though nothing connects them: broad injection or design-related probing early on, then a shift to a narrower, more targeted attack on components or logins later, once attackers figured out what actually worked.

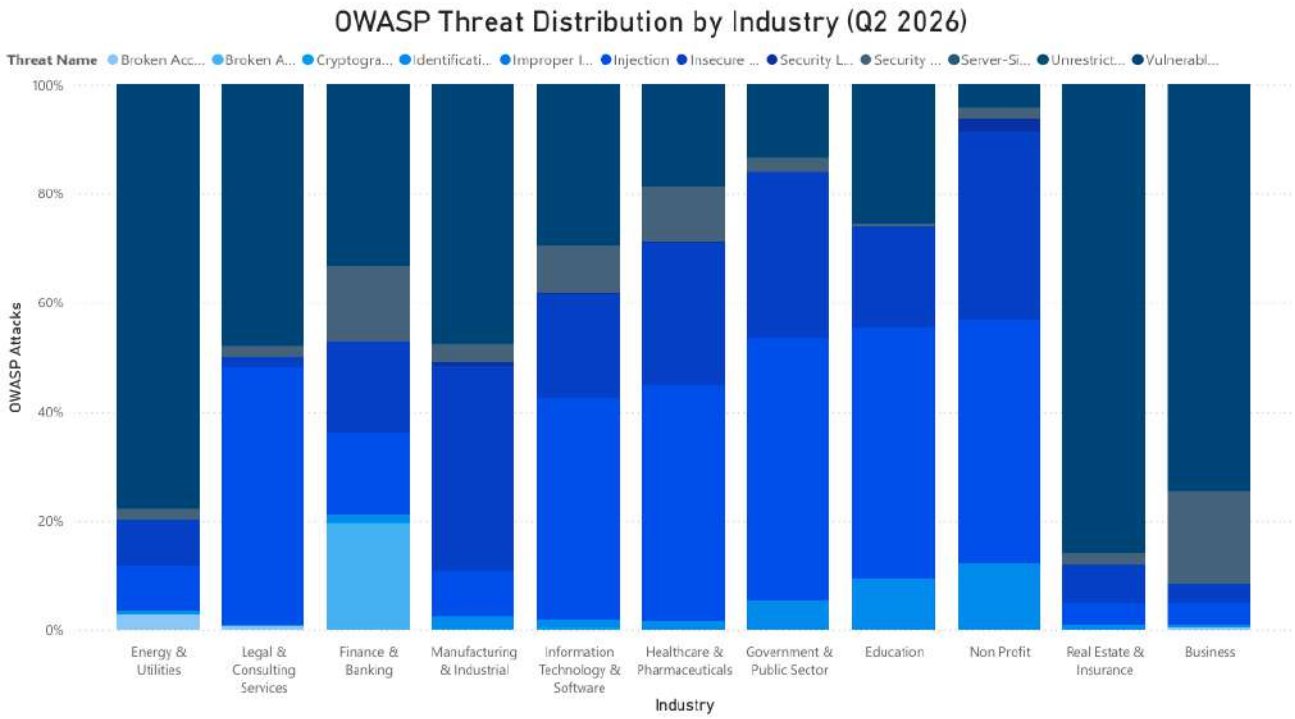
04 | INDUSTRY INTELLIGENCE

# Sector-Wise OWASP Threat Profiles Q2 2026

## Sector-by-Sector Analysis: What Changed and Why

The trends in the previous sections show how the overall threat landscape evolved during Q2. However, estate wide averages only tell part of the story. Every industry experienced a different mix of attacks, risk concentration, and threat progression.

The next 11 sections examine each monitored industry individually. Each profile includes Q2 traffic and attack metrics, the three most prevalent OWASP attack categories, notable attack activity beyond the top three, and the key security takeaway for that sector. Quarter-over-quarter comparisons with Q1 are covered separately in Section 05, allowing each industry profile to focus solely on what happened during Q2.




*Q2 2026 all-industry OWASP distribution, shown here for reference before the sector-by-sector breakdown.*

## Q2 2026 All-Industry OWASP Distribution

The above below provides a high-level view of attack distribution across all monitored industries before moving into the individual sector analyses. While component exploitation remained the dominant trend overall, the distribution varied significantly by industry. Some sectors faced highly concentrated attack patterns dominated by a single vulnerability class, while others experienced a more balanced mix of threats requiring layered defensive strategies. The following pages explore those differences in detail.

## Finance & Banking

Finance & Banking covers core banking APIs, payment gateways, loan and account systems, and the logins that protect all of it. That combination of money and identity data makes this sector a constant target, not just for opportunistic scanners, but for tools built specifically to go after banks.

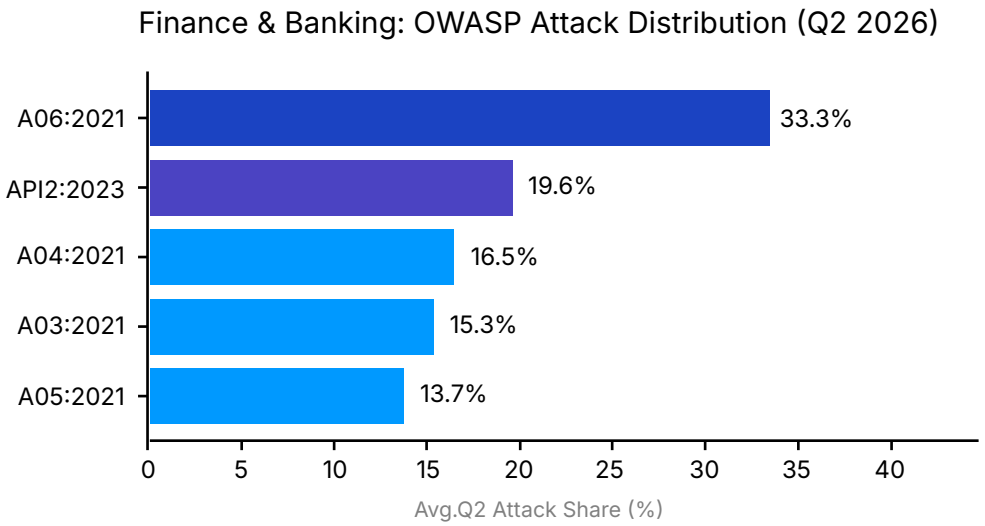
### Q2 2026 Industry Snapshot

| 253,622,019 | 3,263,603 | 1.29% | 3.02% |
|---|---|---|---|
| Total Requests (Q2) | Total Attacks (Q2) | Avg. Attack Rate | Peak Monthly Rate |

*Monthly attack rate , April: 0.03% • May: 3.02% • June: 0.76% Monitored footprint: across 35 domains (93,246 attacks per domain this quarter).*

Finance gave us the clearest story of the quarter. Attacks were up 144.2% over Q1, but the size of the increase matters less than its shape: April was quiet, May brought a wave of scanning, and June repeated almost exactly what happened in Q1's March, a sharp spike in login attacks. A sector that goes quiet for two months and then spikes hard in one is being tested on a schedule, not probed at random.

| OWASP Category | Threat | Avg. Q2 Share | Peak % |
|---|---|---|---|
| A06:2021 | Vulnerable and Outdated Components | 33.30% | 41.66% May |
| API2:2023 | Broken Authentication | 19.61% | 92.41% June |
| A04:2021 | Insecure Design | 16.47% | 34.82% April |



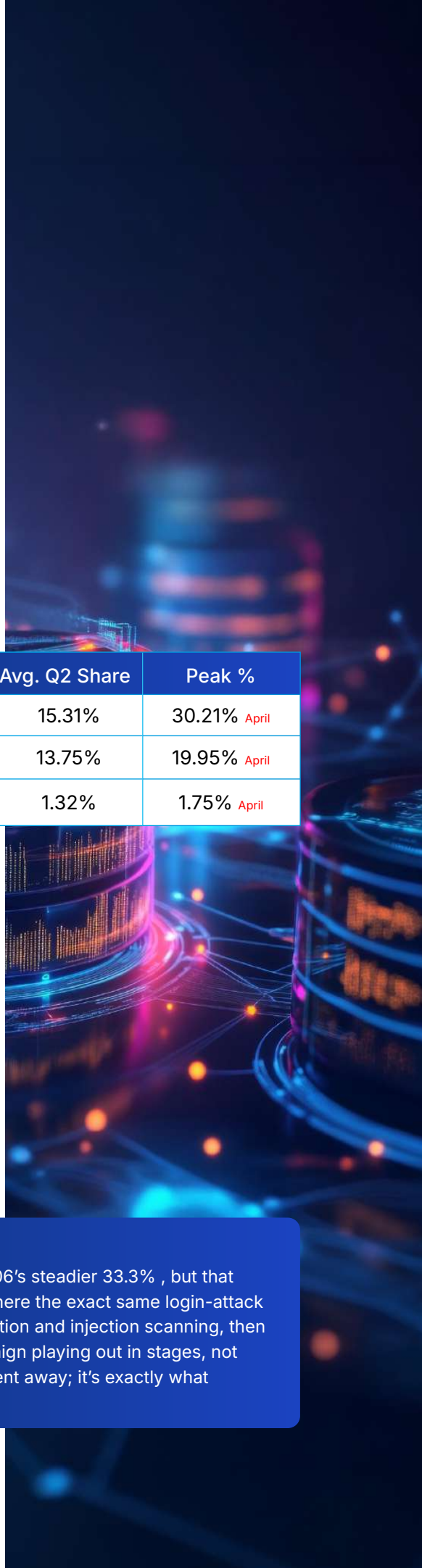
Although A06:2021 (Vulnerable and Outdated Components) remained Finance's largest threat, the defining Q2 trend was API2:2023 Broken Authentication, which surged to 92.4% of June attacks after minimal activity in April and May,mirroring Q1's 99% spike in March.

This recurring pattern suggests attackers first exploited outdated banking components before shifting to credential, token, and session attacks. Meanwhile, Insecure Design peaked at 34.8% in April, highlighting persistent authorization weaknesses that patching alone cannot resolve.

## Other Notable Attack Activity

| OWASP Category | Threat | Avg. Q2 Share | Peak % |
|---|---|---|---|
| A03:2021 | Injection | 15.31% | 30.21% April |
| A05:2021 | Security Misconfiguration | 13.75% | 19.95% April |
| A07:2021 | Identification and Authentication Failures | 1.32% | 1.75% April |

Injection and misconfiguration attacks both peaked in April, before the bigger May/June wave, consistent with attackers casting a wide net early (probing loan and account pages, checking for exposed admin panels) before narrowing in on specific components and logins later in the quarter. A low, steady stream of credential-stuffing attempts ran in the background the whole time, regardless of what else was happening that month.



**Threat Analysis**

API2:2023's quarterly average (19.6%) looks unremarkable next to A06's steadier 33.3% , but that average is hiding the real story. This is the second quarter running where the exact same login-attack pattern has shown up, and the April-to-June sequence (misconfiguration and injection scanning, then component fingerprinting, then the login attack) looks like one campaign playing out in stages, not three separate events. A quiet two months isn't a sign the problem went away; it's exactly what happened right before it came back.

## Energy & Utilities

Energy & Utilities runs customer billing portals right alongside operational systems that can take years to patch or replace. That gap , modern web applications sitting in front of infrastructure stuck on a much slower upgrade cycle, is what defines this sector's risk more than any single attack type.

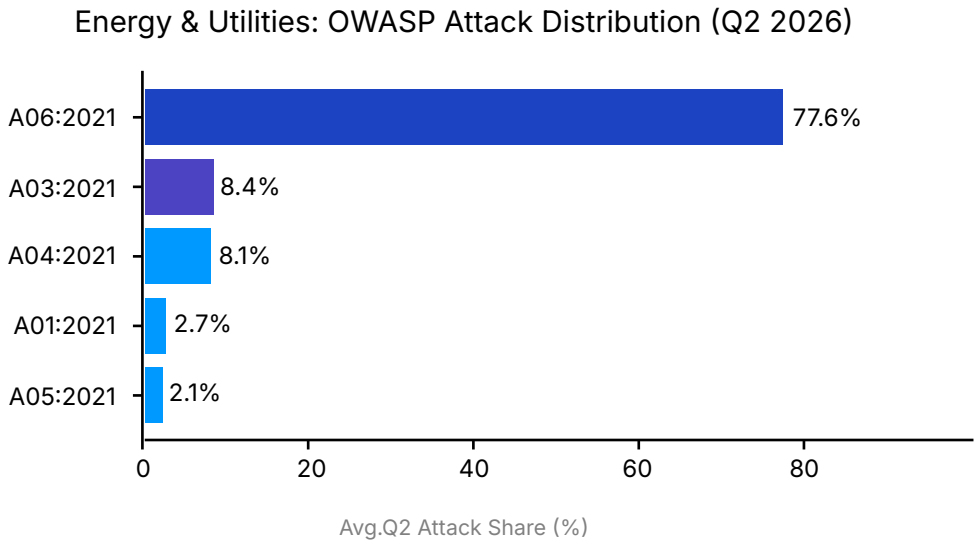
### Q2 2026 Industry Snapshot

| 476,287,538 | 4,247,684 | 0.89% | 1.40% |
|---|---|---|---|
| Total Requests (Q2) | Total Attacks (Q2) | Avg. Attack Rate | Peak Monthly Rate |

*Monthly attack rate , April: 0.23% • May: 1.40% • June: 1.29% Monitored footprint: across 118 domains (35,997 attacks per domain this quarter).*

Energy had the largest attack volume of any sector this quarter and the second-biggest jump over Q1, more than quadrupling in size. Unlike Finance's spike and retreat pattern, Energy just kept climbing: the attack rate went from 0.23% in April to 1.40% in May and stayed roughly there through June, while its leading attack type got more dominant every single month instead of leveling off.

| OWASP Category | Threat | Avg. Q2 Share | Peak% |
|---|---|---|---|
| A06:2021 | Vulnerable and Outdated Components | 77.55% | 85.51% June |
| A03:2021 | Injection | 8.41% | 21.46% April |
| A04:2021 | Insecure Design | 8.14% | 32.94% April |



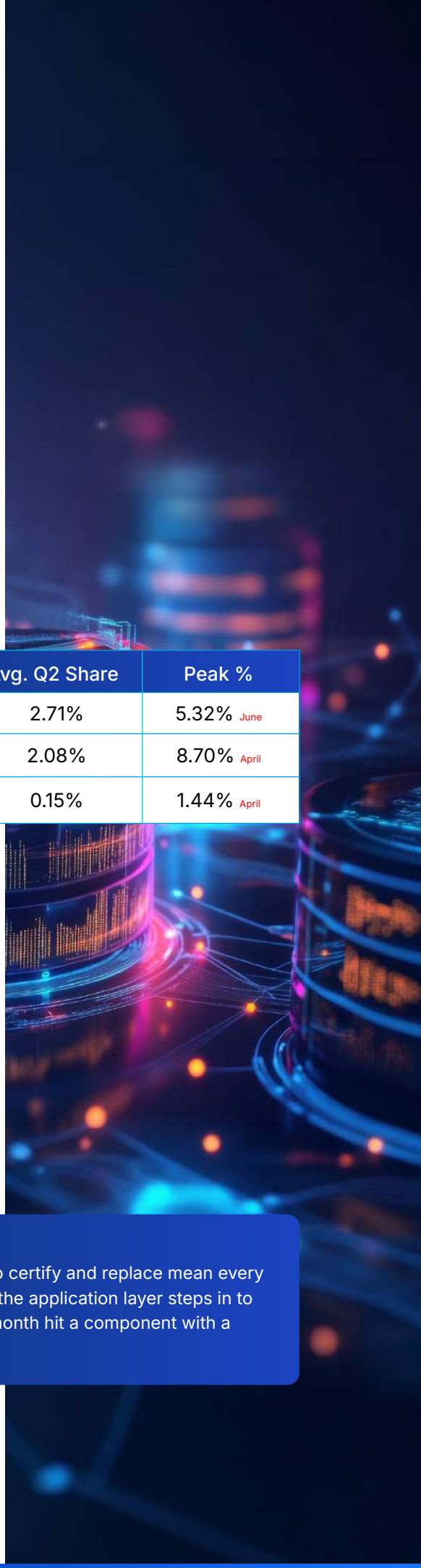
Outdated Components became Energy's defining threat, rising from an already-high 57.7% average in Q1 to 85.5% in June. The steady increase points to aging vendor systems, inconsistent patching across distributed environments, and operational software that cannot be upgraded quickly, leaving known vulnerabilities exposed for longer.

Injection and Insecure Design peaked together in April before A06 took over, suggesting attackers first mapped weaknesses across billing portals and customer-facing systems, then shifted to exploiting specific vulnerable components as the quarter progressed.

## Other Notable Attack Activity

| OWASP Category | Threat | Avg. Q2 Share | Peak % |
|---|---|---|---|
| A01:2021 | Broken Access Control | 2.71% | 5.32% June |
| A05:2021 | Security Misconfiguration | 2.08% | 8.70% April |
| API2:2023 | Broken Authentication | 0.15% | 1.44% April |

Broken access control only showed up in June, nothing in April or May, which makes it worth watching heading into Q3 rather than dismissing it as background noise. A small login-attack signal also showed up in April, echoing the much bigger pattern seen in Finance; in an estate this size, even a small reading on login attacks deserves the same attention as the bigger component problem.



**Threat Analysis**

Energy's risk comes from its infrastructure: systems that take years to certify and replace mean every known vulnerability in this estate stays exploitable until something at the application layer steps in to cover it. A June reading above 85% means nearly every attack that month hit a component with a known fix the operational systems simply couldn't apply yet.

# Legal & Consulting Services

Legal & Consulting Services runs on document management systems, case search tools, and portals built separately for each client , systems that handle sensitive case files but often go years between vendor updates, with access rules that get more inconsistent the more they're customized.

## Q2 2026 Industry Snapshot

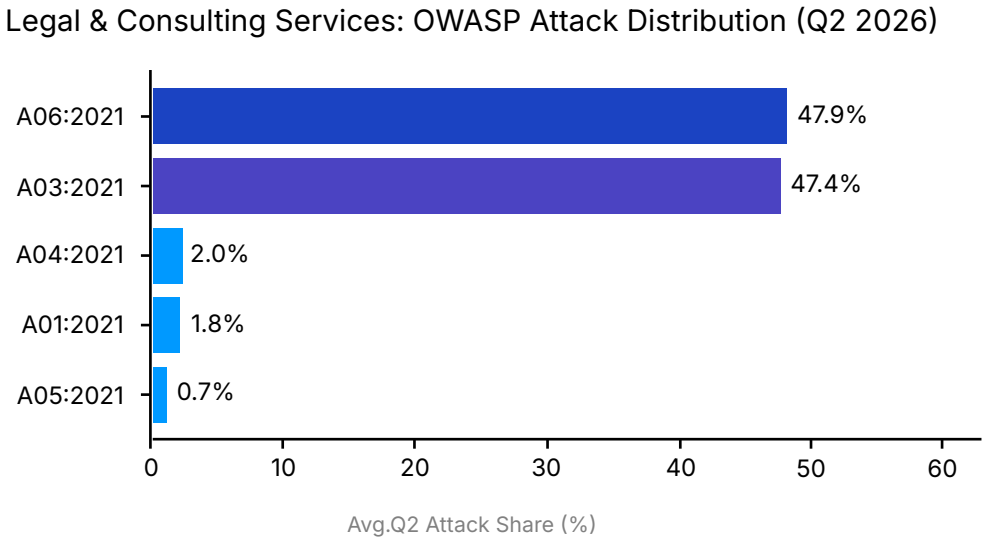
| 712,276,385 | 3,458,401 | 0.49% | 1.25% |
|---|---|---|---|
| Total Requests (Q2) | Total Attacks (Q2) | Avg. Attack Rate | Peak Monthly Rate |

*Monthly attack rate , April: 0.05% • May: 1.25% • June: 0.06% Monitored footprint: across 43 domains (80,428 attacks per domain this quarter).*

Legal had the second-highest attack density of any sector and a 341.8% jump over Q1, almost all of it from one month. May saw roughly 34 times April's attack volume, then June dropped back down sharply. That kind of spike-then-drop points to a focused, time-limited campaign rather than steady pressure across the whole quarter.

## Top 3 Attack Categories

| OWASP Category | Threat | Avg. Q2 Share | Peak% |
|---|---|---|---|
| A06:2021 | Vulnerable and Outdated Components | 47.92% | 49.48% April |
| A03:2021 | Injection | 47.39% | 49.38% April |
| A04:2021 | Insecure Design | 1.99% | 21.85% June |



Outdated Components and Injection remained almost evenly matched throughout April and May, each accounting for roughly 47–49% of attacks, including May's major spike. This suggests attackers simultaneously targeted vulnerable components and injection flaws, requiring both patch management and injection protection to mitigate the surge.

After May, the pattern shifted as Insecure Design rose to 21.9% of June attacks, pointing to persistent authorization and permission weaknesses that remained even after the main attack wave subsided.

## Other Notable Attack Activity

| OWASP Category | Threat | Avg. Q2 Share | Peak % |
|---|---|---|---|
| A05:2021 | Security Misconfiguration | 1.84% | 24.95% June |
| A01:2021 | Broken Access Control | 0.72% | 9.34% June |
| A07:2021 | Identification and Authentication Failures | 0.09% | 0.20% April |

Misconfiguration and access-control issues both jumped sharply in June, right alongside the rise in design-related attacks, the same month attackers seem to have shifted from high-volume scanning toward more precise, targeted probing. Together, these three June changes look like a second, quieter phase of the same campaign rather than something new and unrelated.

**Threat Analysis**

May's spike looks like a finished attack, not an ongoing one, volume dropped more than 95% by June, suggesting attackers moved on. But whatever component, injection, and access-control weaknesses they found during that spike are still there until fixed, whether or not attack volume has come back down.

## Manufacturing & Industrial

Manufacturing & Industrial runs supply-chain portals and vendor integrations that typically sit on multi-year hardware and software cycles, which means the tools in place often fall behind the pace of newly discovered vulnerabilities.

### Q2 2026 Industry Snapshot

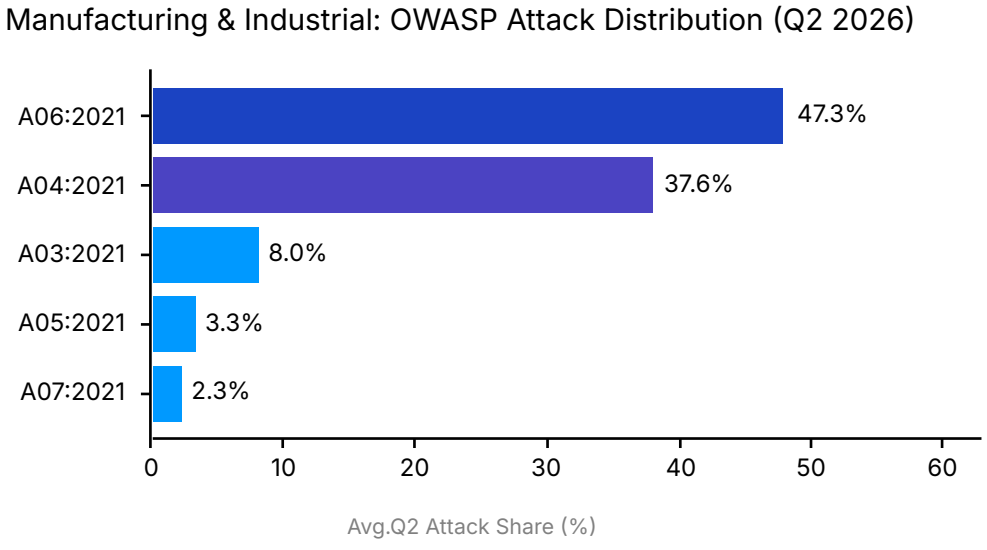
| 434,702,253 | 2,513,747 | 0.58% | 1.24% |
|---|---|---|---|
| Total Requests (Q2) | Total Attacks (Q2) | Avg. Attack Rate | Peak Monthly Rate |

*Monthly attack rate ,April: 0.19% • May: 0.28% • June: 1.24% Monitored footprint: 132 domains (19,044 attacks per domain this quarter).*

Manufacturing had the sharpest single-month jump in the whole report: attacks grew only modestly from April to May, then jumped about 365% from May to June. Combined with a 648.9% increase over Q1 overall, this is one of the clearest examples this quarter of a sector's risk changing shape mid-quarter rather than trending smoothly.

### Top 3 Attack Categories

| OWASP Category | Threat | Avg. Q2 Share | Peak% |
|---|---|---|---|
| A06:2021 | Vulnerable and Outdated Components | 47.33% | 49.55% June |
| A04:2021 | Insecure Design | 37.60% | 43.89% June |
| A03:2021 | Injection | 8.03% | 24.37% May |



Outdated Components and Insecure Design tracked closely throughout the quarter, both peaking in June as attacks surged 365%, suggesting attackers exploited both weaknesses within the same supply-chain systems rather than through separate campaigns.

Injection peaked earlier in May (24.4%), indicating an initial probing phase before attackers shifted to broader exploitation in June, a compressed version of the probe-then-strike pattern also observed in Legal & Consulting.

## Other Notable Attack Activity

| OWASP Category | Threat | Avg. Q2 Share | Peak % |
|---|---|---|---|
| A05:2021 | Security Misconfiguration | 3.35% | 8.26% April |
| A09:2021 | Security Logging and Monitoring Failures | 0.68% | 3.92% April |
| A07:2021 | Identification and Authentication Failures | 2.30% | 7.31% May |

Logging gaps showed up too, and while the share is small, it matters here: it means part of this estate had real blind spots right when the bigger attacks were ramping up, so some of June's activity may never have tripped an alert in April or May. A tiny signal for undocumented APIs also appeared in May, worth tracking as this sector's API footprint keeps growing.

**Threat Analysis**

Components and design weaknesses running neck-and-neck, both peaking in the same month attacks spiked, tells us this isn't one simple gap to close, it's two separate weaknesses being hit at the same points at once. That's exactly the kind of risk that needs constant monitoring to catch before it accelerates again.

## Healthcare & Pharmaceuticals

Healthcare & Pharmaceuticals covers patient portals, e-prescription tools, and clinical data systems , areas where privacy regulations and old, hard-to-replace systems usually slow down how fast problems get fixed.

### Q2 2026 Industry Snapshot

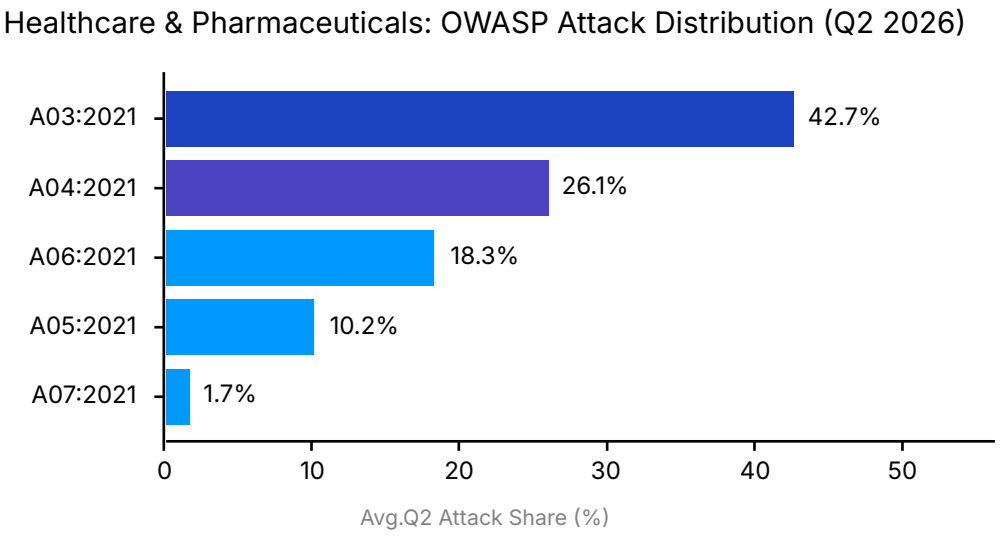
| 51,519,064 | 828,054 | 1.61% | 2.09% |
|---|---|---|---|
| Total Requests (Q2) | Total Attacks (Q2) | Avg. Attack Rate | Peak Monthly Rate |

*Monthly attack rate , April: 0.07% • May: 1.89% • June: 2.09% Monitored footprint: 40 domains (20,701 attacks per domain this quarter).*

Healthcare is the biggest surprise in this report: a sector that saw only 13,234 attacks in all of Q1 saw 828,054 in Q2 , a 62-fold jump. That's not a small shift in an already-watched risk; it's a sector going from barely on the radar to a real target within one quarter. And it kept climbing every month, from a 0.98% attack rate in April to 2.09% by June.

### Top 3 Attack Categories

| OWASP Category | Threat | Avg. Q2 Share | Peak% |
|---|---|---|---|
| A03:2021 | Injection | 42.70% | 47.60% May |
| A04:2021 | Insecure Design | 26.11% | 26.57% June |
| A06:2021 | Vulnerable and Outdated Components | 18.34% | 39.53% April |



Healthcare's attack profile shifted significantly from Q1, moving from outdated components to sustained Injection attacks, which remained above 40% throughout Q2 and peaked near 48% in May. This consistent pressure suggests deliberate targeting of patient-facing applications rather than opportunistic scanning.

Outdated Components peaked early in April (39.5%) before declining, indicating an initial reconnaissance phase that gave way to broader exploitation of Injection and Insecure Design weaknesses for the rest of the quarter.

## Other Notable Attack Activity

| OWASP Category | Threat | Avg. Q2 Share | Peak % |
|---|---|---|---|
| A05:2021 | Security Misconfiguration | 10.21% | 14.18% June |
| A07:2021 | Identification and Authentication Failures | 1.68% | 2.22% June |
| A09:2021 | Security Logging and Monitoring Failures | 0.02% | 0.06% May |

Misconfiguration attacks grew every single month and hit their highest point in June, right alongside design attacks , which tells us attackers are finding exposed settings as they explore this newer target, not just its injection and design weaknesses. A small, steady stream of login attacks ran throughout, suggesting basic account-takeover attempts happening quietly in the background the whole time.

**Threat Analysis**

A 62-times jump in attacks isn't something you can write off as a fluke , it's the strongest sign in this report that Healthcare has landed on attackers' target lists for real. And because injection, design weaknesses, and misconfiguration all grew together across the quarter, instead of one thing spiking and fading, this looks like broad exploration of the whole sector rather than a single one-off attack.

## Public Sector

Public Sector runs citizen service portals, permitting systems, and public records , systems that need to stay open to the public by design, which limits how tightly access can be locked down even as attacks grow.

### Q2 2026 Industry Snapshot

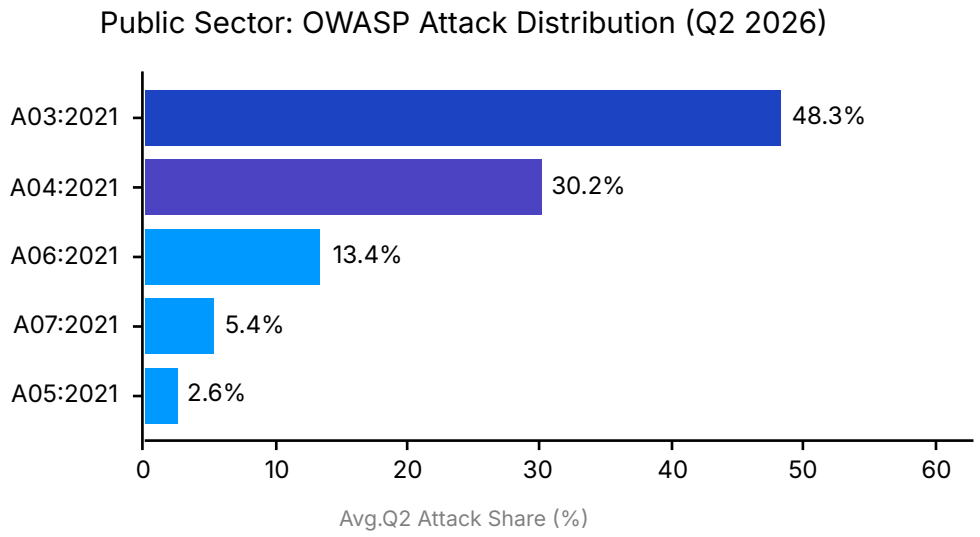
| 70,754,137 | 572,675 | 0.81% | 2.15% |
|---|---|---|---|
| Total Requests (Q2) | Total Attacks (Q2) | Avg. Attack Rate | Peak Monthly Rate |

*Monthly attack rate , April: 2.15% • May: 0.18% • June: 0.13% Monitored footprint: across 16 domains (35,792 attacks per domain this quarter).*

Government attacks more than tripled over Q1 (+204.7%), with the sharpest activity in April rather than building toward the end of the quarter , the opposite order from most other sectors this quarter. April's attack rate of 2.15% was the highest single month anywhere in Government's Q2 data, before things eased through May and June.

### Top 3 Attack Categories

| OWASP Category | Threat | Avg. Q2 Share | Peak% |
|---|---|---|---|
| A03:2021 | Injection | 48.33% | 51.11% April |
| A04:2021 | Insecure Design | 30.19% | 33.46% April |
| A06:2021 | Vulnerable and Outdated Components | 13.41% | 67.06% June |



Injection and Insecure Design peaked together in April, driving the quarter's highest attack volume and indicating broad automated scanning of public-facing government portals and records systems.

By June, Outdated Components rose to 67.1% even as overall attacks declined, suggesting a shift from widespread reconnaissance to more targeted exploitation of known vulnerable systems.

## Other Notable Attack Activity

| OWASP Category | Threat | Avg. Q2 Share | Peak % |
|---|---|---|---|
| A07:2021 | Identification and Authentication Failures | 5.38% | 6.01% April |
| A05:2021 | Security Misconfiguration | 2.62% | 2.94% May |
| A10:2021 | Server-Side Request Forgery | 0.03% | 0.40% May |

Login attacks held a steady, moderate share all quarter , attempting logins against citizen and staff portals that kept going regardless of whatever else was leading that month. A small SSRF finding in May, while tiny, fits with attackers testing how records systems talk to other government systems behind the scenes.

**Threat Analysis**

The government went from broad scanning in April to focused, targeted attacks in June , which suggests attackers spent the early weeks mapping the public-facing surface before narrowing in on the specific old components worth exploiting. That means April-style broad scanning shouldn't be dismissed once volume drops; it's often what comes right before the more targeted attack.

## Information Technology & Software

IT & Software covers SaaS platforms, developer-facing APIs, and shared infrastructure where one successful attack can potentially spread across many customers at once; that's the defining risk here, regardless of how the quarter's totals moved.

### Q2 2026 Industry Snapshot

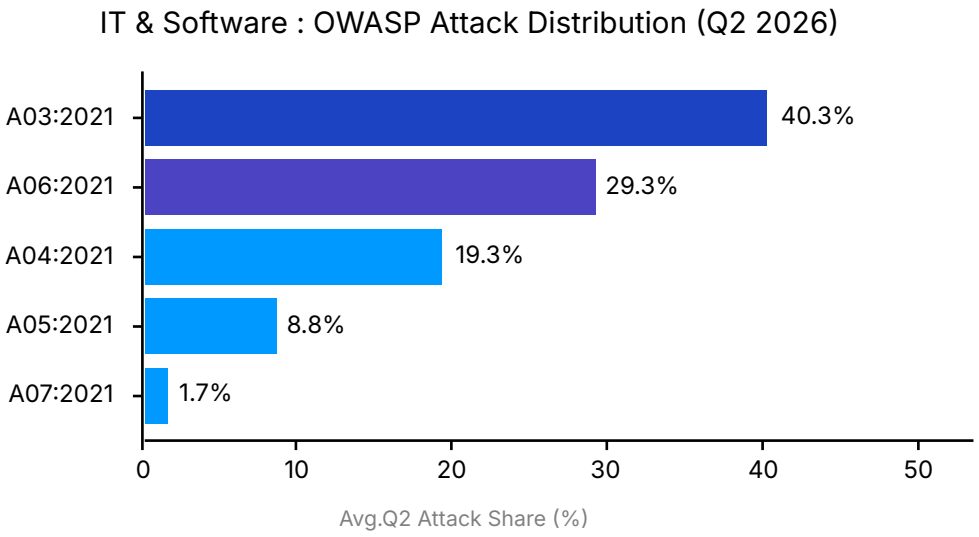
| 137,870,008 | 838,669 | 0.61% | 1.08% |
|---|---|---|---|
| Total Requests (Q2) | Total Attacks (Q2) | Avg. Attack Rate | Peak Monthly Rate |

*Monthly attack rate , April: 0.28% • May: 0.67% • June: 1.08% Monitored footprint: across 169 domains (4,963 attacks per domain this quarter).*

IT & Software saw the biggest volume drop of any sector: attacks fell 93.3% from Q1's 12.6 million to Q2's 838,669. That's not a sign this sector got safer , Q1's huge number came from a short burst of automated scanning, and Q2's lower, steadier numbers likely reflect that burst ending and normal, targeted probing continuing underneath it. The attack rate still climbed all quarter, from 0.27% in April to 1.08% in June.

### Top 3 Attack Categories

| OWASP Category | Threat | Avg. Q2 Share | Peak% |
|---|---|---|---|
| A03:2021 | Injection | 40.34% | 52.35% May |
| A06:2021 | Vulnerable and Outdated Components | 29.28% | 46.61% June |
| A04:2021 | Insecure Design | 19.33% | 22.20% April |



Injection remained the dominant threat throughout Q2, peaking at 52.4% in May and reflecting sustained probing of developer-facing APIs and search interfaces.

By June, Outdated Components rose to 46.6%, following the same probe-then-strike pattern seen in Healthcare and Manufacturing, as attackers shifted from broad testing to exploiting confirmed vulnerable components,an especially high risk in shared SaaS environments where a single flaw can impact multiple customers.

## Other Notable Attack Activity

| OWASP Category | Threat | Avg. Q2 Share | Peak % |
|---|---|---|---|
| A05:2021 | Security Misconfiguration | 8.78% | 12.39% April |
| A07:2021 | Identification and Authentication Failures | 1.73% | 2.12% May |
| A02:2021 | Cryptographic Failures | 0.26% | 0.61% April |

Misconfiguration hit its highest point in April, the same window design weaknesses peaked , consistent with early-quarter probing of exposed developer and admin tools. A small number of cryptographic-failure findings, while low in share, matter here: token and key-handling mistakes can affect every customer relying on that API.

**Threat Analysis**

Don’t read the 93.3% drop as good news , it reflects Q1’s scanning burst ending, not attackers losing interest. Injection stayed above 40% all quarter and outdated components climbed sharply into June, so IT & Software’s real exposure , made worse by how far one bad exploit can spread , is still one of the more serious risks in this report.

## Real Estate & Insurance

Real Estate & Insurance runs property listing sites, claims processing, and policy management , often built on third-party data feeds and older underwriting systems that don't get replaced often.

### Q2 2026 Industry Snapshot

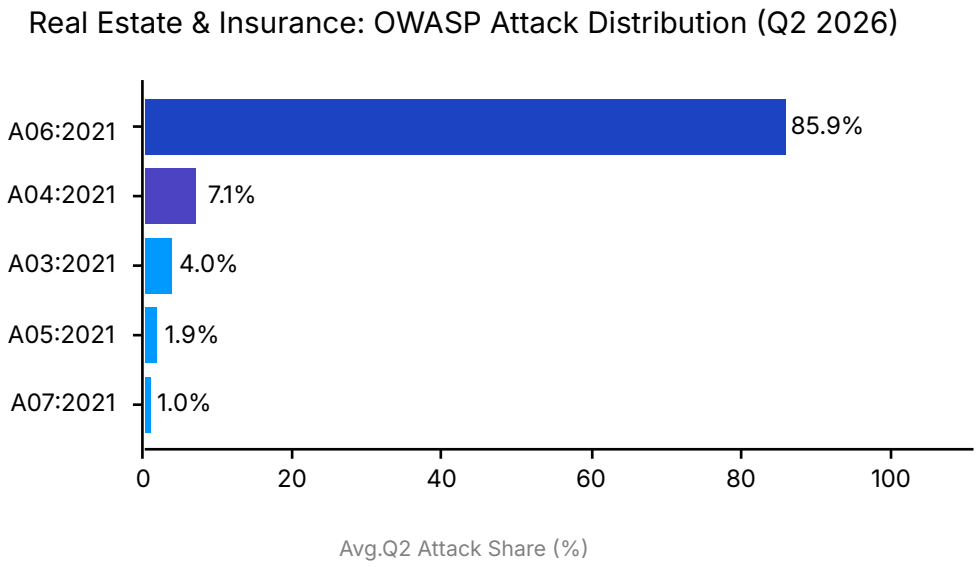
| 6,124,351 | 97,110 | 1.59% | 3.95% |
|---|---|---|---|
| Total Requests (Q2) | Total Attacks (Q2) | Avg. Attack Rate | Peak Monthly Rate |

*Monthly attack rate , April: 3.95% • May: 0.74% • June: 0.23% Monitored footprint: across 7 domains (13,873 attacks per domain this quarter).*

Real Estate & Insurance had the second-sharpest drop of any sector, falling 68.6% from Q1. Still, April had the highest attack rate anywhere in this whole report, at 3.95%, before easing off through May and June,a small but heavily targeted group of sites.

### Top 3 Attack Categories

| OWASP Category | Threat | Avg. Q2 Share | Peak% |
|---|---|---|---|
| A06:2021 | Vulnerable and Outdated Components | 85.85% | 88.37% May |
| A04:2021 | Insecure Design | 7.13% | 35.98% June |
| A03:2021 | Injection | 4.02% | 5.86% June |



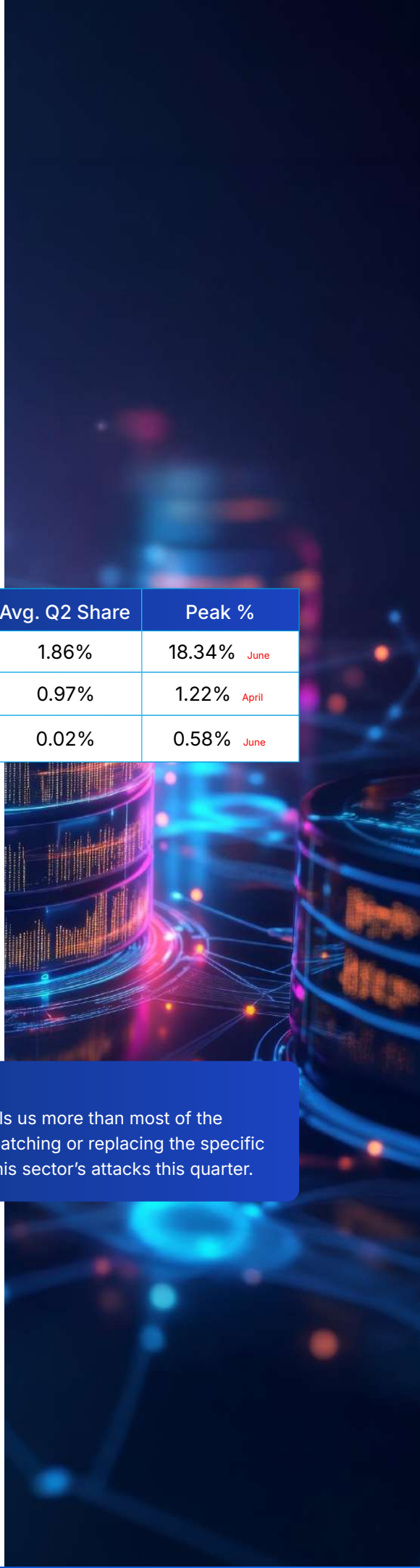
Outdated Components dominated throughout Q2, accounting for 85–88% of attacks each month ,the most concentrated attack pattern in this report. This suggests attackers repeatedly targeted the same vulnerable claims platforms, plugins, and integration libraries rather than diversifying their efforts.

Insecure Design rose to 36.0% in June, indicating growing interest in underwriting and claims-workflow weaknesses after the primary component vulnerabilities had been extensively exploited.

## Other Notable Attack Activity

| OWASP Category | Threat | Avg. Q2 Share | Peak % |
|---|---|---|---|
| A05:2021 | Security Misconfiguration | 1.86% | 18.34% June |
| A07:2021 | Identification and Authentication Failures | 0.97% | 1.22% April |
| A01:2021 | Broken Access Control | 0.02% | 0.58% June |

Misconfiguration jumped to an 18.3% share in June, right alongside design weaknesses' own rise , both pointing to a brief moment of variety away from this sector's usual, overwhelming focus on outdated components. Worth watching in Q3 to see if it sticks or goes back to the near-total dominance we saw in April and May.



**Threat Analysis**

An 85%+ average stuck in one category, all three months running, tells us more than most of the quarter-over-quarter swings in this report: it means one type of fix , patching or replacing the specific outdated components involved , would clear up the vast majority of this sector's attacks this quarter.


# Education

Education covers student information systems, learning platforms (lms systems) , and admissions tools , examination platforms and proctoring systems. These are  places that naturally see uneven traffic tied to the school calendar, which is different from traffic driven by attackers.

## Q2 2026 Industry Snapshot

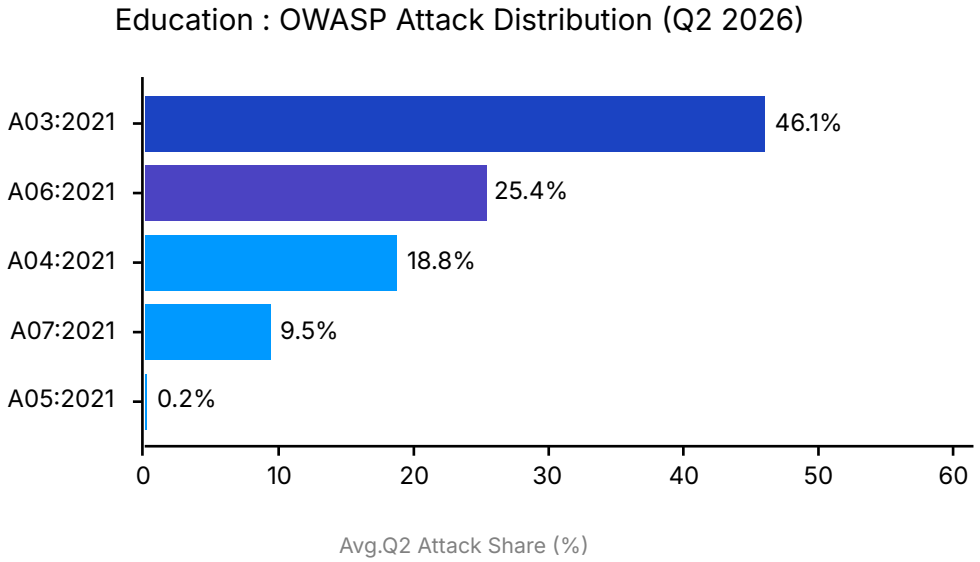
| 81,997,129 | 281,218 | 0.34% | 0.61% |
|---|---|---|---|
| Total Requests (Q2) | Total Attacks (Q2) | Avg. Attack Rate | Peak Monthly Rate |

*Monthly attack rate , April: 0.15%  •  May: 0.27%  •  June: 0.61% Monitored footprint: across 9 domains (31,246 attacks per domain this quarter).*

Education saw a steady, unremarkable 32.8% increase over Q1 , ordinary growth, not a sudden shift. The attack rate climbed steadily each month, from 0.19% in April to 0.62% in June, and the leading attack type stayed the same the whole quarter.

## Top 3 Attack Categories

| OWASP Category | Threat | Avg. Q2 Share | Peak% |
|---|---|---|---|
| A03:2021 | Injection | 46.07% | 48.54% June |
| A06:2021 | Vulnerable and Outdated Components | 25.40% | 32.11% June |
| A04:2021 | Insecure Design | 18.77% | 26.08% April |



Injection has remained the dominant attack throughout Q2, indicating sustained probing of student portals and admissions systems rather than an escalating campaign.

Outdated Components rose to 32.1% in June alongside Injection,reflecting a modest expansion in attack techniques rather than the clear probe-then-strike pattern seen in sectors like Healthcare and Manufacturing.

## Other Notable Attack Activity

| OWASP Category | Threat | Avg. Q2 Share | Peak % |
|---|---|---|---|
| A07:2021 | Identification and Authentication Failures | 9.48% | 17.56% April |
| A05:2021 | Security Misconfiguration | 0.23% | 0.35% May |
| A10:2021 | Server-Side Request Forgery | 0.04% | 0.15% May |

Login attacks hit a 17.6% peak in April , the standout education finding this quarter. That's a concentrated wave of attempted logins against student and staff accounts early in the term, which fits bot-driven account-takeover tools that seem to treat the school calendar as a cue to strike.

**Threat Analysis**

Education's story this quarter is the calmest in the report: one attack type led the whole way through, growth was gradual instead of driven by a single event, and the one real spike , April's login attacks , is a well-understood bot problem, not a deeper structural issue.

*Two additional single-occurrence findings appeared in the raw April domain-level logs but fell below this report's per-domain Top-5 reporting threshold, so they are excluded from the aggregated figures above: a single CVE-2021-44228 (Log4Shell) probe on one monitored domain (0.16% of that domain's April activity) and a single generic crawler detection on another domain (0.10%). Both are noted here for transparency; neither changes the Top 3 or Other Notable findings, which reflect confirmed, recurring activity above the reporting threshold.*

## Business

The Business sector here covers business-services and e-commerce/retail sites , customer account portals, checkout flows, and CMS-driven storefronts , tracked across the smallest number of domains of any sector this quarter.

### Q2 2026 Industry Snapshot

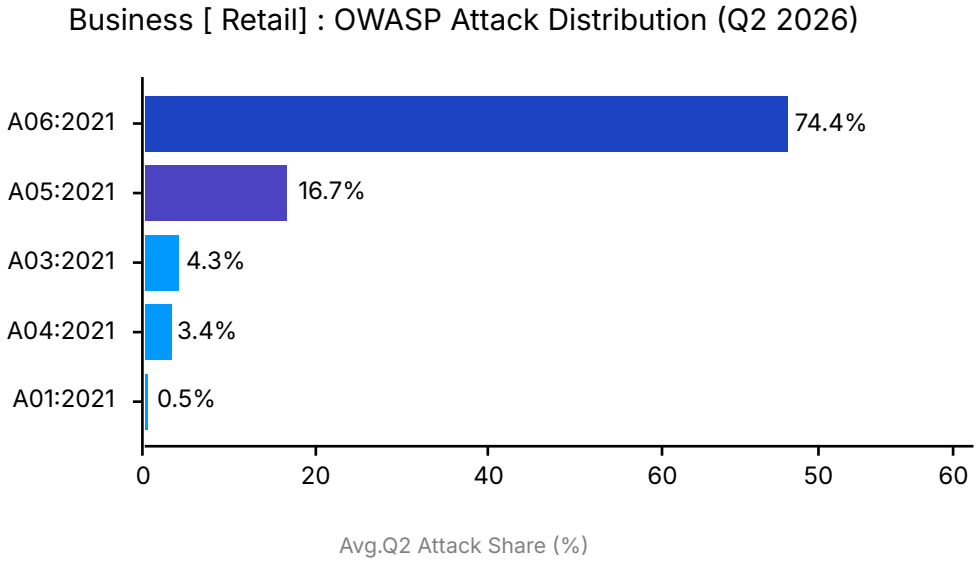
| 68,791,379 | 59,004 | 0.09% | 0.12% |
|---|---|---|---|
| Total Requests (Q2) | Total Attacks (Q2) | Avg. Attack Rate | Peak Monthly Rate |

*Monthly attack rate , April: 0.06% • May: 0.08% • June: 0.12% Monitored footprint: across 5 domains (11,801 attacks per domain this quarter).*

This is one of only two sectors where attacks actually fell this quarter, down a modest 6.9% from Q1 , essentially flat next to the much bigger swings we saw elsewhere. The attack rate stayed low all quarter, peaking at just 0.12% in June, the lowest ceiling of any sector in this report.

### Top 3 Attack Categories

| OWASP Category | Threat | Avg. Q2 Share | Peak% |
|---|---|---|---|
| A06:2021 | Vulnerable and Outdated Components | 74.44% | 80.32% May |
| A05:2021 | Security Misconfiguration | 16.73% | 19.42% June |
| A03:2021 | Injection | 4.34% | 7.76% April |



Outdated components remained the dominant threat throughout Q2,accounting for 74–80% of attacks and pointing to persistent exploitation of legacy cms plugins and e-commerce components.

Security misconfiguration peaked at 19.4% in June, indicating increased exposure from storefront and account-management configurations,though component exploitation remained the primary risk.

## Other Notable Attack Activity

| OWASP Category | Threat | Avg. Q2 Share | Peak % |
|---|---|---|---|
| A04:2021 | Insecure Design | 3.43% | 6.97% April |
| A01:2021 | Broken Access Control | 0.48% | 0.97% June |
| A07:2021 | Identification and Authentication Failures | 0.24% | 0.53% April |

Insecure design peaked in April, ahead of misconfiguration's later rise in June , again fitting the broad-probe-then-narrow-in pattern we've seen elsewhere. Access-control and login-attack findings both stayed low and steady , more like routine background bot traffic than a specific, active campaign against this sector.

**Threat Analysis**

Business is the calmest, lowest-intensity sector this quarter: volume is basically flat, the attack-rate ceiling is the lowest in the report, and the dominant outdated-components problem, while a big share, sits on top of the smallest attack volume of any industry here. Basic hygiene,keeping components current, reviewing configuration , would cover most of what we saw.

05 | Q1 → Q2 COMPARISON

# What Changed Between Q1 and Q2 2026

### The 18% overall drop hides very different stories underneath

Total attacks fell 18% from Q1 to Q2 (20M → 16.4M) while traffic grew 17% (≈2B → 2.33B requests). But seven of eleven industries actually saw attacks go up this quarter, four of them by more than 140%. The overall drop comes almost entirely from one sector settling down after a huge Q1 spike , not from things generally getting quieter.

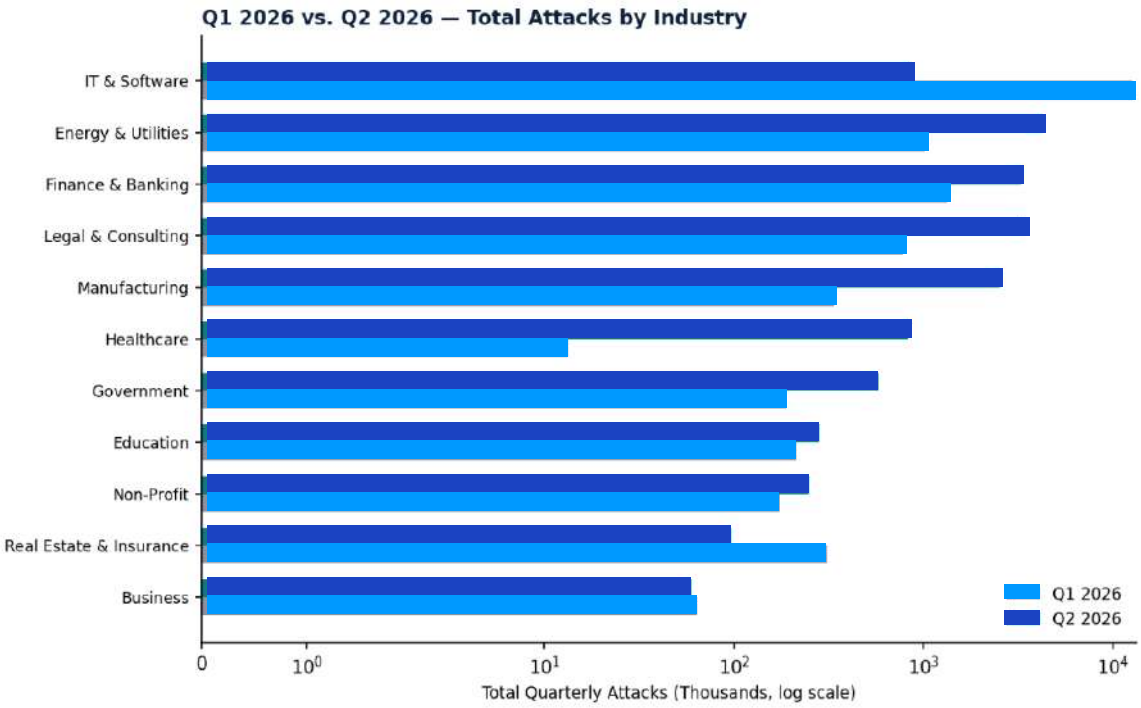



*Figure 4. Q1 2026 vs. Q2 2026 total attacks by industry (log scale).*

| Industry | Q1 Total | Q2 Total | Change |
|---|---|---|---|
| Healthcare & Pharmaceuticals | 13,234 | 828,054 | +6157.0% |
| Manufacturing & Industrial | 335,741 | 2,513,747 | +648.9% |
| Legal & Consulting Services | 782,878 | 3,458,401 | +341.8% |
| Energy & Utilities | 1,020,560 | 4,247,684 | +316.1% |
| Government & Public Sector | 187,959 | 572,675 | +204.7% |
| Finance & Banking | 1,336,584 | 3,263,603 | +204.7% |
| Non Profit | 172,951 | 247,332 | +43.0% |
| Education | 211,812 | 281,218 | +32.8% |
| Business | 63,351 | 59,004 | −6.9% |
| Real Estate & Insurance | 308,901 | 97,110 | −68.6% |
| Information Technology & Software | 12,584,365 | 838,669 | −93.3% |

### HOW "CHANGE" IS CALCULATED

Change % = (Q2 Total − Q1 Total) ÷ Q1 Total × 100. Work example , Finance & Banking: (3,263,603 − 1,336,584) ÷ 1,336,584 × 100 = +144.2%. Q1 totals are the published per-industry figures from the Q1 2026 report (summed across January–March); Q2 totals are month sums from this quarter's telemetry,described in Limitations.

Why this matters: A single percentage doesn't tell a CISO where to actually focus the industry breakdown. Healthcare jumping 6,157% means a sector that barely registered in Q1 needs real security investment now, not next year.

Four other sectors more than doubling or tripling shows attackers aren't settling on fixed targets they're actively probing and shifting quarter to quarter, which means last quarter's risk assessment is already out of date. And the two big drops, IT & Software and Real Estate & Insurance, aren't a sign those sectors got safer.

In both cases, a one-time spike from Q1 simply didn't repeat, the underlying exposure (outdated components, weak API authentication) is still sitting there, waiting to be probed again.The headline number says attacks fell 18% and things are calming down. The industry breakdown says the opposite: figure out where the real movement is, because it isn't evenly spread.

06 | FORECAST & INDUSTRY BENCHMARKS

# Q2 2026 in the Broader Threat Landscape

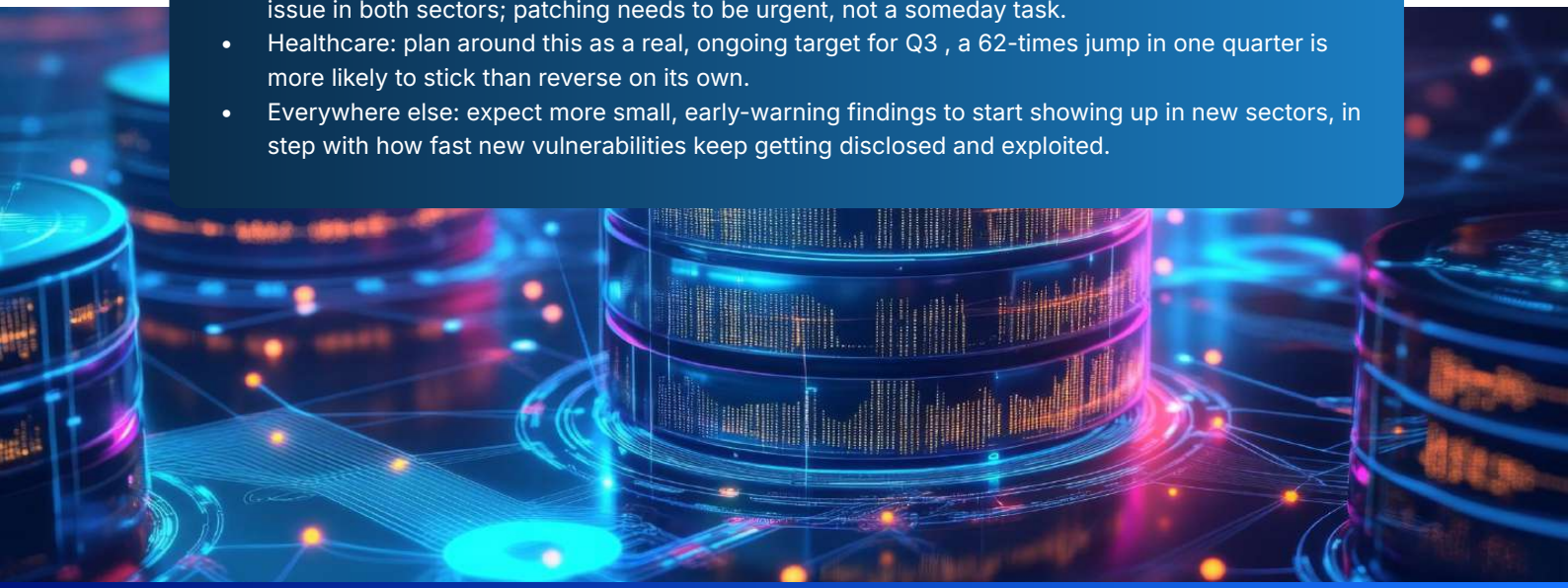
## How this compares to the wider industry picture

Outside research from 2025–26,including Mandiant's M-Trends findings, Cisco Talos data, and reports from Cloudflare and NETSCOUT , describes the same shift we're seeing in our own numbers: attacks moving away from noisy, broad scanning and toward precise, business-targeted campaigns, with exploited vulnerabilities now overtaking stolen passwords as the top way attackers get in.

| Industry | What Outside Research Shows | What We Found in Q2 | Do They Match? |
|---|---|---|---|
| Finance (BFSI) | Vulnerability attacks and DDoS both spiking sharply around geopolitical events, per external reporting | Login attacks hit 92.4% in June, up 144.2% for the quarter | Yes , Finance is escalating in both views |
| Insurance | Vulnerability attacks reported as the fastest-growing threat of any sector studied | Real Estate & Insurance: outdated components made up 85–88% of attacks all quarter | Yes , component risk defines this sector either way |
| Healthcare | Industry research points to accelerating attacks and rising DDoS activity | Healthcare: up 6,157% for the quarter (13K → 828K) | Our numbers show an even sharper jump than the wider industry trend |
| Manufacturing | External data shows years of steady growth in vulnerability exploitation | Manufacturing: up 648.9% for the quarter, the sharpest single-month jump we saw | Yes, and more pronounced , our data is moving faster |
| SaaS / IT | Industry benchmarks flag a real chance of a major DDoS event each year | IT & Software: down 93.3% after Q1's scanning burst wore off | The drop reflects a scan ending, not a threat that's gone away. |

### What to watch heading into Q3

- Finance: expect the login-attack spike to come back again , possibly around September, following the March/June pattern , unless ongoing monitoring closes that two-month blind spot.
- Energy & Manufacturing: the outdated-components problem is close to becoming almost the only issue in both sectors; patching needs to be urgent, not a someday task.
- Healthcare: plan around this as a real, ongoing target for Q3 , a 62-times jump in one quarter is more likely to stick than reverse on its own.
- Everywhere else: expect more small, early-warning findings to start showing up in new sectors, in step with how fast new vulnerabilities keep getting disclosed and exploited.



## 07 | Recommendations

### 01 Patch Virtually, and Patch Fast

Outdated components made up 48.2% of every attack we blocked , and 85.9% in Real Estate & Insurance, 77.6% in Energy & Utilities. Where real component upgrades take months or years, virtual patching at the firewall is the only thing that closes the gap between a bug being disclosed and someone exploiting it.

### 02 Keep a Live Inventory of Every API

Finance's login-attack pattern , quiet in April and May, then 92.4% of June's attacks, matching the exact same shape from Q1's March , shows that a quarterly API audit will miss a pattern that disappears for two months and comes back on the third.

### 03 Use Behavior-Based Bot Detection

Education's 17.6% spike in April and Non-Profit's 15.1% spike, both in login attacks, plus a steady low-level hum in Government and Business, point to automated login-abuse tools running in the background no matter what else is happening that month.

### 04 Protect Against DDoS at Every Layer

Real Estate & Insurance hit a 3.95% attack rate in April and Finance hit 3.02% in May, both showing that a volume spike can arrive with almost no warning and hit hard in a single month. Protection needs to cover both the big, obvious floods and the quieter attacks built to slip under normal rate limits.

### 05 Protect Business Logic, Not Just Code

Design weaknesses grew in over half the industries we tracked , Manufacturing (37.6%, almost tied with component attacks), Government (30.2%), Non-Profit (34.4%, the top category by June). Patching components or filtering injection attacks won't catch these, they need protection built around how the application actually behaves.

### 06 Keep Firewall Rules Actively Tuned

The scan-first, strike-later pattern showed up in five different industries this quarter. A firewall ruleset that only gets reviewed once a quarter will always be a step behind an attack that visibly changes shape within that same 90 days.

### 07 Make MFA and Credential Protection Standard

Finance's login-attack problem, plus a steady trickle of login attacks in nearly every other industry, makes the case that strong multi-factor authentication and ongoing session checks should be standard everywhere,not a nice-to-have reserved for the highest-risk apps.

### 08 Be Ready to Respond Fast to New Vulnerabilities

Outdated components went from 41.8% to 48.2% of all attacks between Q1 and Q2,known vulnerabilities are being exploited more,not less. Every organization needs a tested plan for rolling out an emergency virtual patch the moment a serious new CVE drops.

08 | CONCLUSION

# Q2 2026 Application Threat Analysis Summary & Takeaways

**KEY TAKEAWAY**

Finance & Banking's API2:2023 Broken Authentication surge recurred in June at 92.4% of monthly activity , confirming Q1's forecast that this was a durable, not one-off, attack pattern. Combined with A06's continued deepening (48.2%, up from 41.8%) and Healthcare's 62× volume increase, Q2 shows the application threat landscape concentrating around fewer, more persistent techniques rather than broadening. These are structural conditions that will persist into Q3 unless addressed at the runtime protection layer.

Q2 2026 telemetry reinforces rather than contradicts Q1's structural conclusions: component vulnerabilities and injection remain the two dominant cross-sector threats, and API-layer authentication abuse in Finance is now a confirmed recurring pattern rather than an isolated event. The sharpest change this quarter is Healthcare's emergence as an actively targeted sector, significant enough to warrant its own re-baseline heading into Q3. Across the reconnaissance-to-exploitation sequencing seen in five separate industries, the throughline is consistent: attackers are probing broadly before committing to concentrated exploitation, and organizations that treat a quiet month as resolution rather than a pause are the ones most likely to be caught unprepared when the pattern recurs.

## Limitations

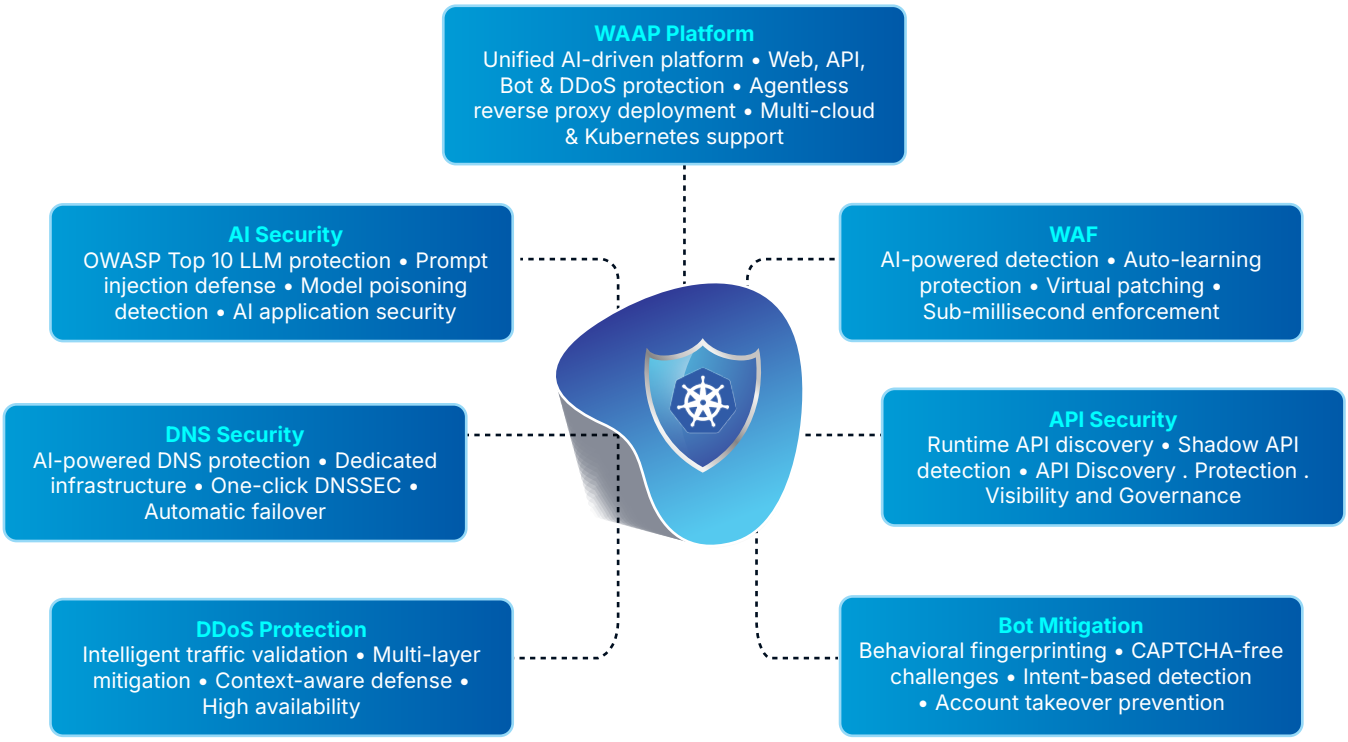
- Q2 2026 reflects telemetry from Prophaze-monitored domains only; findings emphasize relative exposure and directional insight across the monitored estate, consistent with Q1's methodology.
- OWASP category classifications describe classes of weakness being probed, not confirmed vulnerabilities or successful compromises at any specific organization.
- Threats recorded at 0% represent confirmed but negligible activity, fewer than 10 events per 100,000 requests , zero does not mean absent. This applies throughout this report, including the "Other" category rows in the OWASP breakdown tables and any month/industry combination where a category is not separately listed.
- Industry classification reflects the categorization used in the Prophaze monitoring dataset; Business & Retail combines business-services and e-commerce/retail platforms under a single category, consistent with Q1.
- Q1 comparison figures are drawn from the published Q1 2026 report; minor rounding differences between per-industry sums and headline totals in that report are preserved as originally published.

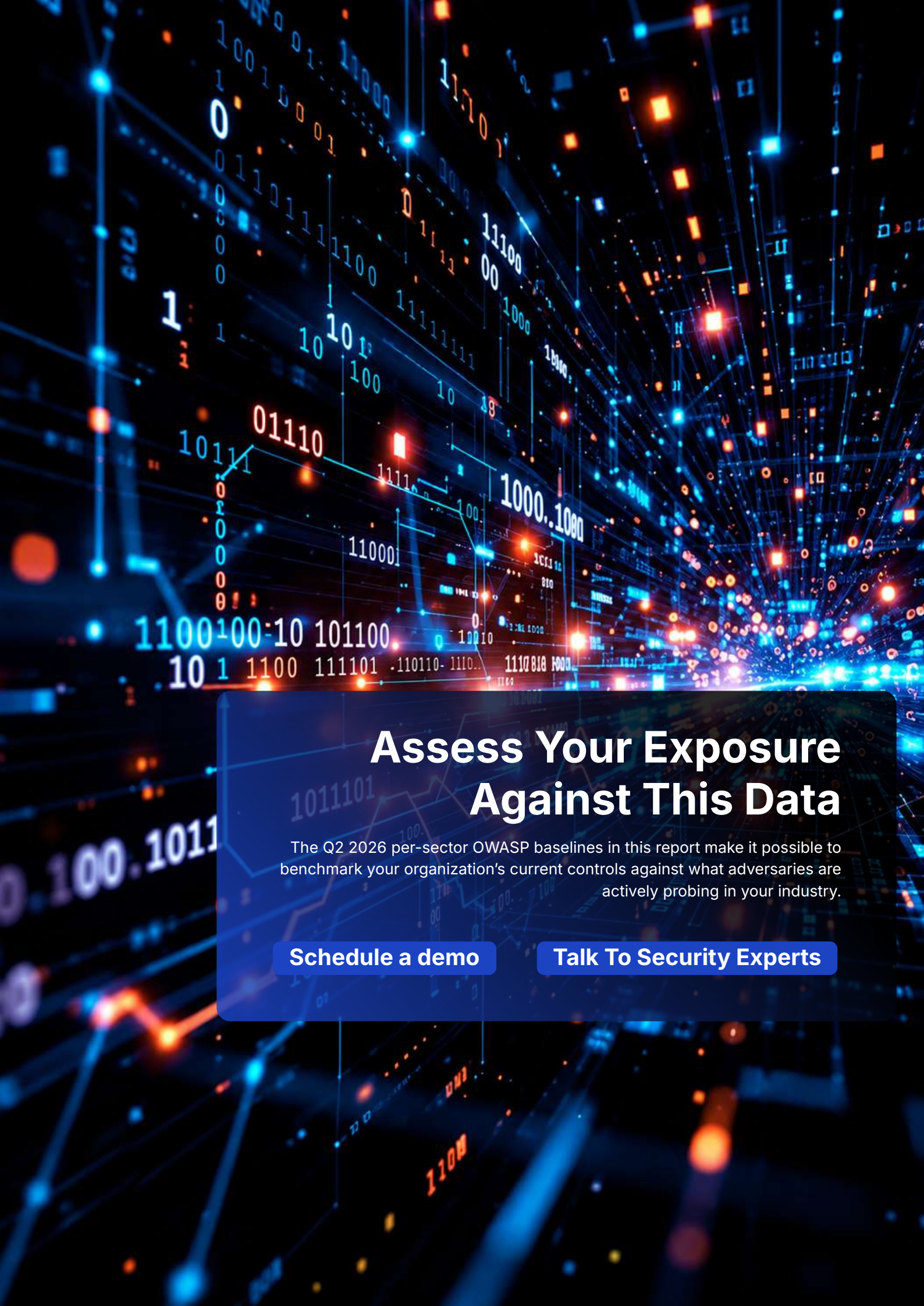
09 | PROPHAZE PLATFORM

# One Platform. Every Attack Vector. Any Environment.

## PROPHAZE Fully Manage 360° Web Application Security That You Can Afford

AI-powered. Monitored 24×7 by security analysts. Protecting against DDoS, bots, API attacks, OWASP Top 10, and zero-day threats.



# Assess Your Exposure Against This Data

The Q2 2026 per-sector OWASP baselines in this report make it possible to benchmark your organization's current controls against what adversaries are actively probing in your industry.

**Schedule a demo** **Talk To Security Experts**