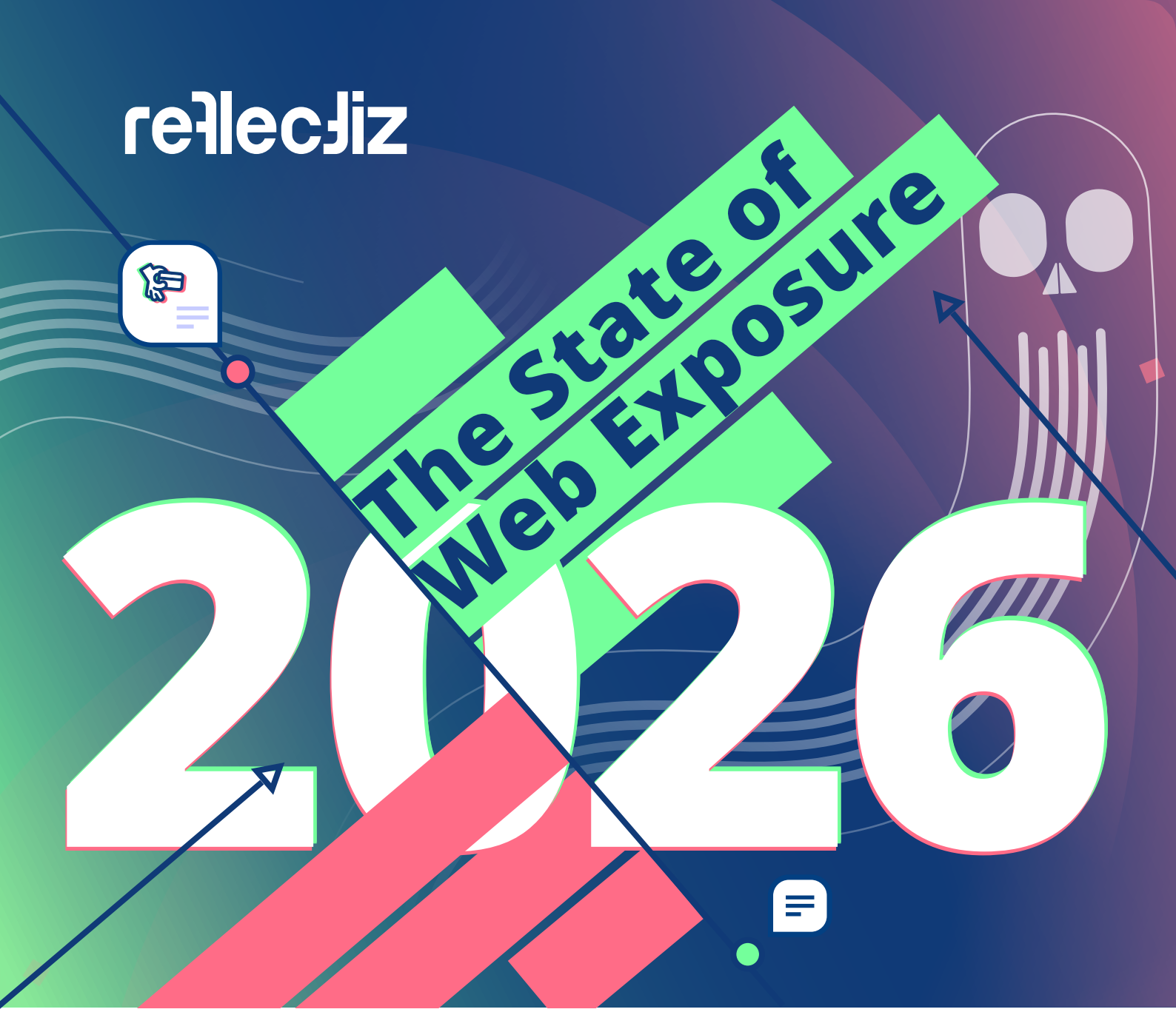


Web Exposure: The Invisible Supply Chain Crisis

Gartner coined "Web Exposure" to describe risks from the dozens of third-party apps, CDN repositories, and open-source tools that modern websites depend on for tracking and functionality. Each connection expands the exposure surface, creating targets for attackers. While these dependencies are unavoidable, they can be secured – starting with ensuring third-party apps don't unnecessarily access sensitive personal, financial, and health data.

The 2026 State of Web Exposure Report reveals a troubling paradox: while organizations reduced some third-party dependencies, unjustified access to sensitive data surged from 51% to 64%, nearly double the rate of justified access. These applications have no legitimate business need for the data they're accessing.

Analyzing 4,700 leading websites across 10 industries, Reflectiz found accelerating security polarization. Insurance slashed malicious activity by 60%, jumping five positions to become the cleanest sector. Education's malicious activity quadrupled to 14.3%. Healthcare stagnated across all risk metrics despite strict HIPAA obligations. Marketing and Digital departments now drive 43% of all third-party risk, often operating without security oversight.

The gap between leaders and laggards is widening. What follows proves it.

THE CRISIS

64%

of apps accessing sensitive data lack business need

up from **51%** in 2024

14.3%

of education sites are compromised

quadrupled from **3.75%** in 2024

81% of security teams call web attacks a top priority

But only

39%

have deployed solutions.

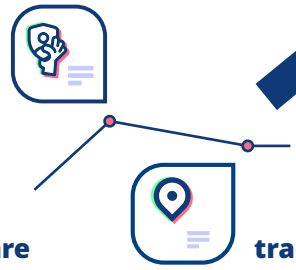
43%

of web risk is originated in the Marketing/Digital department

SECTOR-SPECIFIC RISKS

2.5

apps on average in healthcare sites access Protected Health Information (PII/PHI) without authorization.



16

trackers per publisher site

33% increase, highest exposure.

EMERGING THREATS

3.8x

more recently registered domains on compromised sites vs. clean sites.

16.5%

of sites with marketing pixels use the TikTok pixel second to Facebook pixel at 53%.

10% (2024) → **14%** (2025)

Retail payment frame risk up 4 percentage points, expanding skimming attack surface at checkout

11% (2024) → **15%** (2025)

of improper PII access comes from tag managers.

28% (2024) → **39%** (2025)

of public CDN apps are cloud services.

PROGRESS IS POSSIBLE

40%

reduction in apps running in payment frames

reduction in apps running in payment frames across industries

Methodology

This report utilizes data from Reflectiz's proprietary Exposure Rating system. Reflectiz continuously monitors millions of websites, producing a vast pool of information that enables highly accurate calculation of web risk exposure ratings. The system analyzes various risk factors in this dynamic dataset and consolidates them into a single, easy-to-understand metric, allowing for direct comparisons of web risk exposure between different websites.

To provide a comprehensive and representative view of observed threats, Reflectiz researchers have normalized the data to the 75th percentile of customers. This approach eliminates outliers and extreme cases that might distort the overall findings.

To ensure privacy, all data in this report has been anonymized.

The research was conducted in November 2025, using Exposure Rating data gathered over one year. This year's analysis expanded, providing a broader and more robust view of the web security landscape.

This report includes Exposure Rating results of the top 100 websites in each industry (by highest number of visitors).

Survey Methodology

Reflectiz surveyed 128 security leaders in late 2025 to align technical findings with practitioner insights. Respondents represent large organizations (95% with 1,000+ employees) in healthcare, finance, and retail. This survey (n=128) provides qualitative context on budgets and priorities to support the technical analysis of 4,700 websites.

Table of Contents

Introduction

What is Web Exposure?

Web exposure encompasses all third-party code, scripts, and integrations that execute on your website, creating potential attack vectors beyond your direct control. Unlike traditional perimeter security that protects servers and networks, web exposure represents the client-side risk landscape – everything that runs in users' browsers, from Google Analytics and Facebook Pixel to payment processors and tag management platforms.

Each third-party app introduces supply chain risk: if any connected vendor is compromised, attackers can inject malicious code directly into your customers' sessions, harvesting sensitive data, skimming payment information, or deploying ransomware. Web exposure is especially dangerous because most organizations lack visibility into what third-party code is actually running on their sites, how it's accessing customer data, or whether it's been compromised.

Understanding Exposure Rating

Reflectiz's Exposure Rating system consolidates multiple risk factors into a single grade (A-F), enabling direct security comparisons across websites and industries. The rating analyzes:

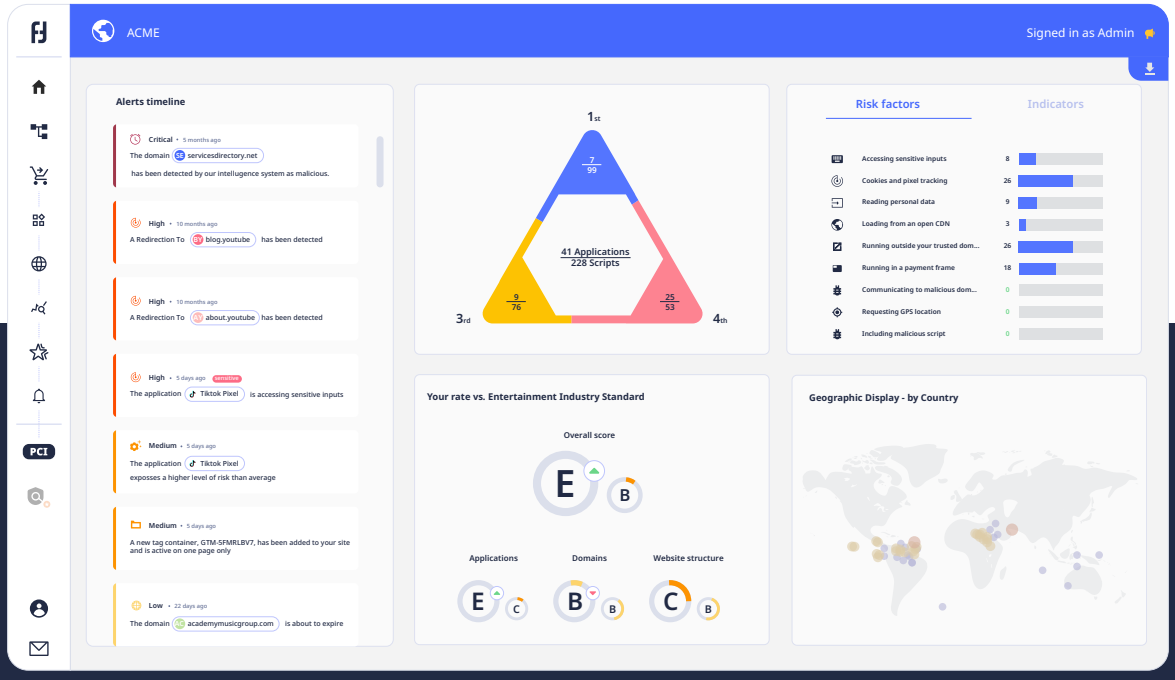
Third-party app volume and toxicity (trackers, analytics, marketing tools)

Sensitive data access patterns (credit cards, credentials, PII/PHI)

Payment frame security (scripts running during checkout)

Supply chain dependencies (public CDN usage, recently registered domains)

Malicious activity indicators (infections, redirects, mixed content vulnerabilities)



reflectiz

Key Findings

The web exposure landscape in 2025 revealed a troubling paradox: while organizations reduced some third-party dependencies, unjustified access to sensitive data surged dramatically. Combining technical analysis of 4,700 websites with insights from 128 security leaders reveals both what is happening and why organizations struggle to address it.

Top 5 Findings

1.

Security Gap Widens

Organizations cluster at average ratings (B-C grades) while Government and Education malicious activity surges; Insurance and Healthcare lead improvements.

2.

The Priority-Action Gap

While 81% of security teams rank web protection as a top priority, only 39% have dedicated solutions. Resource constraints -- budgets (34%), regulation (32%), and staffing (31%) -- fuel this gap. Consequently, unjustified data access surged to 64%, nearly doubling legitimate access (36%).

3.

Sector-Specific Risk Patterns

Apps in Retail payment frames decline 29% (from ~7 to ~5 apps per site). Healthcare stagnates completely, Finance moves backward on sensitive data.

4.

Malicious Site Indicators Emerge

Recently registered domains appear 3.8x more on compromised sites, the strongest malicious activity predictor.

5.

Marketing and Digital Drive Exposure

Combined 43% of third-party risk, with Marketing alone (26%) exceeding IT departments (18%).

1. Security Gap Widens

Mid-Range Clustering

Organizations increasingly gravitated toward average exposure ratings (grades B and C), with fewer A-grade top performers. While F-grade sites remained relatively stable at approximately 4%, the overall trend shows clustering toward median security posture rather than excellence.

Malicious Activity Surges in Critical Sectors

Government sites exploded from 2% to 12.9%, while Education infections increased from 3.75% to 14.3%.

Insurance Leads Security Turnaround

Slashed malicious activity from 3.3% to 1.3%. Meanwhile, Healthcare maintained its #1 overall security ranking for the second consecutive year.

2. The Priority-Action Gap

Recognition Without Resources

81% rank web protection as top priority, yet only 39% have dedicated solutions. 66% allocate ≤25% of security budgets to web security.

Budget (34%), regulation (32%), and staffing (31%) constraints create equal pressure, forcing "good enough" over excellence.

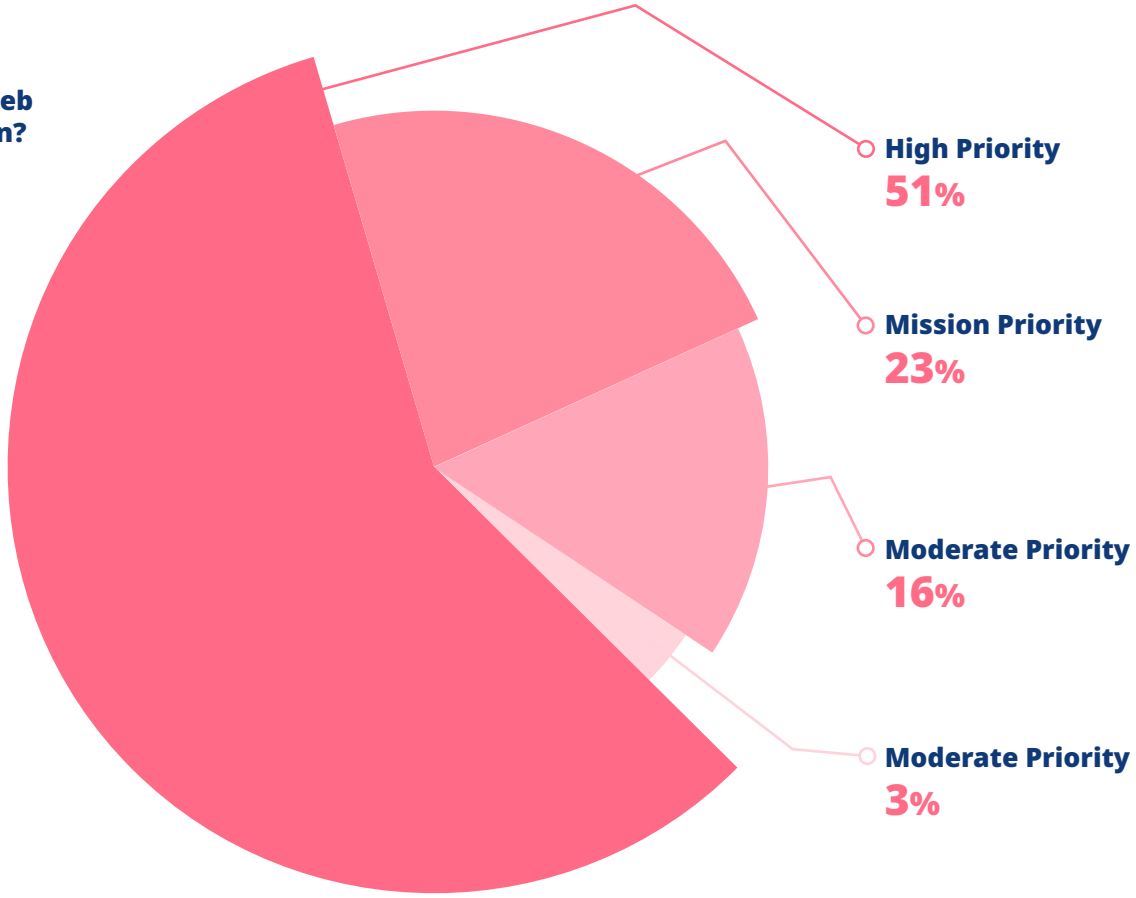
Fighting Yesterday's Battles

Organizations deploy WAFs (21%) for server-side threats while only 8% use Client-Side testing -- a 2.6× mismatch. 24% rely on "general tools" not built for web exposure, creating false protection.

The Governance Vacuum

48% connect to 26+ domains, yet 14% don't know their exposure. Without automated governance, unjustified data access surged from 51% to 64%, nearly double legitimate access (36%). Organizations discover this only during breaches.

How Critical is Web Attack Protection?



81% classify it as high/ mission priority

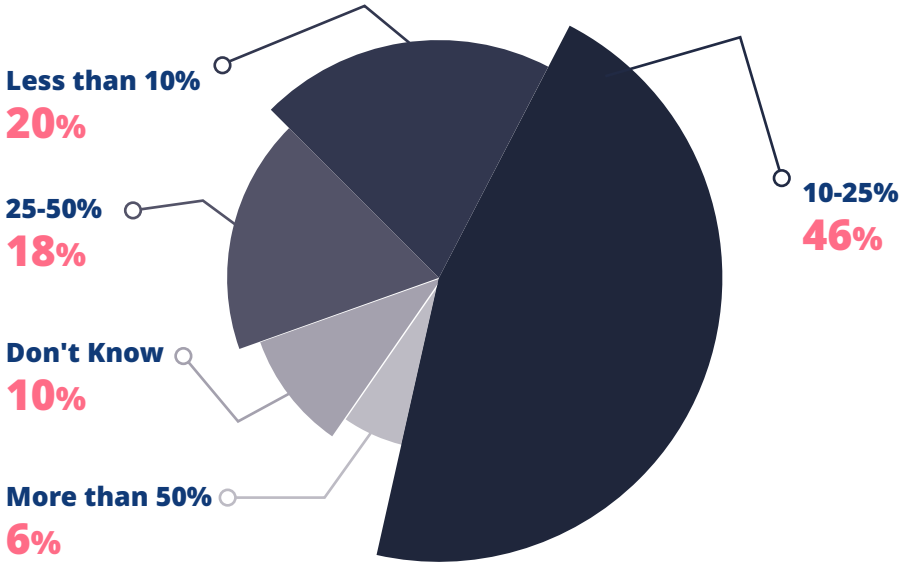
ONLY 3% consider it low priority, showing universal recognition of the threat.

ONLY 39% have dedicated solutions, creating a 42-point priority-action gap.

Web Security Budget Allocation

66%

allocate 25% or less — Web security receives modest funding despite being labeled a high priority by most.



3. Sector-Specific Risk Patterns

Retail

Apps running in payment frames decreased 29% (from ~7 to ~5 apps), showing per-site improvement. However, unjustified access of apps in payment frames increased from 10% to 14%, implying a growing risk.

Healthcare

Complete stagnation across all metrics; 59% tracker exposure unchanged, 25% personal data access unchanged, showing dangerous complacency in a HIPAA-regulated environment.

Finance

Sensitive data exposure increased from 10% to 11%, moving in the wrong direction as fintech partnerships outpace security controls.

Entertainment

Tracker usage exploded 25% while maintaining highest payment frame risk, reflecting aggressive monetization over security.

Publishers

Tracker exposure reached 16 per site (33% increase), driven by ad tech proliferation and content delivery dependencies.

4. Malicious Site Indicators Emerge

Volume Over Toxicity

Compromised sites use twice as many apps (32 vs 16) but similar risk per app; attack surface expansion, not app quality, drives malicious activity.

Recently Registered Domains

Appear 3.8x more often on malicious sites (15% vs 4%), emerging as the strongest single predictor of compromise.

Mixed Content Vulnerability

63% of compromised sites mix HTTPS/HTTP protocols versus 34% of clean sites, creating exploitable security gaps.

CDN Supply Chain Risk

Compromised sites load 2.2x more content from public CDNs, confirming supply chain attacks through shared infrastructure.

5. Marketing and Digital Drive Exposure

Marketing Dominates Risk Creation

Marketing (25.68%) accounts for the largest departmental footprint, with Digital (17.23%) and IT (18.38%) following. Combined, Marketing and Digital create 43% of all third-party exposure.

IT Accountability Doubles

Unjustified sensitive data access by IT-managed apps surged from 8% to 16%, with cloud services and e-commerce platforms over-permissioned.

Google Tag Manager Dominance

Accounts for 8% of all unjustified sensitive data access (single worst offender) with Shopify (5%) and Facebook Pixel (4%) close behind.

Progress vs. Stagnation

The gap between leaders and laggards is widening. Retail cut payment frame apps by 29% (from ~7 to ~5 per site), proving systematic cleanup works, yet Retail's overall payment frame risk increased from 10% to 14%, expanding the skimming attack surface at checkout as e-commerce adoption outpaced controls. Meanwhile, Healthcare showed zero progress across every metric despite HIPAA obligations, and Finance moved backward with sensitive data exposure rising from 10% to 11%.

The lesson
regulatory frameworks alone fail; organizations need automated governance and cross-functional accountability to secure customer data.

What is "Unjustified Access"?

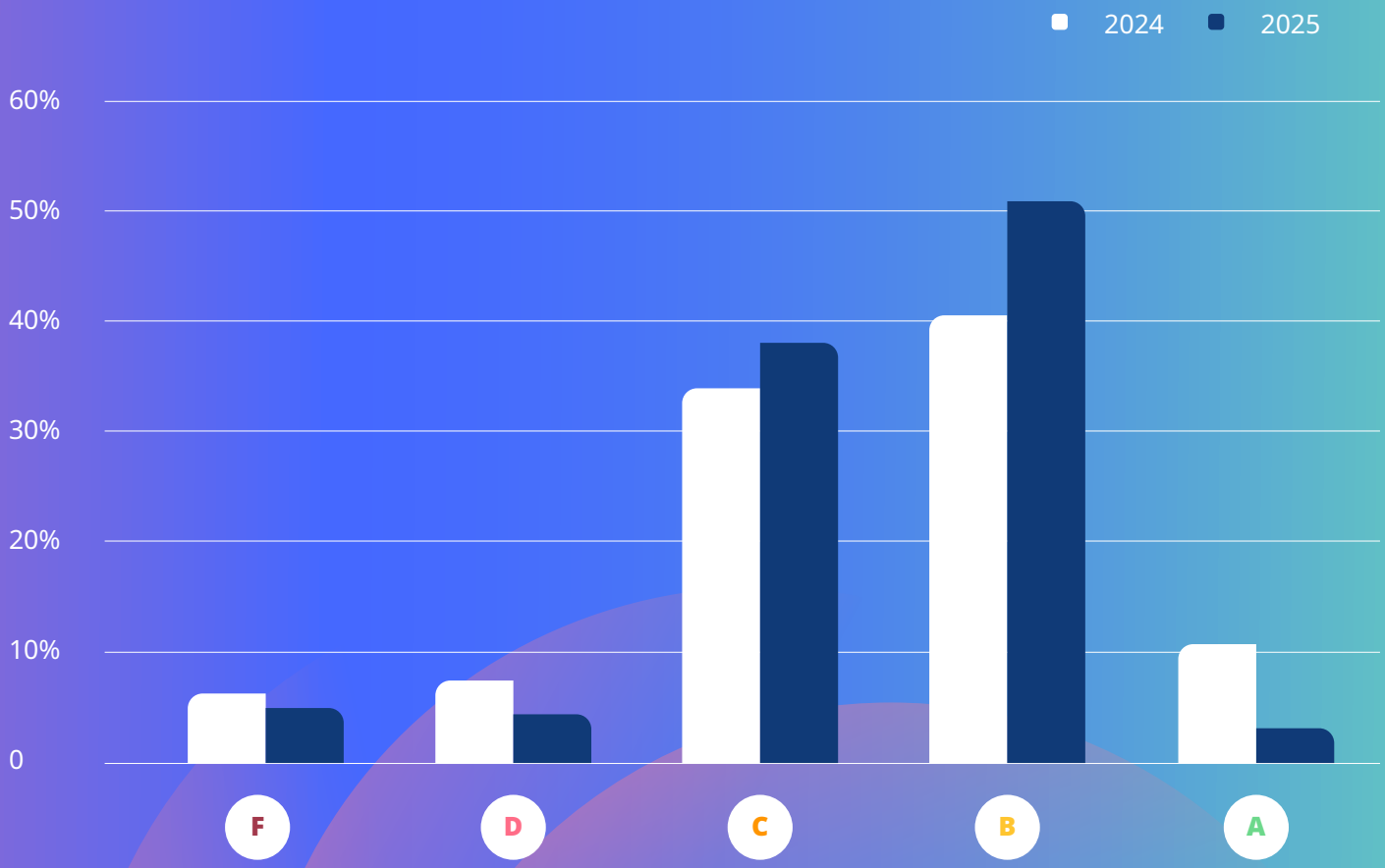
Access is flagged when a third-party script meets any of these criteria:
Irrelevant Function: Reading data unnecessary for its task (e.g., a chatbot accessing payment fields). Zero-ROI Presence: Remaining active on high-risk pages despite 90+ days of zero data transmission.

Shadow Deployment: Injection via Tag Managers without security oversight or "least privilege" scoping. Over-Permissioning: Utilizing "Full DOM Access" to scrape entire pages rather than restricted elements.

Exposure Rating:

Grade Breakdown

Websites distribution by Exposure Rating across industries [4700 leading websites included]. ‘A’ represents the lowest risk while ‘F’ represents the highest risk.

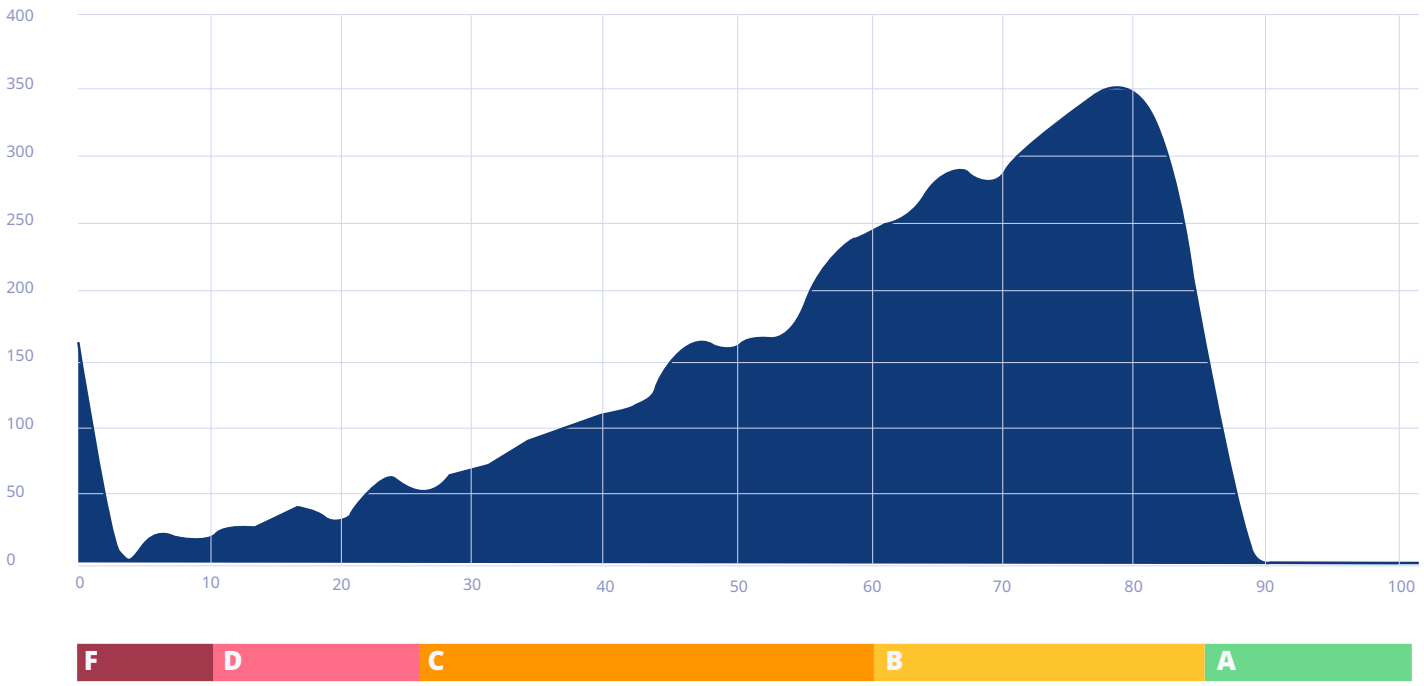


reflectiz

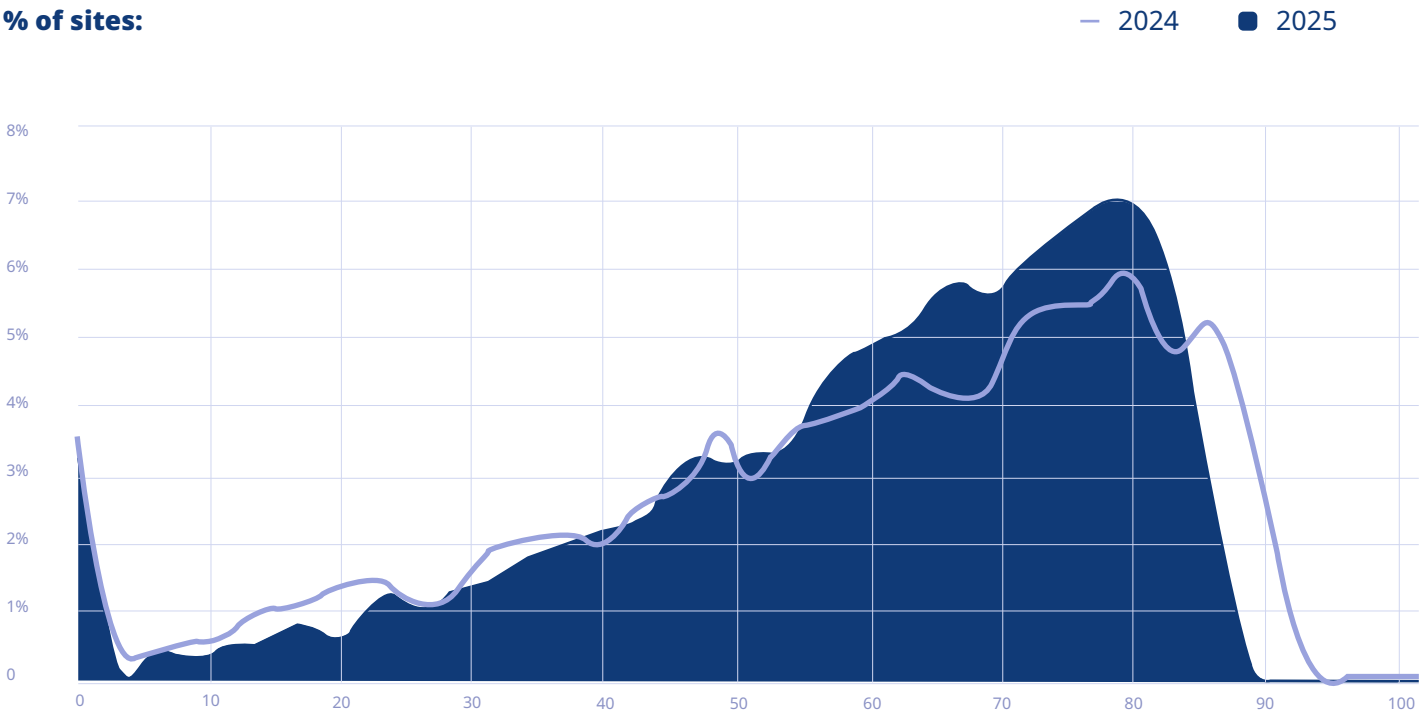
Shifting Toward the Middle

2025 saw a notable shift toward mid-range security ratings, with more organizations achieving C and B grades compared to 2024. The proportion of sites at both ends of the spectrum decreased -- fewer F and D grades (poorest performers) as well as fewer A grades (top performers).

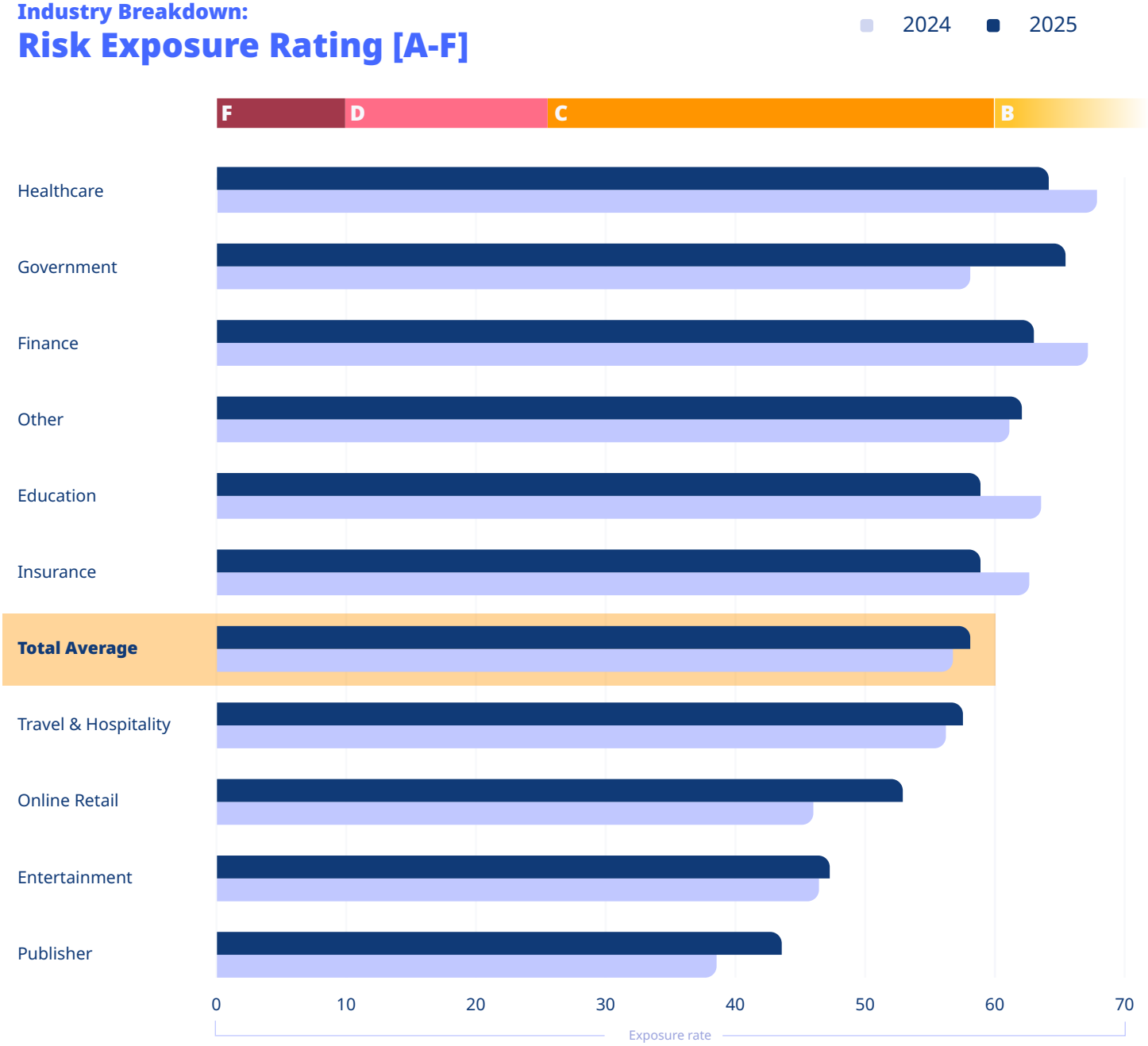
# of sites:



% of sites:



Industry Breakdown:
Risk Exposure Rating [A-F]



Education and Insurance in freefall
Both dropped 2 positions as digital expansion outpaces security investment.

Finance slips despite strong posture
Fell from 2nd to 3rd, likely due to fintech integrations expanding attack surfaces.

Healthcare alone holds the top spot
Only sector maintaining its grade year-over-year, driven by strict HIPAA compliance.

Entertainment hits rock bottom
Dropped to 9th as streaming platforms multiply vulnerabilities.

The security gap widens
Disparity between best and worst performers grows as top sectors improve while bottom sectors decline.

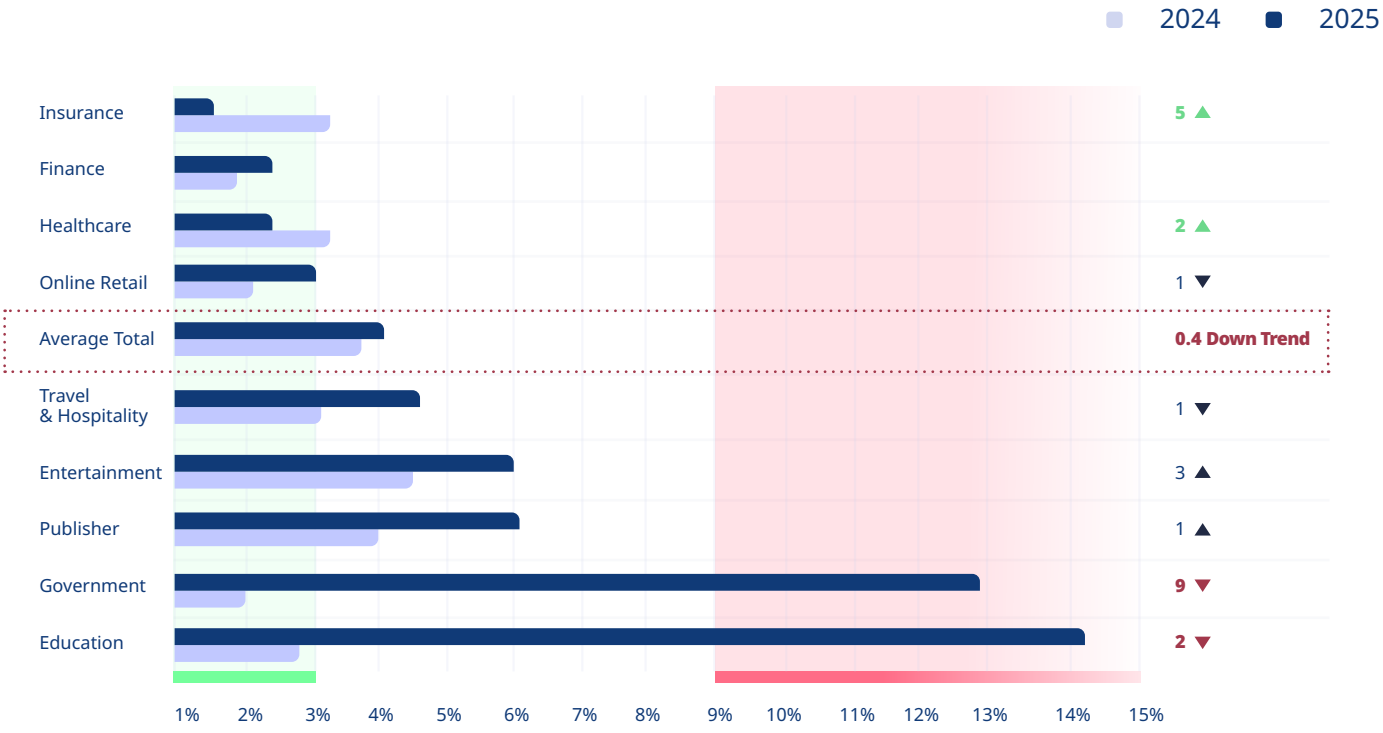
Consumer-facing industries remain riskiest
Travel, Retail, Entertainment, and Publishing stuck at the bottom with no improvement trend.

	2024	2025	Trend
Healthcare	1	1	
Government	6	2	4 ▲
Finance	2	3	1 ▼
Other	5	4	1 ▲
Education	3	5	2 ▼
Insurance	4	6	2 ▼
Travel & Hospitality	7	7	
Online Retail	9	8	1 ▲
Entertainment	8	9	1 ▼
Publisher	10	10	

Malicious Activity

Malicious or compromised scripts don't announce themselves. They hide in legitimate third-party code, waiting to strike. We scanned 4,700 leading websites to identify which industries harbor compromised sites, and the patterns that predict compromise.

A site is classified as compromised when it exhibits one or more of the following: malicious redirects, known malware signatures, connections to blacklisted domains, or suspicious script behavior.



Malicious activity on education sites quadruples

Surged from 3.75% to 14.3%, now hitting 1 in 7 sites.

Government explodes from 2% to 12.9%

The most dramatic deterioration in the report.

Entertainment and Publishing exceed average

Rose to 6.0% and 6.1% respectively; both worsening year-over-year.

Insurance becomes cleanest sector

Dropped from 3.3% to 1.3%, jumping 5 positions.

Finance deteriorates despite low baseline

Increased from 1.75% to 2.4%, signaling more sophisticated attacks.

Conclusion

Government (12.9%) and Education (14.3%) now show up to 11x higher malicious activity rates than Insurance (1.3%), exposing how budget-constrained institutions are losing the supply chain security battle.

Profile of compromised sites

	"Clean"	Compromised activity	Ratio
# of 3rd party apps	16	32	Twice more
# of 3rd party domains	36	100	2.7 times more
Mixed content (HTTPS + HTTP headers)	34%	63%	1.9 times more

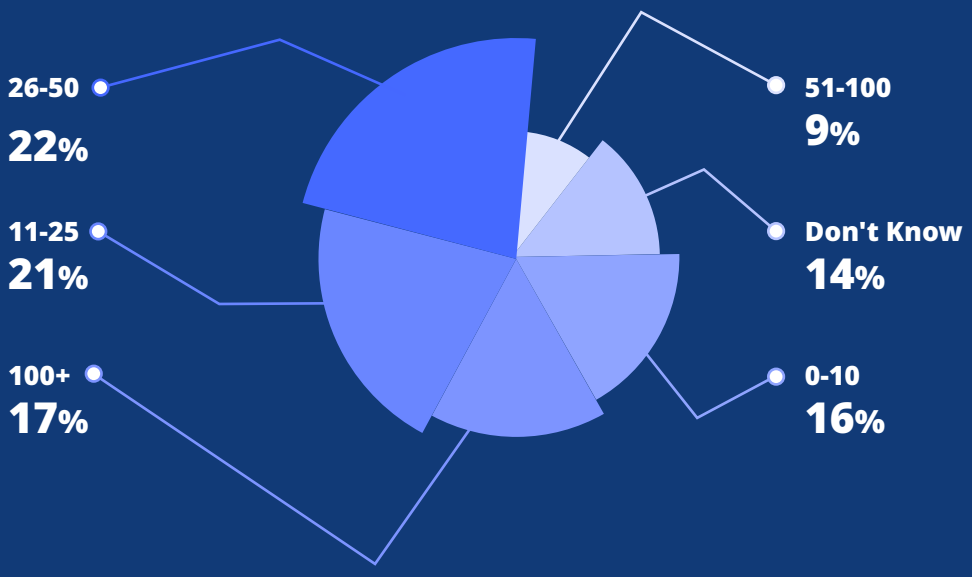
Attack surface expansion, not app toxicity, correlates with compromise. Organizations with weaker governance accumulate dependencies, creating more entry points for attackers.

Selected risk factors by 3rd party component – occurrence per site comparison

Risk source	Risk factor	"Clean"	Compromised activity	Ratio
# of 3rd party apps	Altering Page Structure	10.9	19.2	1.8
# of 3rd party apps	Redirect	0.03	0.07	2.2
# of 3rd party apps	Loaded From a Public CDN	0.8	1.8	2.2
# of 3rd party apps	Self Deleting Code	0.3	0.7	2.2
# of 3rd party apps	Tracker	5.9	11.9	2.0
# of 3rd party domain	Recently registered	4% of sites	15% of sites	3.8

Survey validates research:
48% already in high-risk territory (26+ domains), matching our finding that compromised sites average 100 domains vs. 36 for clean sites. The 14% with no visibility operate completely blind.

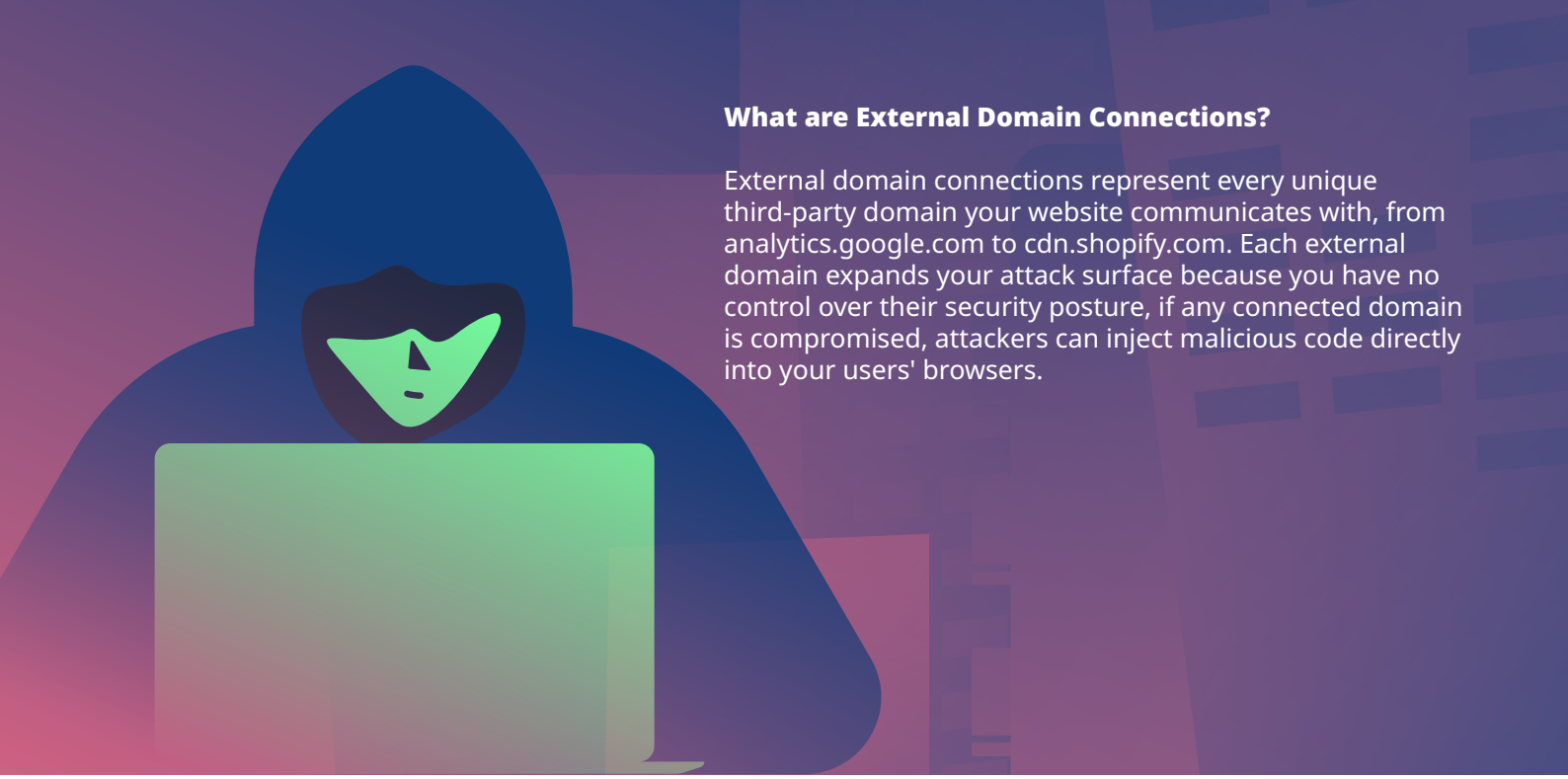
External Domains Your Website Communicates With



48%

interact with 26+ external domains — High third-party exposure creates significant attack surface, with 14% lacking visibility altogether.

reflectiz



What are External Domain Connections?

External domain connections represent every unique third-party domain your website communicates with, from analytics.google.com to cdn.shopify.com. Each external domain expands your attack surface because you have no control over their security posture, if any connected domain is compromised, attackers can inject malicious code directly into your users' browsers.

Key Findings:

Compromised vs. Clean Sites

Volume, not toxicity

Compromised sites use twice as many apps (32 vs 16) but similar risk per app, meaning attack surface expansion drives infection, not app quality.

Recently registered domains are smoking guns

Appear 3.8x more often on malicious sites (15% vs 4%), making new domain connections the strongest infection predictor.

Mixed content: a vulnerability gateway

63% of compromised sites mix HTTPS/HTTP vs 34% of clean sites, nearly doubling exposure as attackers exploit protocol gaps.

Trackers double on compromised sites

11.9 per compromised site vs 5.9 on clean sites (2x), suggesting tracker scripts are common infection vectors or indicators of lax security hygiene.

Public CDN risk intensifies

Compromised sites load 2.2x more content from public CDNs (1.8 vs 0.8), confirming supply chain attacks through shared infrastructure.

Self-deleting code appears 2.2x more often

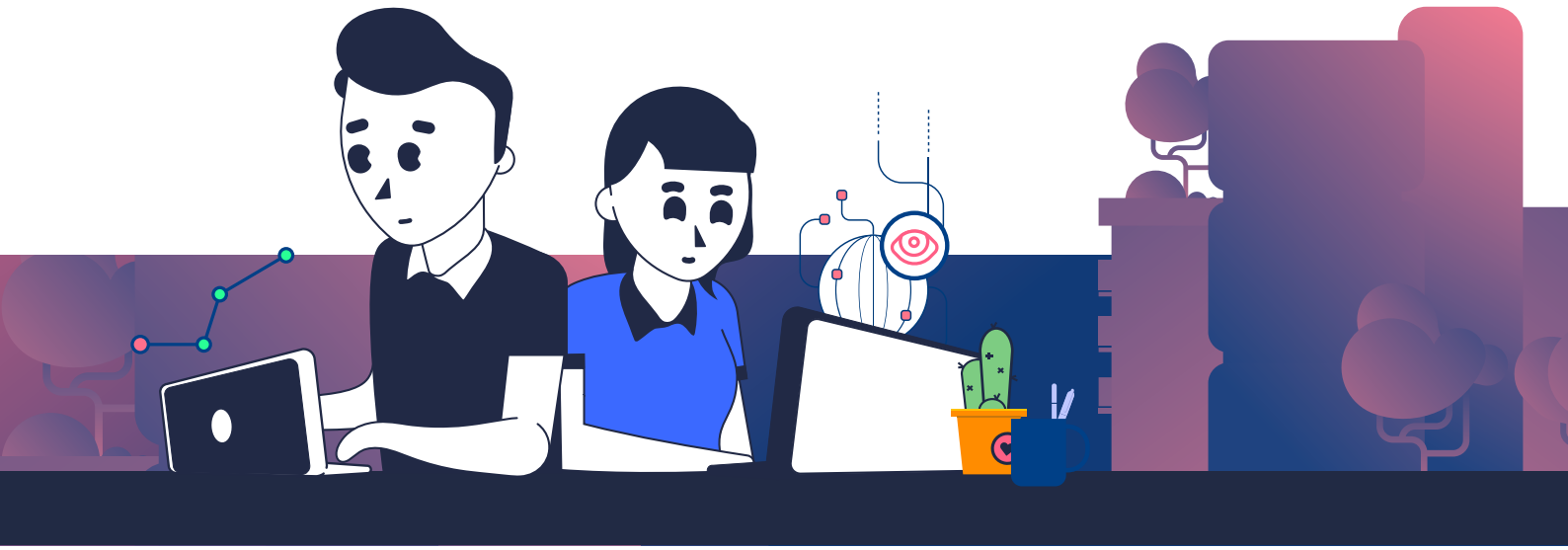
0.7 occurrences on malicious sites vs 0.3 on clean sites, indicating active evasion techniques to avoid detection.

Domain sprawl correlates with compromise

Compromised sites connect to 2.7x more third-party domains (100 vs 36), expanding attack surface and making monitoring nearly impossible.

Redirects signal trouble

Appear 2.2x more on compromised sites (0.07 vs 0.03), used for malvertising, phishing chains, and traffic monetization schemes.



Risk Exposure Factors Across Industries

2026 Risk factors we focuse

1. Apps accessing sensitive data

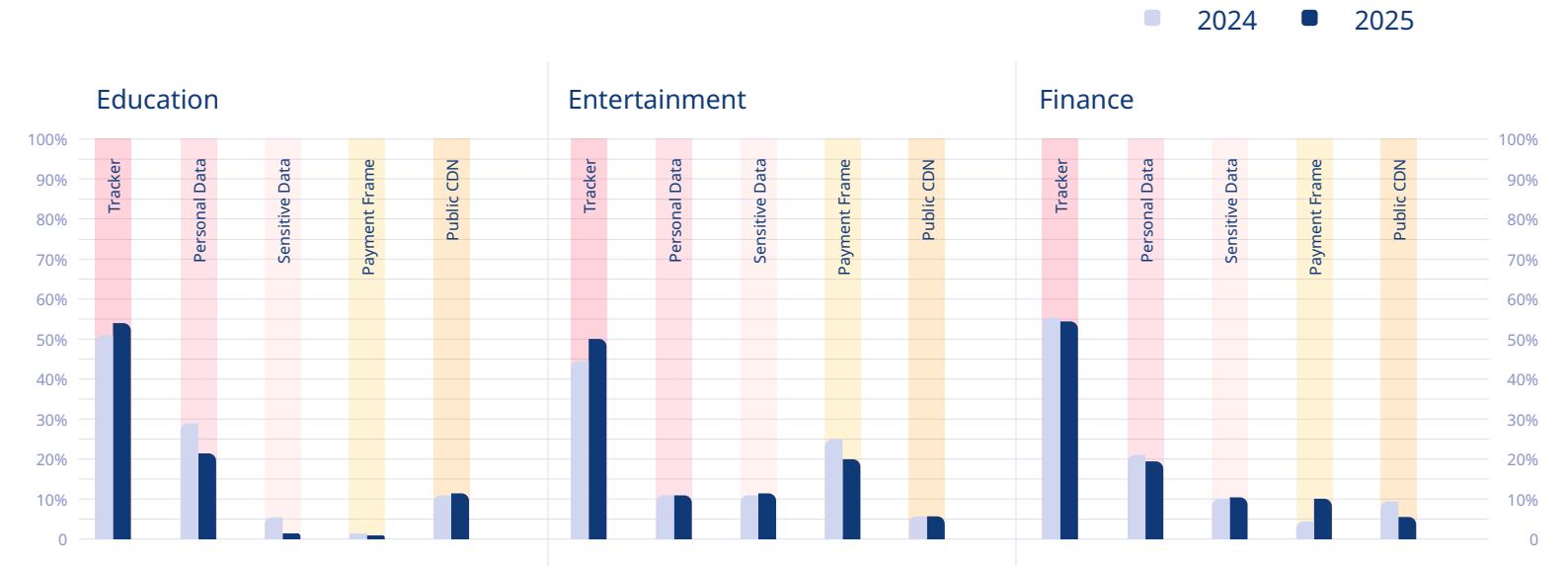
2. Apps accessing personal data

3. Trackers on checkout pages

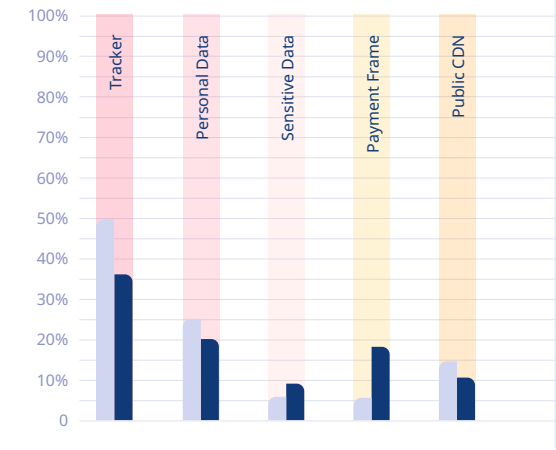
4. Apps running in payment frames [iframes]

5. Apps loaded from public CDNs

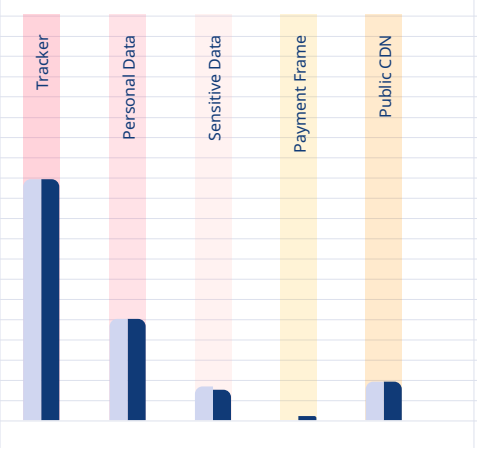
Breakdown per industry:



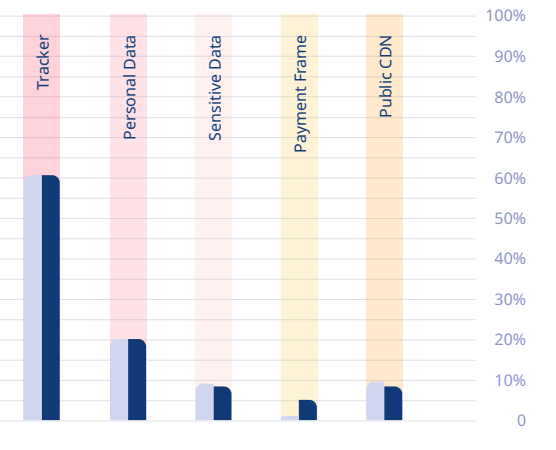
Government



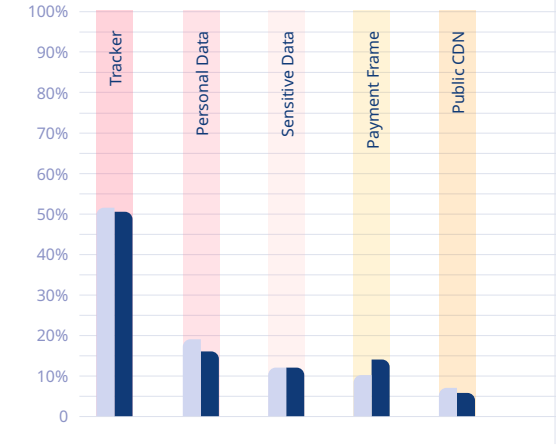
Healthcare



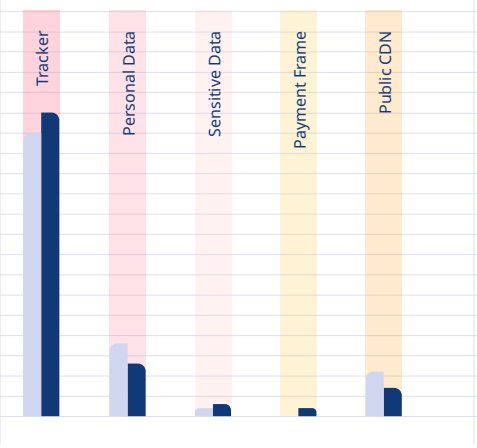
Insurance



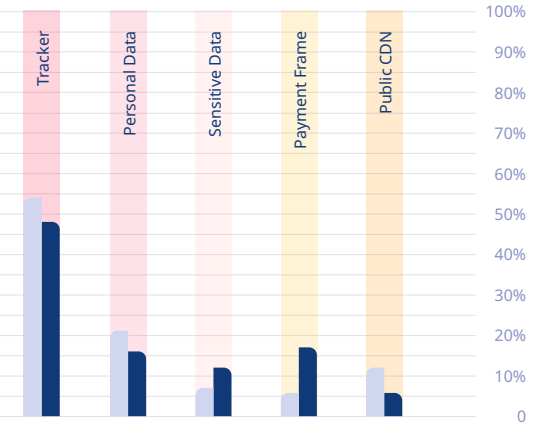
Online Retail



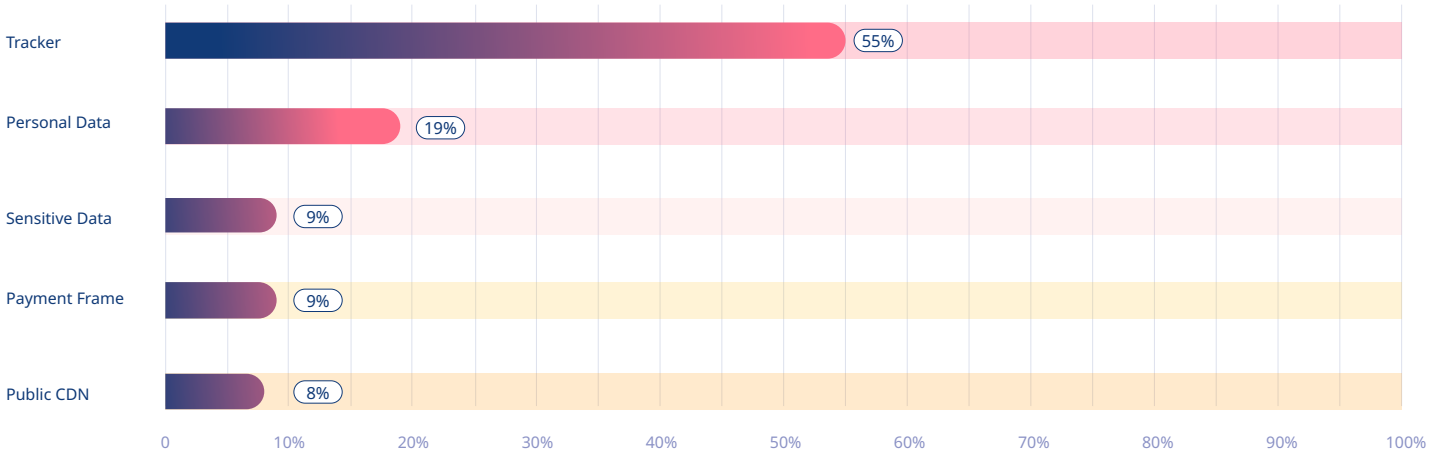
Publisher



Travel & Hospitality



Overall 2024 - 2025 Same results



Year-Over-Year Analysis:

Key Sectors

RETAIL

10% → **14%***
2024 2025

Retail payment frame risk up 4 percentage points, expanding skimming attack surface at checkout.

Tracker exposure barely moves

dropped 2 points to 51%, still exposing half of all sites.

18% → **16%** (-1pp)
2024 2025

Personal data improves slightly

Sensitive data flat at 12%
zero progress protecting critical information.

HEALTHCARE

Complete stagnation

virtually no movement across any risk factor.

Tracker exposure stuck at

59%

unchanged despite HIPAA obligations.

Personal data highest in study

25%

unchanged, worst PII leakage of any sector.

FINANCE

56% → **54%**
2024 2025

(-2pp) Modest tracker decline

Sensitive data exposure rises

10% → **11%**
2024 2025
wrong direction for financial information.

21% → **19%** (-2pp)
2024 2025

Personal data falls slightly

Still high for banking sector.

SURVEY INSIGHT: Perception vs. Reality

When asked about top threats, security leaders ranked:

28%
Data breaches/leaks

20%
Compliance violations

6%
Magecart/card skimming (last place)

Yet our research shows 14% payment frame risk across retail sites. Organizations prioritize regulatory penalties over root cause prevention, explaining why 53% of payment frame apps lack justification.

* Represents percentage of retail sites with third-party apps running in payment frames

Overall Trends

Averages Hide Dramatic Sector Divergence

Frozen at the surface

Grand Total unchanged across all five factors (55% trackers, 19% personal data, 9% sensitive/payment, 8% CDN), suggesting industry-wide stagnation.

Volatility beneath

Individual sectors show dramatic swings: Government payment frames surged +12pp, Entertainment trackers +6pp, Travel payment frames +11pp, while Healthcare and Insurance remained completely static.

Payment frame polarization

Retail (+4pp), Finance (+6pp), Government (+12pp), and Travel (+11pp) all increased risk, yet Entertainment (-5pp) decreased. Average masks opposing trends.

Tracker divergence intensifies

Education (+7pp), Entertainment (+6pp), Publisher (+5pp) surge, while Government (-7pp), Travel (-6pp) decline. No unified strategy emerges.

Compliance doesn't equal security

Healthcare (HIPAA) and Finance show minimal-to-zero improvement on trackers/personal data despite regulatory pressure, proving frameworks alone are insufficient.

Bottom Line

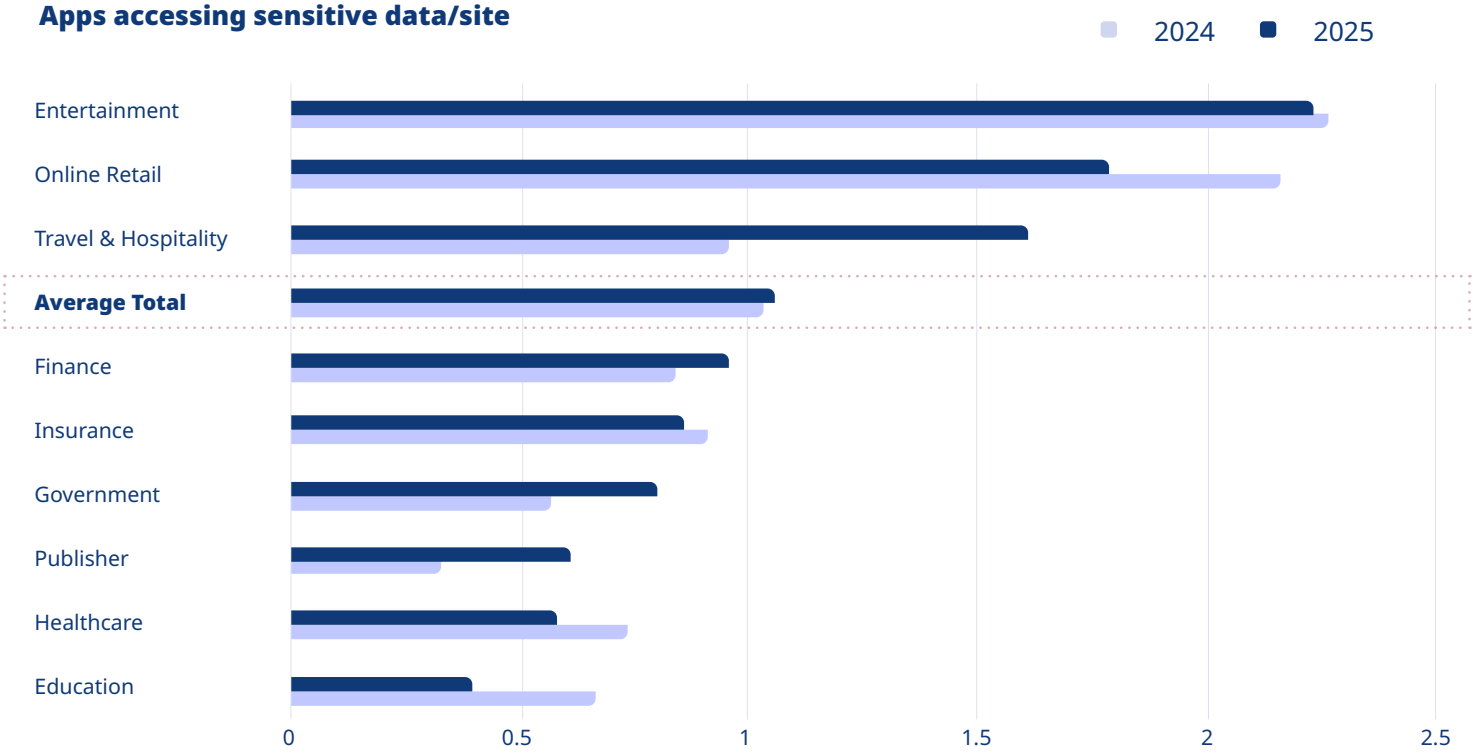
The frozen average conceals dangerous polarization. Leading sectors reduce payment risk while others triple exposure. Healthcare/Insurance complacency persists despite regulations. Organizations aren't converging toward best practices; they're fragmenting into leaders and laggards, with critical infrastructure (Government, Education) deteriorating fastest.

Risk Exposure Factors in Depth

Apps accessing sensitive data

Sensitive data includes credit card numbers, CVVs, social security numbers, and account credentials: information that enables identity theft, financial fraud, or account takeover. When third-party apps access these fields, they can exfiltrate data to external servers, store it insecurely, or become vectors for supply chain attacks like Magecart and web skimming. Organizations often grant sensitive data access without reviewing whether the third-party app legitimately needs it, creating compliance violations and expanding breach impact.

Apps accessing sensitive data/site



Publisher sites triple sensitive data access

Jumped from 0.25 to 0.75 apps per site, a 200% surge and the report's largest increase.

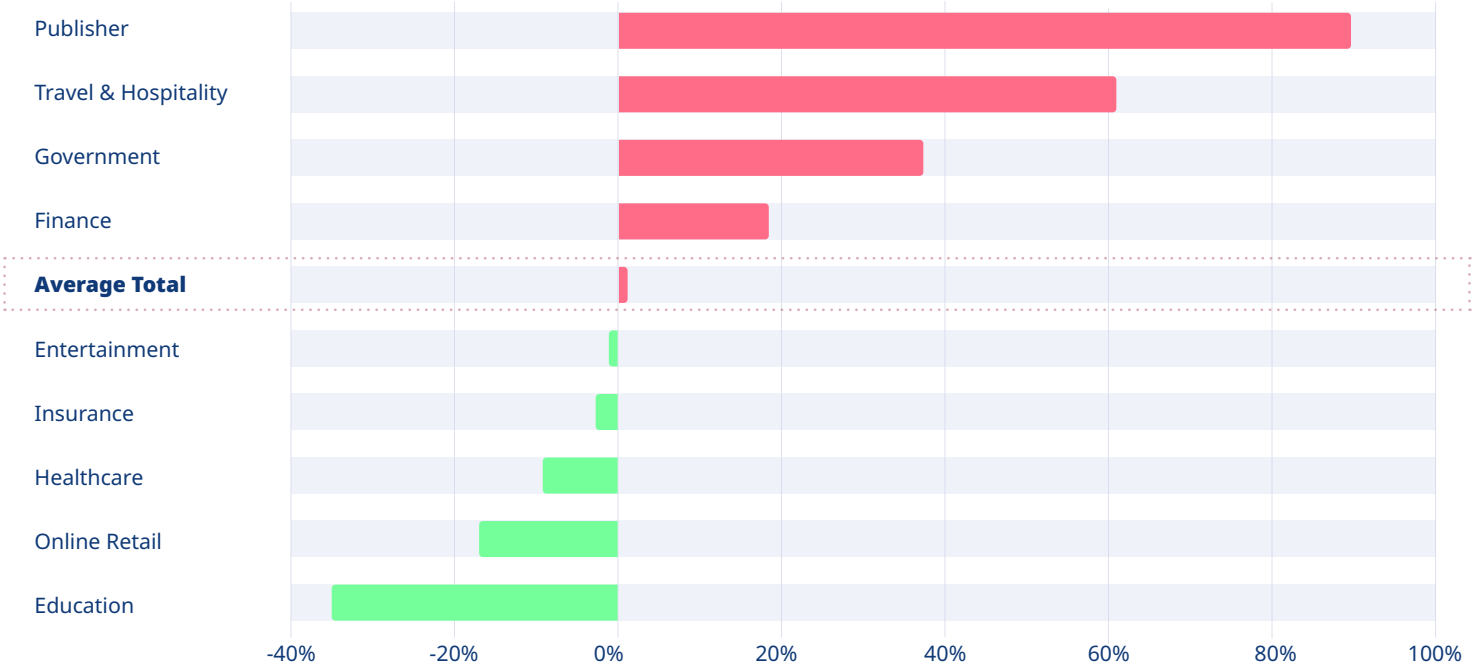
Travel & Hospitality soars 60%

Second-largest increase, driven by booking integrations and payment processing expansions.

Retail shows rare improvement

Dropped from ~2.0 to ~1.5 apps per site, a ~25% reduction despite maintaining highest absolute exposure levels.

Change in % from 2024 to 2025



SURVEY VALIDATION: Why Payment Frame Risk Persists

Only 8% of organizations deploy Client-Side protection on checkout pages. Meanwhile, 24% rely on "general security tools" inadequate for checkout protection. The tool mismatch explains why unjustified apps payment frame apps surged 30%.

Healthcare drops modestly

Declines slightly in sensitive data access despite HIPAA requirements, one of few sectors showing improvement.

Finance increases 22% despite regulation

Sensitive data apps rise from ~0.9 to ~1.1, suggesting fintech partnerships outpacing security controls.

What type of applications have access to sensitive data?

Justified Apps	2024	2025
Payments & Checkout Solutions	9%	16%
JS Frameworks & Libraries	16%	15%
Development Tools	4%	2%
Security Enforcements	19%	2%
Privacy & Compliance Tools	1%	1%
Total	**49%**	**36%**

Unjustified Apps	2024	2025
General Analytics	**20%**	**16%**
Tag Management Platforms	**10%**	**15%**
Social Media Analytics & Pixels	10%	10%
E-commerce platforms	**4%**	**10%**
Advertising Analytics	3%	5%
User Engagement Tools	2%	3%
Cloud Services	2%	3%
Marketing Automations	1%	1%
Total	**51%**	**64%**

Payment solutions nearly double their reach

jumped from 9% to 16% of justified sensitive data access, reflecting e-commerce expansion but also increased payment skimming risk.

Tag managers become top unjustified offenders

rose from 10% to 15%, now the second-largest category of apps improperly accessing sensitive input fields.

E-commerce platforms explode

150%

surged from 4% to 10% among unjustified apps, suggesting third-party marketplace integrations are over-collecting customer data.

64%

Unjustified access

rose from 51% in 2024, meaning nearly two-thirds of apps accessing sensitive data have no legitimate business need.

Unjustified apps that read sensitive data

App Type Accountability by Department:

Marketing	IT	Digital
General Analytics	Cloud Services	Advertising Analytics
Marketing Automations	User Engagement Tools	Social Media Analytics & Pixels
Media Management & Players	E-commerce platforms	
Tag Management Platforms		

IT department exposure doubles

8% → **16%**

2024 2025

unjustified sensitive data access by IT-managed apps surged from 8% to 16%, now accounting for 1 in 6 violations.

Marketing/Digital remains dominant offender

44% → **48%**

2024 2025

rose slightly from 44% to 48%, responsible for nearly half of all unjustified sensitive data access.

Cloud services and e-commerce platforms lead IT violations

both fall under IT responsibility, suggesting infrastructure and platform integrations are over-permissioned for sensitive data.

App name	App type	
Google Tag Manager	Tag Management Platforms	8%
Shopify	E-commerce platforms	5%
Facebook Pixel	Social Media Analytics & Pixels	4%
Microsoft Clarity	General Analytics	3%
Tiktok Pixel	Social Media Analytics & Pixels	1%
Contentsquare	General Analytics	1%
Quantum Metric	General Analytics	1%
Demandware Salesforce	E-commerce platforms	1%
Pinterest Tag	Advertising Analytics	1%
FullStory	General Analytics	1%
Adobe Dynamic Tag Management	Tag Management Platforms	1%

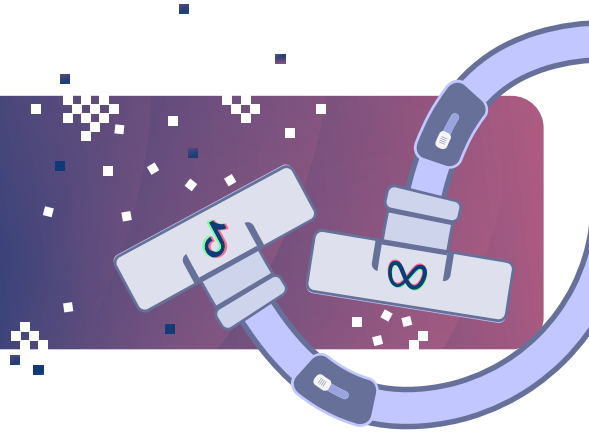
Google Tag Manager dominates violations
accounts for 8% of all unjustified sensitive data access, the single worst offender by far.

E-commerce platforms over-collect aggressively
Shopify (5%) and Demandware Salesforce (1%) combined represent 6% of violations, suggesting checkout integrations exceed necessary permissions.

Amazon CloudFront	Cloud Services	1%
Dynatrace	General Analytics	1%
Google Maps	User Engagement Tools	0.4%

Social media pixels read sensitive fields

Facebook Pixel (4%) and TikTok Pixel (1%) collect data from input fields with no legitimate tracking need, creating privacy and compliance risks.



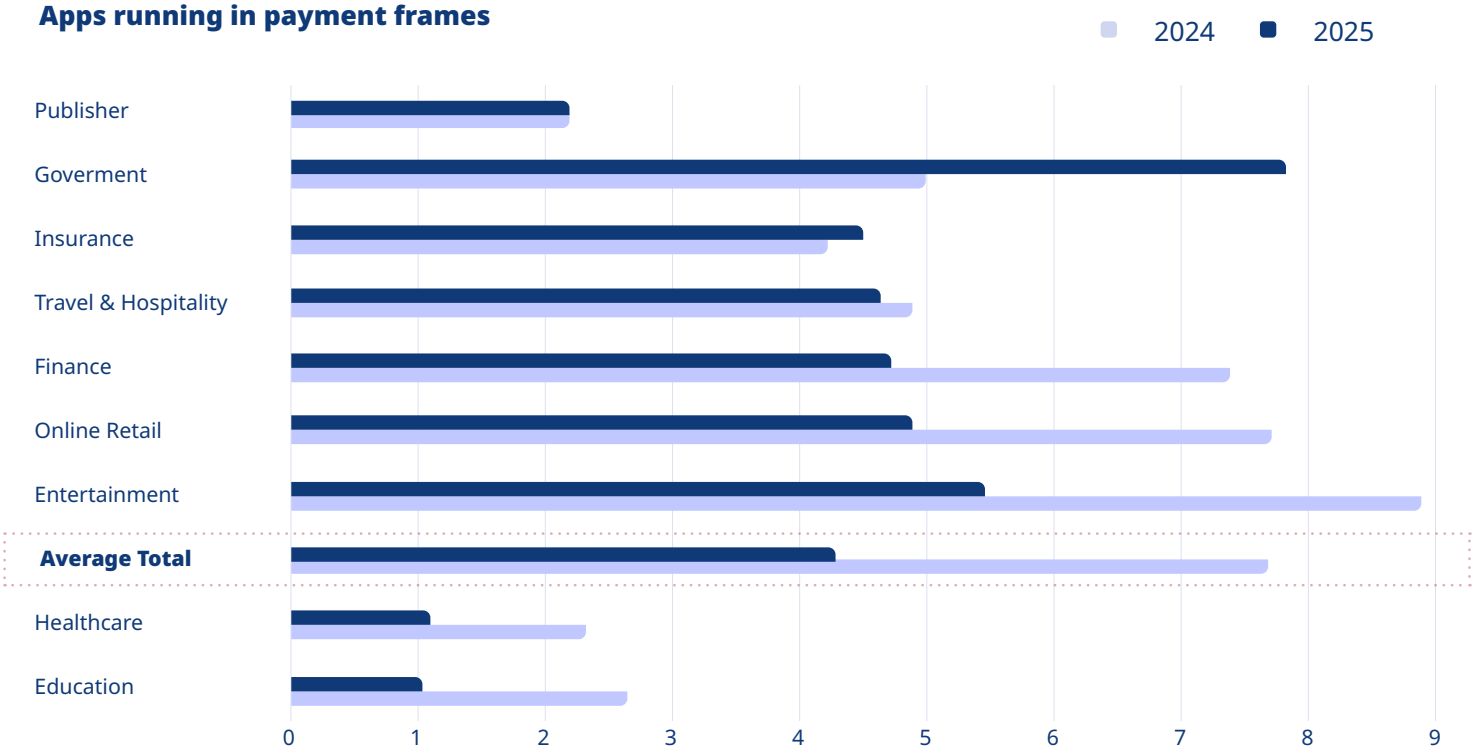
Apps running in payment page frames

[iFrames]

What are Payment Frames and Why Do They Matter?

Payment frames (iframes) are isolated sections of checkout pages where customers enter credit card detail, creating the highest-value target for attackers. Third-party scripts running inside or alongside these frames can intercept payment data in real-time, enabling Magecart-style "digital skimming" attacks that have compromised major retailers including British Airways, Ticketmaster, and Newegg. PCI DSS 4.0 specifically requires organizations to inventory and justify every script with access to payment frames, making unjustified apps a direct compliance failure.

Apps running in payment frames



Overall average drops nearly 40%

fell from ~7.5 to ~4.5 apps in payment frames, showing organizations are finally addressing third-party checkout security.

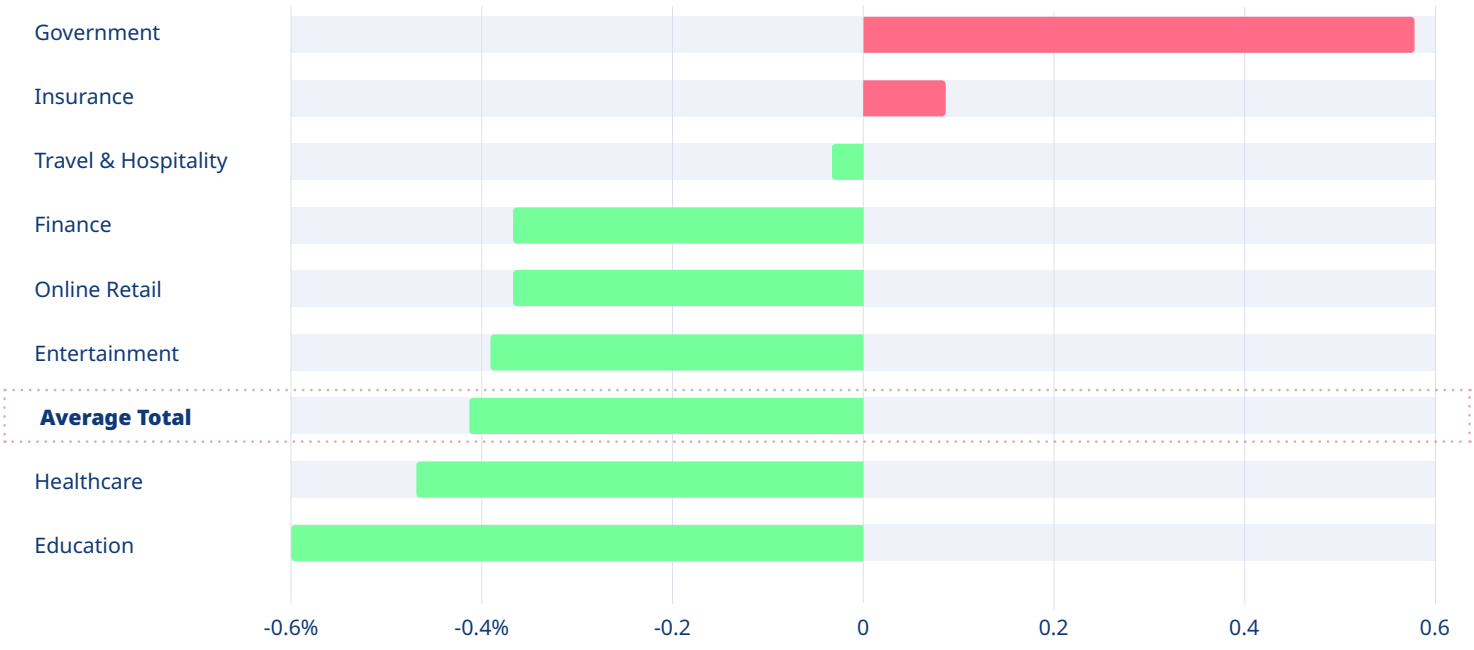
Retail shows meaningful cleanup progress

Online Retail dropped from ~7 to ~5 apps in payment frames (~29% reduction), demonstrating that e-commerce sites are actively addressing checkout security despite high transaction volumes and complex integrations.

Government payment frame exposure surges dramatically

jumped from ~5 to ~8.5 apps per site (70% increase), creating massive skimming vulnerability on public service portals and now representing by far the worst security posture across all sectors.

Change from 2024 to 2025



Retail cleanup mirrors broader sector improvements

Finance (7-5 apps) and Entertainment (9-6 apps) show similar reduction patterns to Retail, indicating coordinated industry response to payment skimming threats, likely driven by PCI DSS 4.0 requirements.

Healthcare and Education set the security standard

both maintain under 2 apps per payment frame, showing Retail still has significant room for improvement despite recent progress. Retail's 5 apps represents 2.5x the best-practice benchmark.

What type of applications are running in payment frames?

Justified Apps	2024	2025
Payments & Checkout Solutions	16%	18%
JS Frameworks & Libraries	12%	12%
User Engagement Tools	6%	8%
Development Tools	7%	5%
Privacy & Compliance Tools	5%	4%
Security Enforcements	6%	3%
Cloude services	1%	3%
Total	**64%**	**53%**

Unjustified Apps	2024	2025
Advertising Analytics	10%	13%
General Analytics	**15%**	**11%**
Tag Management Platforms	9%	9%
E-commerce platforms	**2%**	**7%**
Social Media Analytics & Pixels	5%	4%
Marketing Automations	3%	2%
Design Resources	0%	1%
Media Management & Players	1%	0.4%
Total	**36%**	**47%**

Justified apps decline

17%

Dropped from 64% to 53%, indicating organizations are removing legitimate payment scripts from checkout pages.

Advertising analytics grow at checkout

increased from 10% to 13% unjustified, showing marketers are placing tracking scripts directly in payment environments despite compliance risks.

E-commerce platforms invade payment frames

250%

Unjustified presence exploded from 2% to 7% (250% increase), highest growth among all unjustified categories.

30%

Unjustified apps surge

Rose from 36% to 47%, meaning nearly half of all apps running in payment frames now have no business reason to be there.

App name	App type	
Google Tag Manager	Tag Management Platforms	5%
Shopify	E-commerce platforms	5%
Google Analytics	General Analytics	2%
Facebook Pixel	Social Media Analytics & Pixels	2%
Microsoft Clarity	General Analytics	2%
DoubleClick for Publishers (DFP)	Advertising Analytics	2%
Microsoft Advertising UET	Advertising Analytics	2%
Google Maps	User Engagement Tools	1%
Tiktok Pixel	Social Media Analytics & Pixels	1%
Contentsquare	General Analytics	1%
The Trade Desk	Advertising Analytics	1%
Hotjar Modules Script	User Engagement Tools	1%
Tealium	Tag Management Platforms	1%

Google Tag Manager and Shopify tie for worst offenders each accounts for 5% of unjustified payment frame presence, creating major skimming and compliance risks.

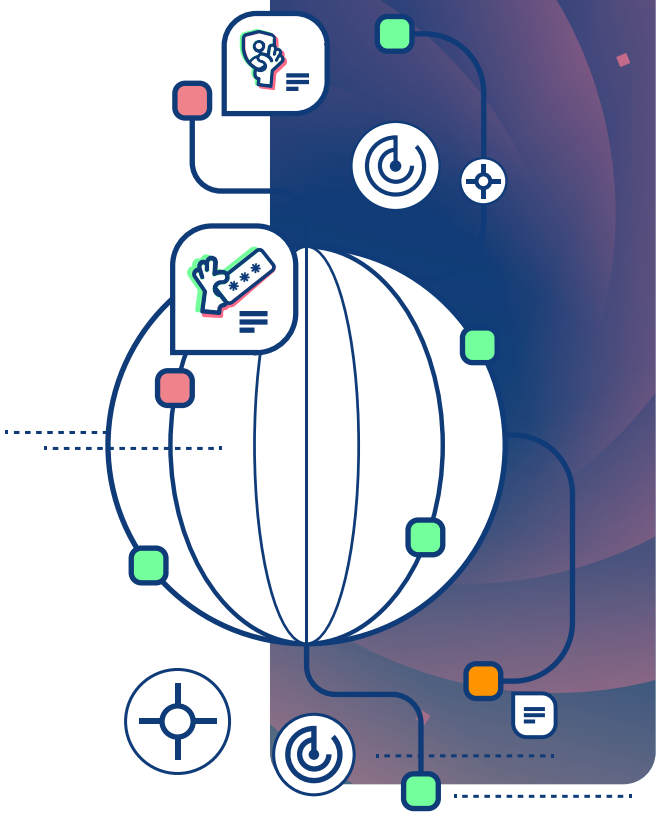
Social media pixels infiltrate checkout pages Facebook Pixel (2%) and TikTok Pixel (1%) run in payment frames with no legitimate purpose, tracking payment behavior for ad targeting.

Apps loaded from public CDNs

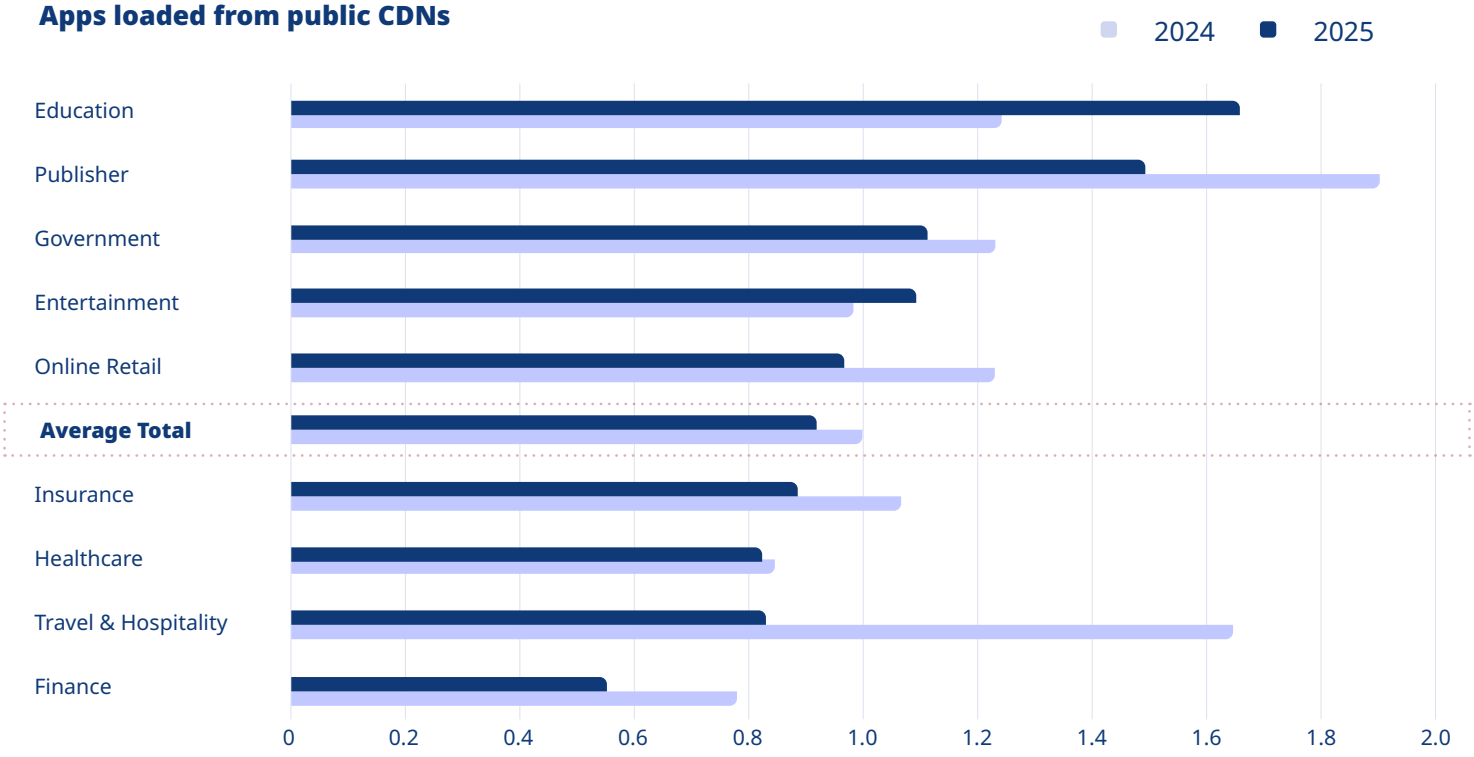
What are Public CDNs and Why Do They Amplify Risk?

Public Content Delivery Networks (CDNs) like Cloudflare, jsDelivr, and Unpkg host JavaScript libraries that multiple websites load, creating shared infrastructure dependencies. When attackers compromise a public CDN or poison cached libraries, they can inject malicious code that executes across thousands of websites simultaneously, as demonstrated in the 2024 Polyfill io supply chain attack that impacted 100,000+ sites.

Organizations loading content from public CDNs lose control over code updates, have no validation mechanisms for script integrity, and create single points of failure that attackers actively target.



Apps loaded from public CDNs



Education CDN dependency surges 35%

Massive increase from ~1.2 to ~1.6 apps per site, expanding supply chain attack surface in already vulnerable sector.

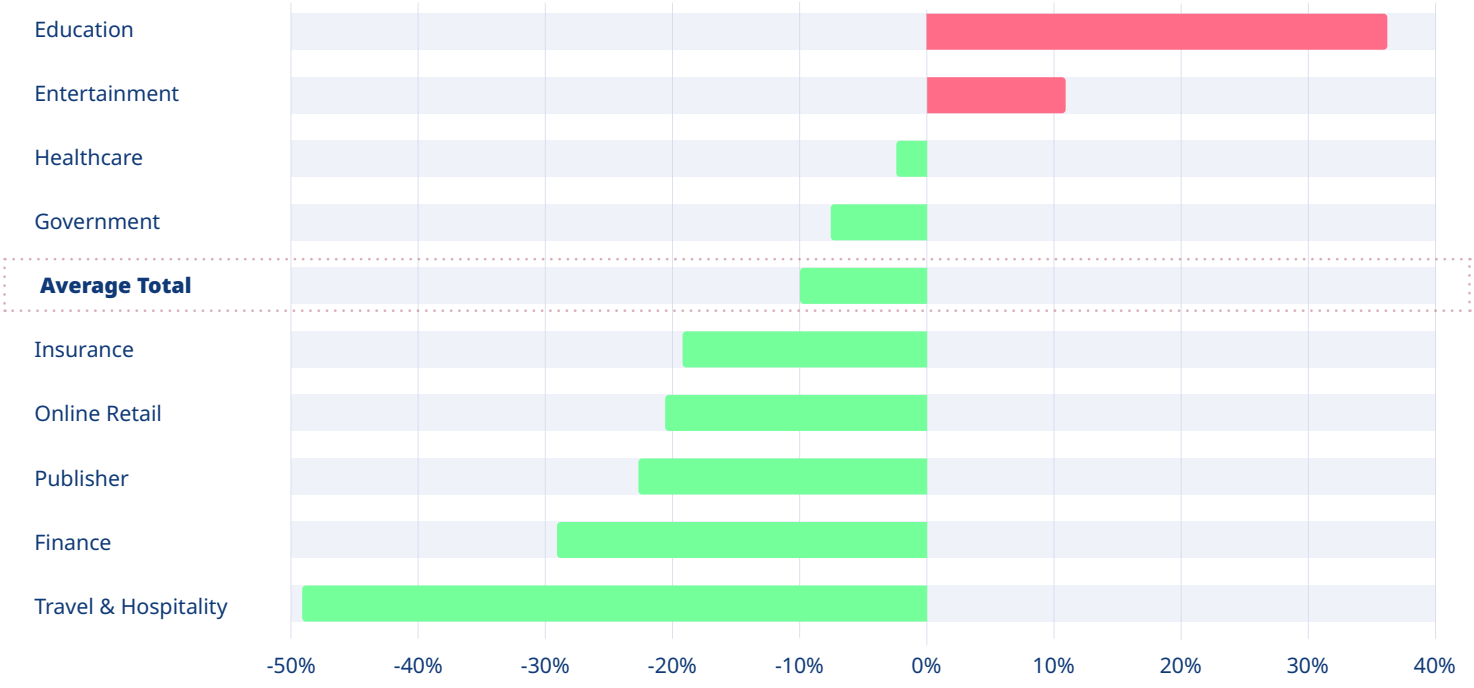
Publisher CDN usage explodes

Jumped approximately 50% from ~1.3 to ~2.0 apps, highest absolute exposure as ad tech and content delivery multiply dependencies.

Travel & Hospitality CDN reliance plummets 50%

Dropped from ~1.7 to ~0.8 apps, most dramatic reduction suggesting aggressive migration to private infrastructure.

Change in % from 2024 to 2025



Finance cuts CDN exposure by 30%

Fell from ~0.7 to ~0.5 apps, showing financial institutions are reducing third-party dependencies for compliance and security.

Most sectors reduce public CDN risk

7 out of 9 industries decreased usage year-over-year, but Education and Entertainment buck the trend with significant increases.

Unjustified Public CDN Exposure Analysis

Exposure by Category	2024	2025
Development Tools	20%	37%
Cloud Services	39%	28%
JS Frameworks & Libraries	28%	25%
User Engagement Tools	5%	
All other categories	11%	10%

Development tools surged to 37%

Unjustified use of dev tools surged to 37%, showing a dangerous trend of testing code moving to public infrastructure.

Unjustified cloud service exposure dropped to 28%, though it remains a top-three risk category.

Top Exposure Sources (CDNs)	2024	2025
Amazon CloudFront	15%	15%
CDNJS	12%	11%
Unpkg	11%	10%
Jsdelivr.net	11%	9%
jQuery	8%	8%
Bootstrap	4%	5%
SlickJS	3%	3%
Cloudfront.net	2%	3%
All the rest	30%	36%

Amazon CloudFront maintains top position

15%

Steady at 15% of all CDN cases year-over-year, remaining the single most-used public CDN provider.

JS delivery CDNs grow market share

CDNJS (12%), Unpkg (11%), and Jsdelivr.net (11%) collectively represent 34% of cases, up from 30% in 2024.

Long tail consolidates slightly

"All the rest" category dropped from 36% to 30%, indicating concentration toward major CDN providers as organizations standardize dependencies.

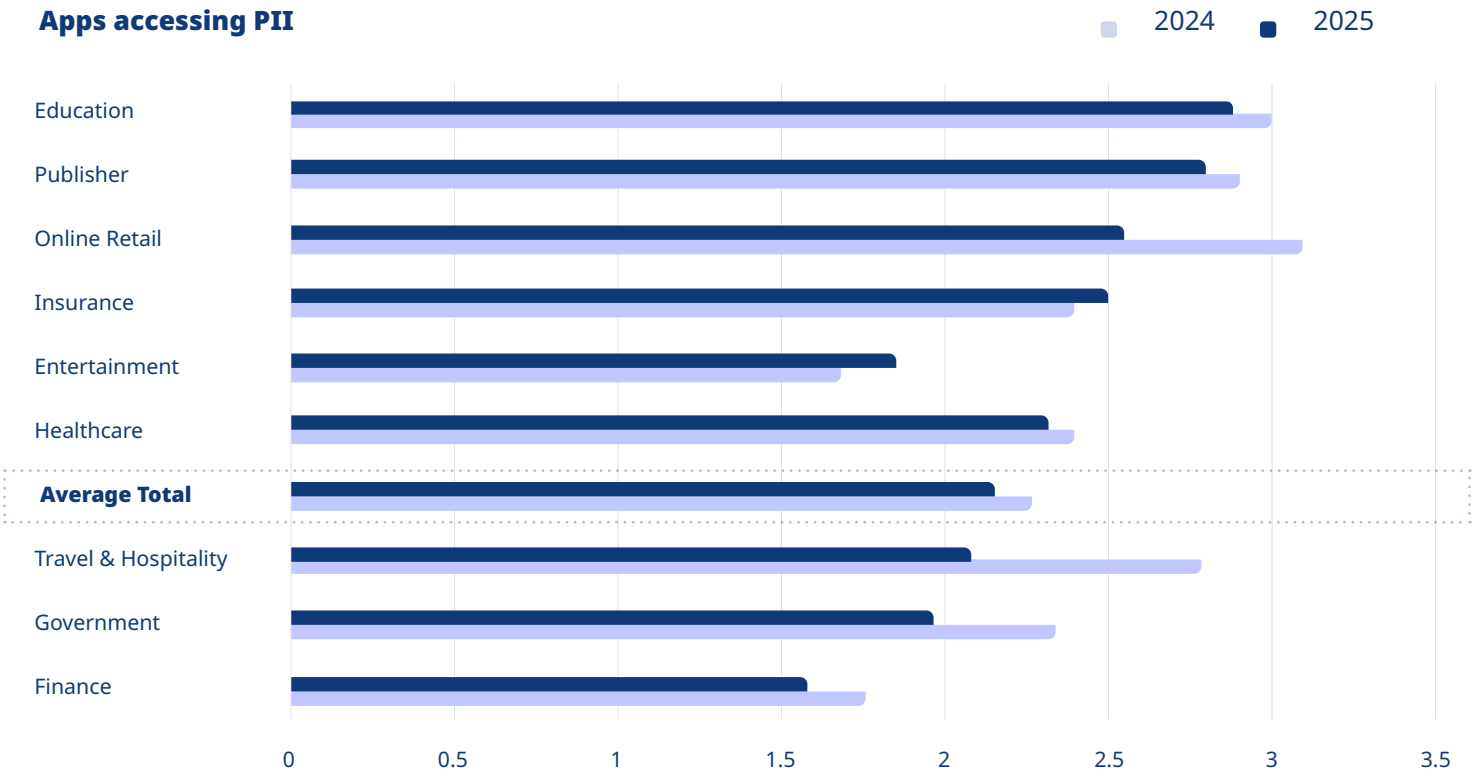
Apps accessing Personal Information

[PII]

What is PII and Why is Unauthorized Access Dangerous?

Personally Identifiable Information (PII) includes names, email addresses, phone numbers, physical addresses, and IP addresses, data that can identify specific individuals and falls under GDPR, CCPA, and other privacy regulations. When third-party apps access PII without legitimate business need, organizations face regulatory fines (up to 4% of global revenue under GDPR), must notify affected users in breach scenarios, and expand their attack surface for phishing and social engineering attacks. Unlike sensitive financial data, PII violations often go undetected until regulators audit data flows or breaches occur.

Apps accessing PII



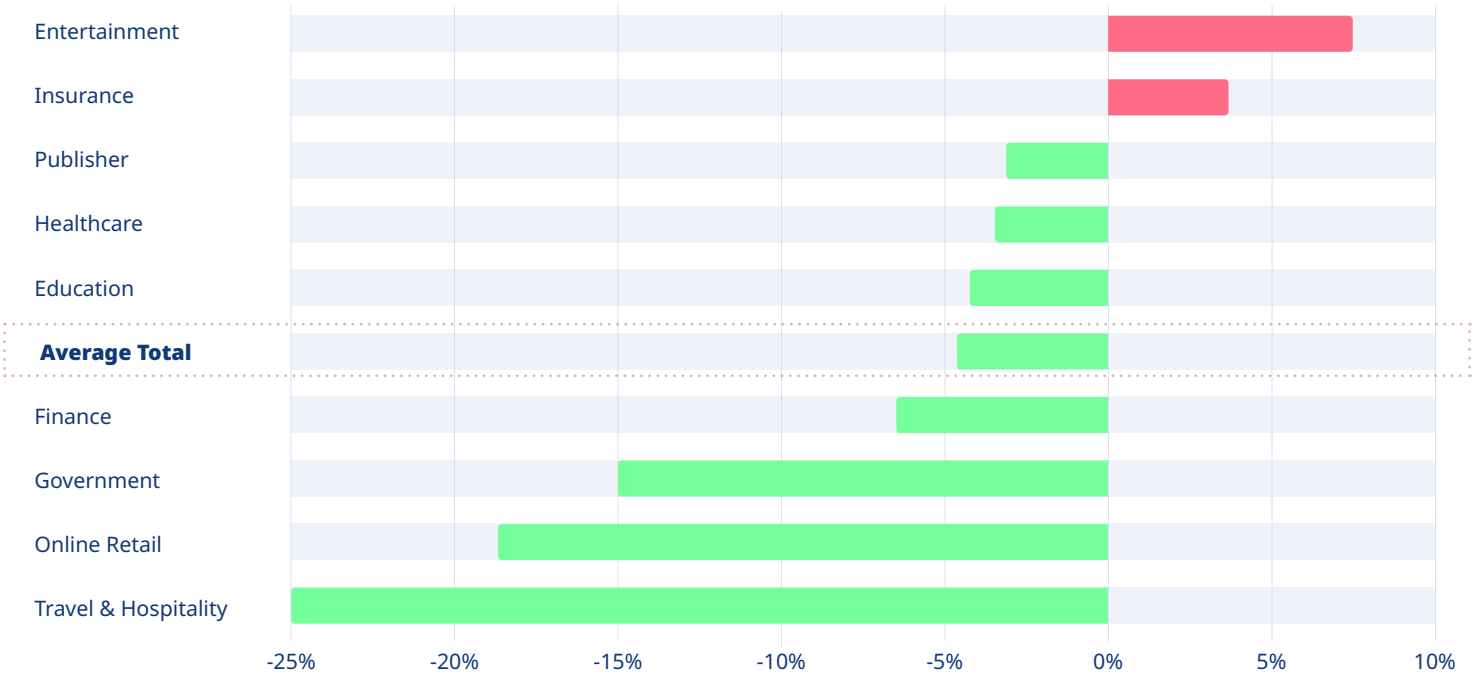
Online Retail cuts PII access by 17%

dropped from ~3.2 to ~2.7 apps per site, largest reduction among major sectors as e-commerce tightens data collection.

Travel & Hospitality slashes PII exposure 25%

fell from ~3.0 to ~2.2 apps, most aggressive cleanup despite handling sensitive booking and payment information.

Change in % from 2024 to 2025



Healthcare shows minimal improvement

declined just 4% from ~2.6 to ~2.5 apps, disappointing progress for a HIPAA-regulated sector handling protected health information.

Finance reduces PII access 5%

dropped from ~1.9 to ~1.8 apps, maintaining lowest absolute exposure but slow pace of improvement for highly regulated industry.

What Types of Applications Accessing Personal Data?

Justified Apps	2024	2025
JS Frameworks & Libraries	22%	18%
Privacy & Compliance Tools	10%	9%
Cloud Services	1%	8%
Development Tools	6%	2%
Payments & Checkout Solutions	11%	2%
Security Enforcements	15%	1%
Total	**65%**	**40%**

Payment solutions cut PII access

82%

Plunged from 11% to just 2% justified access, most dramatic reduction as checkout flows become more privacy-conscious.

Justified PII access plummets

38%

Dropped from 65% to 40%, showing organizations are aggressively removing legitimate apps that read personal data.

Pay Attention	2024	2025
General Analytics	15%	13%
Social Media Analytics & Pixels	4%	7%
Total	**19%**	**20%**

Unjustified Apps	2024	2025
Tag Management Platforms	11%	15%
User Engagement Tools	6%	12%
Advertising Analytics	7%	6%
Marketing Automations	2%	4%
Media Management & Players	1%	1%
E-commerce platforms	1%	1%
Total	**28%**	**40%**

Tag managers dominate unjustified PII collection

Jumped from 11% to 15%, becoming the largest category of apps improperly reading personal information.

User engagement tools double unjustified access

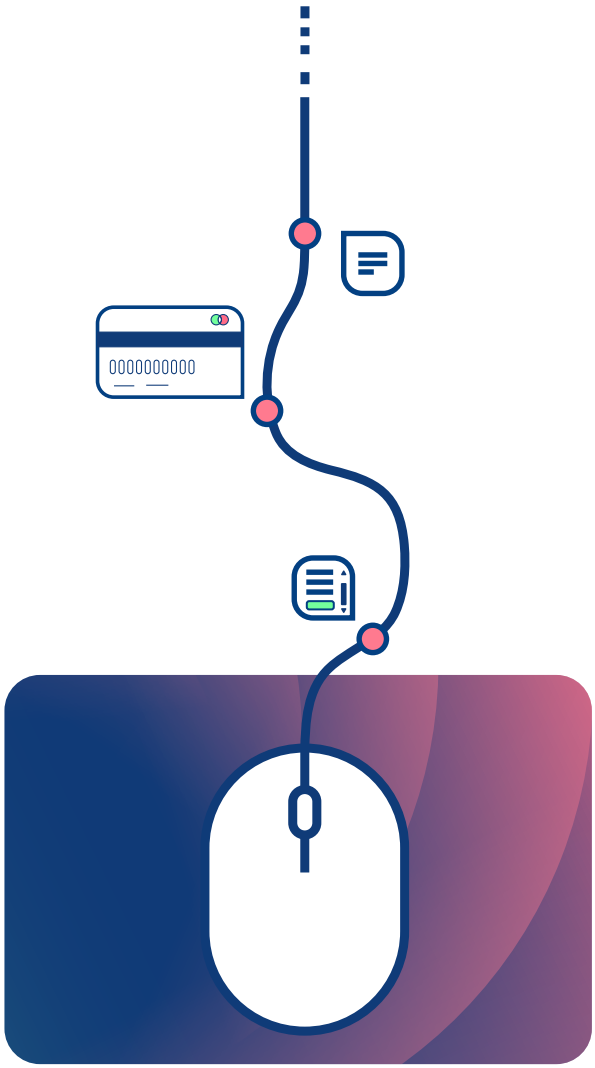
Exploded from 6% to 12%, showing chat widgets and feedback tools are over-collecting customer data.

Unjustified access surges

43%

Rose from 28% to 40%, meaning unjustified and justified PII access are now equal at 40% each, a dangerous compliance shift.

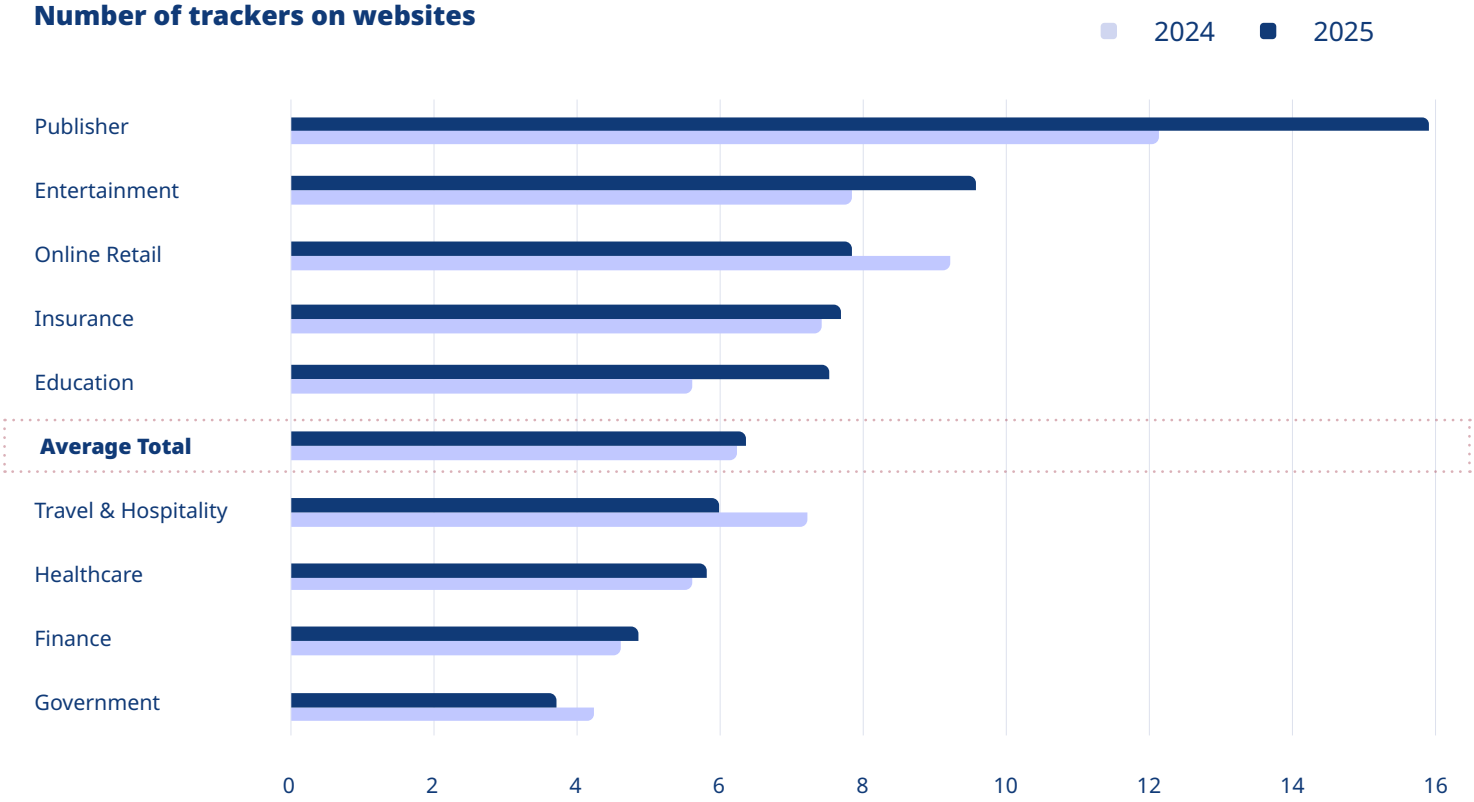
Online Tracking Technologies



What are Trackers and What Risks Do They Create?

Trackers are scripts that monitor user behavior, collect analytics, enable advertising targeting, and measure conversio, typically from vendors like Google Analytics, Facebook Pixel, or TikTok Pixel. Each tracker loads additional third-party code, expands attack surface, can access DOM content (including sensitive fields if misconfigured), and creates privacy compliance obligations under GDPR's consent requirements and evolving cookie regulations. Tracker proliferation is especially dangerous because marketing teams often add them without security review, and abandoned trackers continue running indefinitely, becoming orphaned attack vectors.

Number of trackers on websites



Education tracker explosion

Surged 30% year-over-year to ~6.5 trackers per site, most aggressive increase among all sectors.

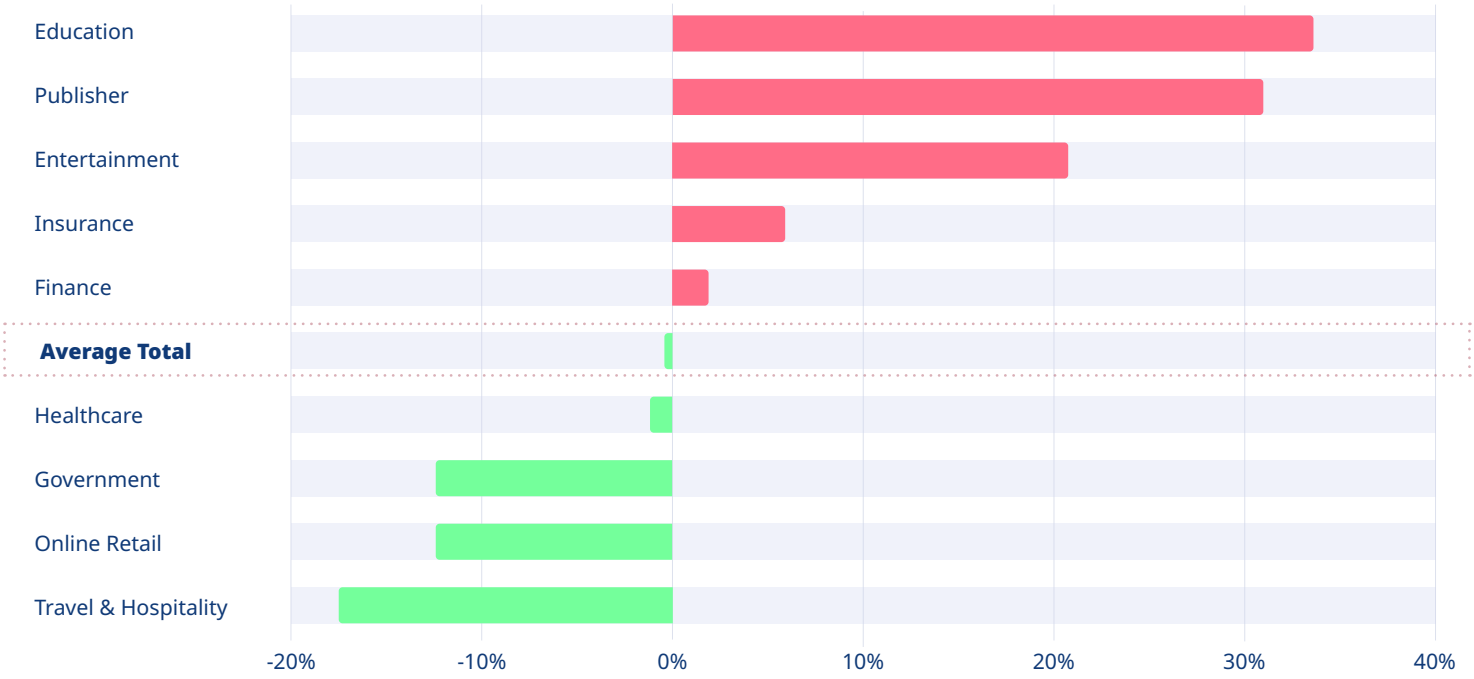
Publisher sites remain tracker heavens

Jumped 33% to ~16 trackers per site, maintaining highest absolute exposure driven by aggressive ad monetization.

Entertainment trackers up 25%

Rose from ~8 to ~10 trackers per site as streaming platforms intensify audience measurement and retargeting.

Change in % from 2024 to 2025



Travel & Hospitality cuts trackers 21%

Dropped from ~7 to ~5.5 per site, largest reduction showing booking platforms are deprioritizing third-party analytics.

Online Retail reduces tracker load 11%

Fell from ~9 to ~8 trackers, balancing conversion optimization with privacy concerns as regulations tighten.

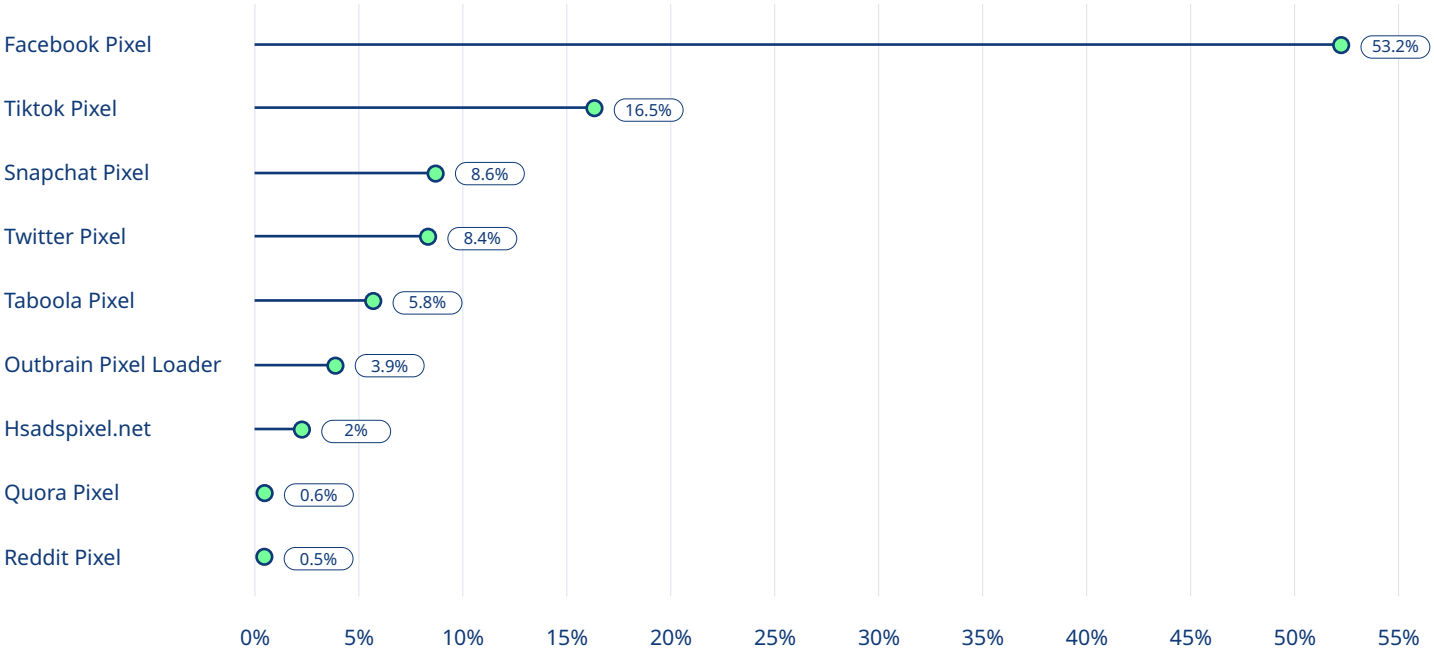
Healthcare shows zero improvement

Remained flat at ~6 trackers, disappointing stagnation for a HIPAA-regulated sector that should prioritize patient privacy.

Finance cuts trackers modestly

Fell 4% from ~5.5 to ~5.3 per site, slowest improvement among financial services despite regulatory pressure and data protection obligations.

Marketing Pixels Trackers Popuarity Rate



Popuarity Rate Among All Trackers

6.3%	Google Tag Manager	1.07%	Google Analytics
5.7%	Facebook Pixel	0.9%	Snapchat Pixel
2.5%	YouTube IFrame	0.9%	Twitter Pixel
1.8%	Tiktok Pixel	0.6%	Taboola Pixel
1.75%	Linkedin Insight Tag	0.4%	Outbrain Pixel Loader
1.54%	OneTrust	0.2%	Hsadspixel.net
1.22%	Clarity.tags	0.1%	Quora Pixel
1.13%	Adobe Dynamic Tag Management	0.1%	Reddit Pixel
1.12%	Pinterest Tag		

Most Popular Trackers

#1: Facebook Pixel

53%

market share

dominates the market. Appears on more than half of all sites using social media pixels, cementing Meta's tracking dominance.

TikTok Pixel second at

16.5%

rapidly growing presence makes it the clear #2 social pixel, though still capturing only 1.8% of total tracker market.

Google Tag Manager leads non-pixel trackers

6.34%

6.34% adoption makes it the most widely deployed tag management platform, appearing on 1 in 16 sites.

5.7%

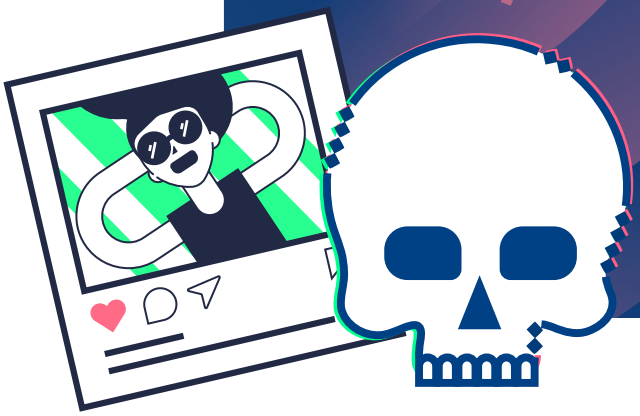
of all trackers are social media pixels. despite high visibility, pixels are a small fraction of total tracking ecosystem compared to analytics and ad tech.

Long tail fragmentation persists top 8 pixels combined represent only

10.8%

of total popularity, showing tracker ecosystem remains highly diverse beyond major platforms.

Risk Origins



Marketing is the primary driver of third-party exposure. Responsible for:

26%

of all third-party app risk. This includes User Engagement Tools (7.80%), Tag Management (6.98%), General Analytics (6.29%), Media Management (2.51%), and Marketing Automations (2.10%). It represents the highest risk footprint of any single department.

Digital/Performance Marketing follows at

17%

Advertising Analytics (12.75%) and Social Media Pixels (4.48%) combined create a significant tracking-based attack surface, specifically tied to campaign execution.

43%

of Third-Party Risk: Marketing and Digital Applications

Together, they deploy more than twice as many third-party components as IT (19.38%). This confirms that the primary source of web exposure originates from customer-facing engagement and tracking tools, rather than core infrastructure or security applications.

19%

Makes IT manages the second-largest footprint

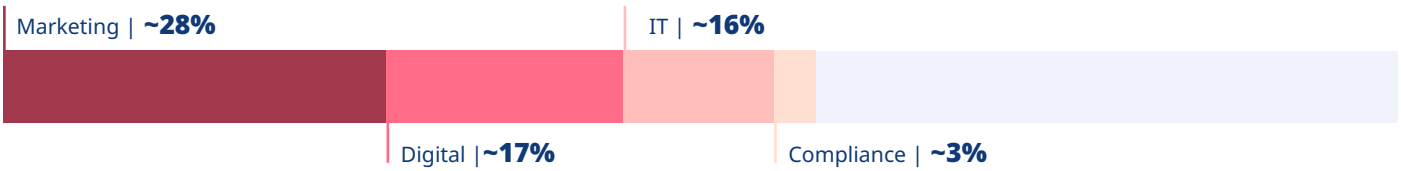
This includes JS Frameworks (4.84%), Cloud Services (4.36%), Payments (4.22%), Development Tools (2.63%), E-commerce platforms (1.60%), Security (1.51%), and Design Resources (0.22%). This highlights significant infrastructure and payment-related complexity.

3%

Compliance has the smallest departmental footprint

Consisting solely of Privacy & Compliance Tools, this remains the smallest footprint despite the high regulatory stakes involved.

Standard Pages



Marketing | ~28%

9.3%	User Engagement Tools
6.4%	Tag Management Platforms
6.0%	General Analytics
3.7%	Media Management & Players
2.4%	Marketing Automations

IT | ~16%

5%	Cloud Services
4.6%	JS Frameworks & Libraries
3.2%	Development Tools
1.3%	Payments & Checkout Solutions
1.3%	Security Enforcements
0.4%	E-commerce Platforms
0.3%	Design Resources

Digital | ~17%

14%	Advertising Analytics
3.4%	Social Media Analytics & Pixels

Compliance | ~3%

3.3%	Privacy & Compliance Tools

Sensitive Pages

Marketing | ~32%

12.5%	Media Management & Players
8.2%	Tag Management Platforms
6.3%	General Analytics
5%	User Engagement Tools
0.2%	Marketing Automations

IT | ~28%

11%	Payments & Checkout Solutions
5.4%	JS Frameworks & Libraries
4.7%	E-commerce Platforms
2.3%	Cloud Services
1.8%	Security Enforcements
1.7%	Development Tools
0.2%	Design Resources

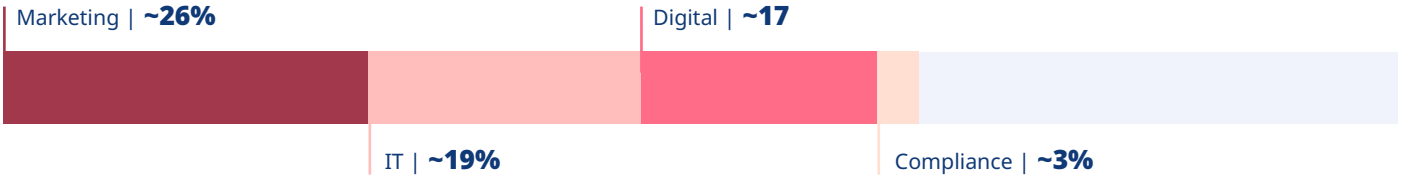
Digital | ~16%

9%	Advertising Analytics
7%	Social Media Analytics & Pixels

Compliance | ~3%

2.6%	Privacy & Compliance Tools

Total



Marketing | ~26%

8%	User Engagement Tools
7%	Tag Management Platforms
6.3%	General Analytics
2.5%	Media Management & Players
2.1%	Marketing Automations

IT | ~19%

4.8%	JS Frameworks & Libraries
4.4%	Cloud Services
4.2%	Payments & Checkout Solutions
2.7%	Development Tools
1.5%	E-commerce Platforms
1.6%	Security Enforcements
0.2%	Design Resources

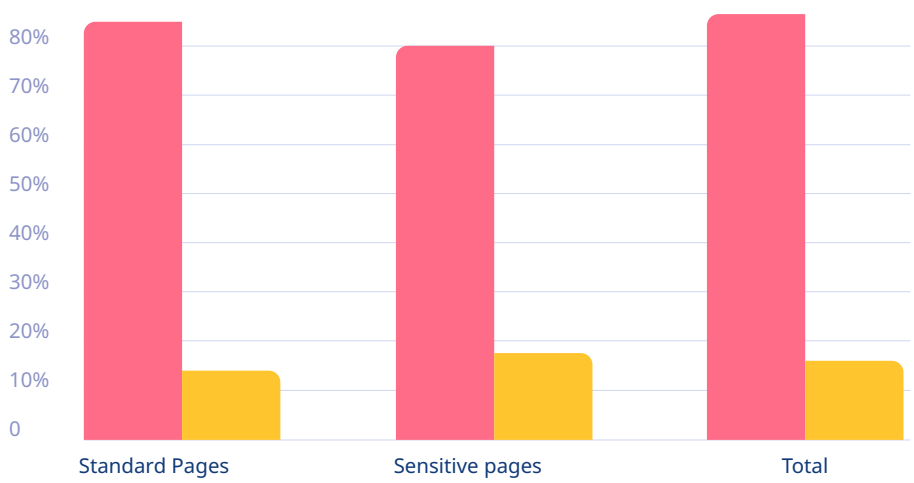
Digital | ~17%

12.8%	Advertising Analytics
4.5%	Social Media Analytics & Pixels

Compliance | ~3%

3%	Privacy & Compliance Tools

1st Party vs 3rd Party



Web Exposure Management's Best Practices

The 8 Security Benchmarks: Leaders vs. Average Organizations

		Leaders	Average
1	Third-party apps (total)	≤8 apps	15-25 apps
2	Payment frame apps	≤2 apps	5-8 apps
3	External domain connections	≤18 domains	30-50 domains
4	Tracking scripts	≤3 trackers	8-16 trackers
5	Justified sensitive data access	100%	40-60%
6	Justified PII access	100%	80-95%
7	Apps accessing PII	≤1 app	2-4 apps
8	Justified payment frame apps	100%	40-60%

Based on analysis of 429 leading websites

77%

of organizations achieve 4-5 benchmarks

0.2%

achieves all 8
(only 1 site: ticketweb.uk)

2 → 3x

higher third-party volume than leading standards is seen across most organizations.

18% → 47%

achievement rates show that justification controls have the widest gaps.

Limit Third-Party Dependencies

Third-party applications can add value, but each one should be carefully evaluated. Use only those that are genuinely necessary.

Examples:

77.2%

kept their third-party apps to eight or fewer.

This shows that meaningful reduction is achievable

Top performers such as **ticketweb.uk** (meeting all eight security benchmarks), **GitHub**, **PayPal**, and **yale.edu** demonstrate that even complex platforms can operate with a minimal third-party footprint.

Restrict Third-Party Apps on Sensitive Pages

Avoid loading third-party applications on login pages, payment pages, or their associated iframes unless absolutely required.

Examples:

21.0%

of leading sites met the benchmark of two or fewer apps in payment frames

18.2%

ensured that all payment-frame apps were fully justified

Organizations like Aaautostores.com and major e-commerce platforms show that secure checkout flows do not require extensive third-party integrations. Secure transactions can be handled with minimal external dependencies.

Minimize External Domain Connections

Limit connections to external domains to reduce attack surface and supply chain vulnerabilities.

Examples:

82.3%

of leading sites maintained 18 or fewer external domain connections.

Companies across retail (**lidl.de**, **c-and-a.com**), finance (**investor.nvidia.com**), logistics (**dhl.com**), and media (**zdf.de**, **xnxx**) demonstrate that a robust web presence does not require a sprawling third-party ecosystem.

Even hospitality sites like marriottvacationclub.com achieve strong security while maintaining full booking functionality.

Implement Strict Tracker Discipline

Online tracking technologies require careful attention, as they are easily misconfigured. Regularly verify that trackers only access the data they are explicitly authorized to access.

Examples:

77.2%

of leading sites achieved three or fewer trackers, a critical benchmark for privacy and security.

Organizations across consumer goods (**kimberly-clark.com**), hospitality (**marriottvacationclub.com**), and international education prove that three trackers are sufficient for comprehensive analytics.

Publisher sites averaging 16 trackers demonstrate how monetization pressure drives unnecessary risk accumulation.

Enforce Data Access Justification

Ensure that only necessary applications access sensitive data and personally identifiable information (PII).

Examples:

46.9%

of leading sites ensured that all sensitive data access was justified

92.8%

achieved this standard for PII

66.7%

limited PII access to a single application at most

Organizations demonstrating data-minimization excellence span technology platforms, financial services, and educational institutions. These examples prove that restricting data access does not compromise core business functions. Unjustified data access creates compliance risk and expands breach impact - eliminate it systematically.

Avoid Recently Registered Domains

Be cautious with recently registered domains (less than six months old), as they may indicate potential malicious activity.

3.8x

more frequent on compromised sites.

Recently registered domains (less than six months old) appear **15% vs 4%** on compromised sites, according to 2025 research, making them the strongest single predictor of malicious activity. Be wary of these domains and conduct thorough investigations whenever they are encountered.

Minimize Public CDN Usage

2.2x

more public CDN content on compromised sites.

Compromised sites load **2.2× more content from public CDNs** than clean sites, according to 2025 research, confirming supply-chain risk through shared infrastructure. Minimize the use of public CDNs and, whenever possible, host required resources behind your firewall to reduce attack vectors.

Foster Cross-Functional Collaboration

43%

of third-party risk comes from Marketing and Digital.

The 2025 research shows that **Marketing and Digital teams account for 43% of third-party risk**, more than double IT's footprint. Strong collaboration between marketing, IT, and security reduces misconfigurations and unsafe practices. A secure and effective website is a shared responsibility, requiring unified governance frameworks with technical enforcement.

Dramatic year-over-year shifts require continuous monitoring.

The 2025 research demonstrates that exposure and the threat landscape are constantly evolving. Static security reviews cannot detect these rapid changes - real-time continuous monitoring systems are essential.

2% → 12.9%

Government malicious activity exploded

14.3% (X4)

Education infections quadrupled

51% → 64%

Unjustified sensitive data access surged

Strong Performers

Meeting 5-6 Benchmarks

Website	Industry	Third-Party Apps	Payment Frame Apps	Trackers	External Domains	Overall Grade
Lidl.de	Retail	8-12	2-3	≤3	18-25	B+
C-and-A.com	Retail	8-12	2-3	≤3	18-25	B+
DHL.com	Logistics	8-12	2-3	3-5	18-25	B+
ZDF.de	Media	10-15	2-3	3-5	20-28	B+
Investor.nvidia.com	Finance	8-12	≤2	≤3	18-25	B+
MarriottVacationClub.com	Travel	10-15	2-3	3-5	20-30	B+
Kimberly-Clark.com	Consumer Goods	8-12	2-3	≤3	18-25	B+
Aaautostores.com	E-commerce	8-12	≤2	≤3	18-25	B+

Elite Security Leaders

Meeting 7-8 Benchmarks

Website	Industry	Third-Party Apps	Payment Frame Apps	Trackers	External Domains	Overall Grade
ticketweb.uk	Entertainment	≤8	≤2	≤3	≤18	A+
GitHub.com	Technology	≤8	≤2	≤3	≤18	A
PayPal.com	Finance	≤8	≤2	≤3	≤18	A
Yale.edu	Education	≤8	≤2	≤3	≤18	A

Conclusion:

Navigating the Web Exposure Crisis

The 2025 web security landscape demands urgent action. Organizations face a critical choice: implement systematic governance over third-party dependencies, or accept exponentially growing risk as unjustified data access becomes the norm.

51% → 64%

Unjustified sensitive data access surged.

60%

increase: Government payment frame exposure jumped from 5 to 8 apps per site.

14.3% (X4)

Education malicious activity quadrupled.

Zero improvement:

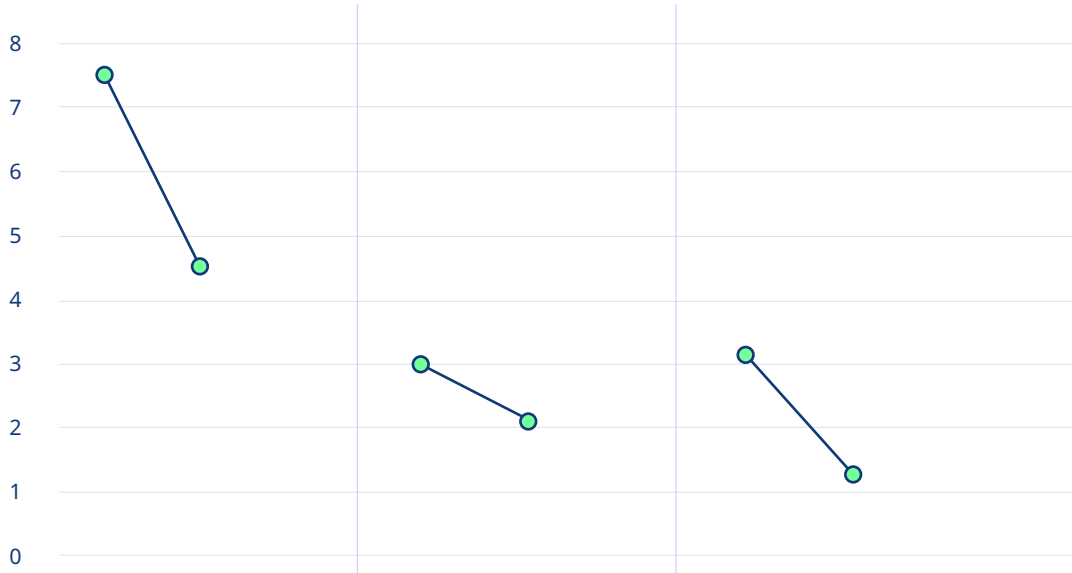
Healthcare showed no progress across all metrics despite HIPAA obligations - a dangerous complacency in a regulated sector.

10% → 11%

Finance moved backward on sensitive data, proving that compliance pressure alone does not drive change.

Reduction Across Key Web Security Metrics

Progress Is Possible



40%

Overall apps running in payment frames decreased from 7.5 to 4.5.

27%

Travel reduced PII access

60%

Insurance cut malicious activity.

Key Imperatives for 2026

Enforce Data Access Justification

With 64% of apps accessing sensitive data without legitimate need,implement automated governance to block unjustified access at the technical layer; policy alone has failed.

Secure Checkout Pages

Despite 40% overall reduction, 47% of remaining apps running in payment frames are unjustified. Leading sites maintain 2 or fewer apps with 100% justification. Google Tag Manager and Shopify, top offenders at 5% each, have no place in payment environments unless essential.

Control Marketing-Digital Footprint

These departments create 43% of all third-party risk. The 82% drop in payment solution PII access proves aggressive cleanup doesn't impede business function, it requires technical controls, not policy restrictions.

Address Critical Infrastructure Collapse

Government and Education malicious activity rates now run 5-10x higher than Insurance, exposing how budget-constrained institutions lose the supply chain battle while private sectors stabilize. Public sector security requires immediate intervention.

Eliminate Weak Signals

Recently registered domains appear 3.8x more on malicious sites --

the strongest infection predictor. Automated blocking of domains registered within 6 months should be default policy, with exceptions requiring explicit review.

Reduce Tracker Proliferation

Leading sites prove 3 trackers suffice. Publisher sites averaging 16 trackers (up 33%) show how monetization pressure drives risk accumulation.

How Leaders Succeed: Four Critical Capabilities

Web threats evolve continuously, third-party code changes externally without control, and attack surfaces expand with every integration. Static quarterly or annual security reviews cannot protect against daily threats.

Success requires:

- **Automated governance** that blocks unjustified data access at the technical layer -- policy alone failed
- **Continuous monitoring** detecting shifts like Government's spike from 2% to 12.9% malicious activity surge in real-time
- **Unified accountability** addressing Marketing/Digital's 43% risk footprint alongside IT's concerns
- **Predictive intelligence** using the 3.8x recently-registered domain signal and CDN dependency patterns

The Divergence Pattern

Organizations aren't converging toward best practices, they're fragmenting into leaders and laggards. Leading sectors slashed payment risk 40% while critical infrastructure tripled exposure. Healthcare and Finance stagnate despite regulations. Even CDN strategies diverge wildly: Education surged 35% while Travel plummeted 50%, proving security approaches are splintering, not standardizing.

The Business Case for Action

Organizations treating web exposure management as a continuous, cross-functional discipline will thrive. The data proves it.

Success stories show what's achievable:

60%
Insurance slashed malicious activity.

17%
Online Retail cut PII access.

25%
Travel reduced PII exposure.

Leading sites maintain minimal third-party footprints with ≤8 apps, ≤3 trackers, and ≤18 domains

The cost of inaction - breached customer data, regulatory penalties, and destroyed trust - far exceeds the investment required for systematic governance. Your website is your digital storefront, transaction platform, and customer relationship hub. Protecting it isn't a technical challenge, it's a business imperative.

The question for 2026 isn't whether to invest in web exposure management, but whether you can afford not to.

See for yourself how Reflectiz can help safeguard your online business

Book a demo

"Reflectiz gives us the visibility we lacked. If a Facebook pixel suddenly starts doing something different, we know. That kind of behaviour protection is what really sets it apart from the other tools we evaluated"

Keyur Lavingia
Head of Security, Village Roadshow

"With Reflectiz, it's almost like having an additional security analyst on site. I now have peace of mind that there is a system constantly watching for anything abnormal on the third-party website. This solution plugged into my existing security setup with ease and was ready to go. It also revealed hidden supply chain risks that I didn't know were there."

Graham Peck
Head of IT & Security, Leeds United

reflectiz