INDUSFACE™

Trends report · 2026

State of Application Security 2026

An analysis of 10.54B+ web and API attacks.

indusface.com

STATE OF APPLICATION SECURITY 2026

The Attack Surface Has Never Been Wider

2025 attack insights and 2026 security priorities from 1,400+ applications and 10.54 billion blocked requests.

1,400+
Applications analyzed

10.54B
Malicious requests blocked

+27%
Attacks per website YOY

$222M
Max ROI Per US Business

KEY FINDINGS

In 2025, attackers abandoned brute-force volume in favor of precision. Short-burst DDoS, API business-logic abuse, and LLM-assisted exploitation replaced noisy campaigns. Static defenses absorbed disproportionate damage. AI-driven managed protection contained incidents faster and at lower cost.

Table of Contents

Research methodology: Data covers 1,400+ AppTrana-protected applications, January–December 2025, across 11 industry verticals and 95 countries. Attack telemetry reflects real enforcement events. Supplementary qualitative data from a survey of 300+ CISOs and senior security leaders.

ABOUT INDUSFACE

The Only AI-Powered, All-in-One AppSec Platform

Indusface secures over 6,500 customers across 95 countries with AppTrana, the industry's only managed WAAP with a 100% uptime SLA and guaranteed zero false positives.

6500+
CUSTOMERS WORLDWIDE
Across 95 countries

100%
UPTIME GUARANTEE
Against Layer 3-7 DDoS

72 hours
VIRTUAL PATCH SLA
Industry-first guarantee

Zero
FALSE POSITIVES
Block-mode from day 1

The managed service advantage

Most teams struggle with sustaining security outcomes. Policies drift, deployments linger in monitoring mode, and DDoS incidents demand 24/7 expertise that is difficult to staff.
AppTrana solves this. Every application in block mode, every vulnerability patched within 72 hours, false positives tuned continuously, no additional headcount required.

Discover · Protect · Remediate

Discover: Automated API and application inventory, including shadow APIs and untracked endpoints.

Protect: AI-powered WAF and DDoS mitigation, 24/7 in block mode, zero false positives.

Remediate: Virtual patching within 72 hours, managed by the Indusface SOC, no dedicated AppSec resource needed.

> *AppTrana is an outcome, not a product. Every application in block mode, protected 24/7, with a team that owns security operations.*

EXECUTIVE SUMMARY

2025: The Year Attacks Got Smarter

Attackers abandoned large, noisy campaigns. In 2025, attacks became shorter, more precise, and tightly aligned with business processes.

+71%

Rise in API attacks. Average per API host ran 20% higher than website hosts; positive security policies blocked 4 in 10.

+56%

Increase in website vulnerability exploits. API vulnerability exploitation jumped 181%, accelerated by LLM-assisted tooling.

90%

Of websites hit by at least one bot attack. Headless browsers and AI-guided behavior make bot traffic nearly indistinguishable from legitimate users.

Attack strategy evolved beyond volume

Volume grew +27%, but the bigger story is methodology. Short-burst precision attacks replaced brute-force floods: 2–3 minute bursts from distributed IP pools, engineered to circumvent static-threshold defenses and outpace human response.

Short-burst DDoS: Over 70% of BFS apps faced at least one monthly burst.

API as primary vector: Undocumented endpoints and limited monitoring create persistent blind spots.

Dwell time risk: 32% of critical vulnerabilities stayed open beyond 180 days.

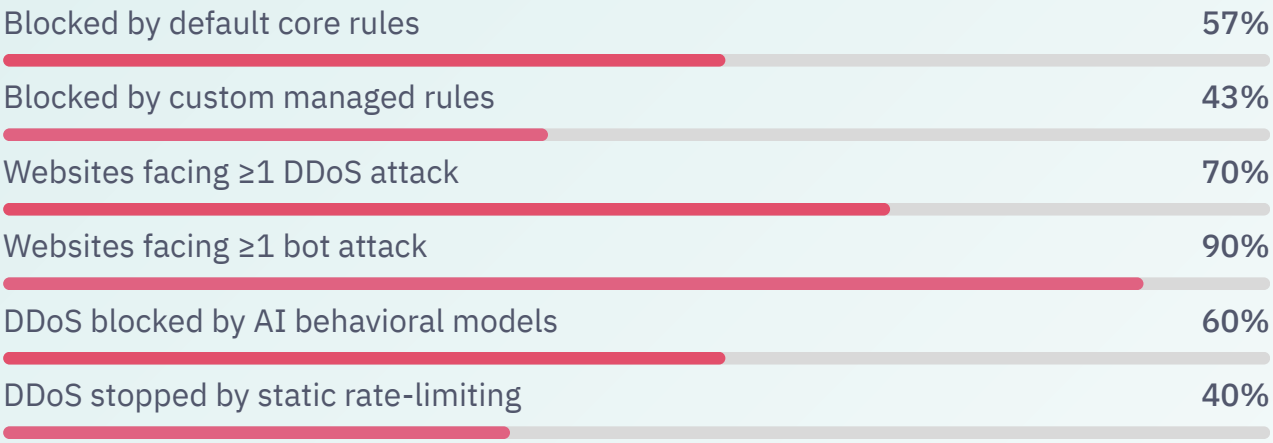
> *"In 2025, the real damage came from attacks that blended into normal traffic, surfacing as cost spikes, performance issues, and operational fatigue."*
>
> Indusface Threat Intelligence, 2025

PROTECTION TRENDS

Inside 10.54 Billion Blocked Attacks

In 2025, every AppTrana-protected site absorbed an average of 7.53 million attack attempts. Behind that number is a consistent pattern, every protected site faced millions of attempts across DDoS, bots, and application-layer threats simultaneously.

How attacks were blocked



The breakdown reveals what modern attack traffic actually looks like: persistent, multi-vector, and designed to find the path of least resistance.

API Attack Escalation

+185%
Bot attacks per API host vs. 2024

+675%
More DDoS on APIs vs. websites. API gateways handle routing, not adversarial security.

+404%
SMB API attacks per host, 2025 vs. 2024

+1,122%
DDoS on SMB APIs, a 10× surge in a single year.

GEOPOLITICAL THREAT

When Geopolitics Triggers Coordinated Attacks

The year's most significant pattern was coordinated infrastructure attacks triggered by geopolitical tension, hitting multiple sectors simultaneously and at a scale that overwhelmed standard perimeter defenses.

172% Peak DDoS spike · BFS · Operation Sindoor

BFS Attack Data 2025

+113%
BFS attacks YoY — 2.72B total

+149%
BFS vulnerability attacks

+28%
BFS DDoS attacks overall

During Operation Sindoor, the Banking and Financial Services sector absorbed a 172% spike in DDoS attacks within 72 hours. Attack origins spanned hundreds of thousands of IPs, the signature of botnet-as-a-service infrastructure at scale.

Motives extended beyond disruption: regulatory interference, trust erosion, and extortion leverage were all observed. Short-burst patterns lasting 2 to 3 minutes, timed to complete before human response, were the dominant method.

Over 70% of BFS apps faced at least one monthly burst across 2025. Static defenses cannot absorb sudden 172% spikes. Only AI-driven behavioral detection with automatic escalation can respond within sub-minute windows.

> *"Any financial institution faces the risk of being a target during regional geopolitical events. Preparation cannot begin after the spike."*
>
> Indusface Threat Intelligence, BFS Sector Analysis 2025

VULNERABILITY EXPLOITS

~18,500 Critical & High Vulnerabilities — 32% Still Open After 6 Months

~18,500+ Critical & High Vulns	**32%** Open after 180 days
+56% API vuln exploitation YoY	**+181%** Website vuln attacks YoY

TOP 5 WEB APP VULNERABILITY CATEGORIES

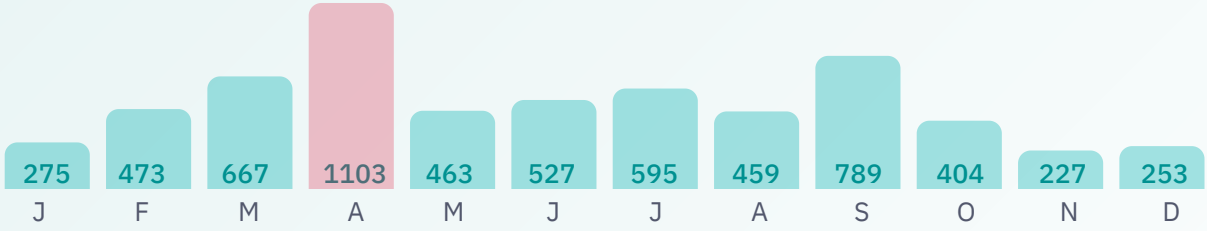
#	VULNERABILITY TYPE
1	PHP Object Injection
2	File Upload (MIME Type Validation)
3	Possible Blind SQL Injection
4	Sensitive Credentials Exposed in Headers
5	Server-Side Request Forgery (SSRF)

TOP OWASP API VULNERABILITY CATEGORIES

#	OWASP API CATEGORY
1	API8:2023 — Security Misconfiguration
2	API6:2023 — Unrestricted Access to Sensitive Flows
3	API10:2023 — Unsafe Consumption of APIs
4	API3:2023 — Broken Object Property Level Auth
5	API2:2023 — Broken Authentication

Zero-Day Vulnerabilities 2025

6,235 zero-days — 2.5× vs 2024 · **99.4%** protected by core rules



The LLM acceleration effect

The 2.5× jump in zero-days correlates with the proliferation of LLM-assisted tooling. Novice attackers can now generate working exploits for published CVEs within hours of disclosure. The exploitation window has collapsed from weeks to days. Virtual patching at the WAF layer is the primary defense while code-level fixes are pending.

32% of critical vulnerabilities stayed open beyond 180 days. Development backlogs are the leading cause.

INDUSTRY TRENDS

Every Sector Paid an Attack Tax in 2025

No vertical was spared.

HIGHEST LOSS

Banking & Financial Services

Total Attacks	**2.72B**
YoY attack growth	**+113%**
Vulnerability attacks	**+149%**
DDoS growth	**+28%**

HIGH RISK

Insurance

Attack growth	**+118%**
DDoS per site	**+143%**
Vulnerability attacks	**+220%**
Peak timing	**Claims season**

ESCALATING

Manufacturing

Total Attacks	**~1.55B**
YoY attack growth	**+110%**
DDoS per site	**+107%**
Vulnerability Attacks	**+167%**

PATIENT DATA

Healthcare

Total Attacks	**~24.14M**
Intensity	**+115%**
DDoS growth	**+39%**
Primary risk	**Patient data**

MOST EXPOSED

SMBs

Total attacks	**~894M**
YoY growth	**+71%**
DDoS share	**85%**
API DDoS	**+1,122%**

API-HEAVY

Retail

Key vector	**API abuse**
Peak risk	**Holiday season**
Common threat	**Bot+scraping**
Gap	**API discovery**

The SMB vulnerability

SMBs recorded ~894 million attacks in 2025, a 71% increase, with teams of fewer than five people managing both infrastructure and security. DDoS is 85% of SMB traffic, nearly 3× the enterprise rate. The 1,122% API DDoS surge reflects rapid API deployment without corresponding governance.

Attackers don't distinguish by size

Insurance (+220% vulnerability attacks) and Manufacturing (+167%) are underinvesting relative to risk. Healthcare presents a different profile: lower volume, but breach consequences dwarf prevention costs.

ROI ANALYSIS

AppTrana Delivered $86M–$222M in Value Per US Business

Two value streams: operational savings from eliminating manual overhead, and risk mitigation from blocking exploit attempts on open vulnerabilities.

$222M

Maximum US ROI per business (Healthcare, 25-app portfolio). Breach avoidance at IBM Cost of Data Breach 2025 benchmark costs plus virtual patching and DDoS monitoring savings.

$2.7M

Maximum RoW ROI per business (Insurance). Based on enforcement actions including the IRDAI Star Health fine and regional breach benchmarks.

INDUSTRY	US ROI / APP	ROW ROI / APP
Banking & FS	$8.91M	$106K
Insurance	$8.64M	$119K
Healthcare	$14.30M	$85K
Retail	$5.11M	$73K
SaaS / Tech	$6.83M	$90K
US Business (25 apps)	**$86M-$222M**	**$1.2M-$2.7M**

> *"We halved the DBIR probability and capped all figures against actual enforcement actions. Even then, the ROI is compelling."*
>
> Indusface ROI Analysis Framework, 2025

SECURITY STRATEGIES FOR 2026

Eight Priorities Every Security Team Must Act On

Always-On Automated Protection

RESPONSE TIME

Attacks lasting 2–3 minutes are over before human response begins. Automated, always-on protection is the **only viable first** line of defense.

Virtual Patch at the Perimeter

VULNERABILITY

32% of critical vulns stay open beyond 180 days. Block at the WAF while dev teams fix the code.

Automate API Discovery

API SECURITY

Undocumented APIs are a security emergency. One-click protection must follow discovery automatically.

Eliminate False Positives

ACCURACY

As attacks blend with traffic, managed WAAP with continuous rule tuning prevents unnecessary disruption.

Behavior-based DDoS

DDOS DEFENSE

Static thresholds can't stop millions of IPs delivering minimal payloads. AI behavioral models are the only mechanism that scales.

Positive Security for APIs

API DEFENSE

API gateways handle routing not business logic abuse or API-layer DDoS. Positive security is required, not optional.

Managed Security for SMBs

SMB

85% of SMB attacks are DDoS. Teams under 5 people cannot staff 24/7 response. Managed WAAP is the only viable model.

Security in the Dev Lifecycle

DEVSECOPS

CI/CD scanning, API discovery, and continuous monitoring must replace the once-a-year pen test.

The managed service imperative

A consistent pattern: effective execution requires ongoing human-in-the-loop management. Detection is automated; tuning, patching, and false-positive resolution determine whether protection stays effective.

Organizations that treat WAAP as deploy-and-forget see protection degrade within months. Active managed services sustain block rates above 99% year-round.

CUSTOMER TESTIMONIALS

Security Leaders on Real-World Results

Customers across banking, FMCG, and housing finance on what AppTrana's managed service delivers in practice.

"The Risk Based Fully Managed Application Security technology offering from Indusface provided us the best value for money."

Kiran Belsekar
EVP — CISO & IT Governance, Bandhan Life

"We do not have a special SOC for Application Security. As our AppTrana product license includes managed services, the Indusface team is the AppSec SOC for us."

Mayuresh Purandare
Head — IT Infrastructure & Cyber Security, Marico

"With AppTrana WAAP, every application runs in block mode and is safeguarded 24/7 with guaranteed 100% uptime. By partnering with Indusface, we have achieved significant operational savings. The depth of support, responsiveness, and commitment we experience with Indusface is truly unmatched."

Anubhhav Rajput
CIO & CTO, Head of Digital Transformation, PNB Housing Finance

INDUSFACE™

DALLAS | BENGALURU | VADODARA | MUMBAI | NEW DELHI

Contact Us: +1 866 458 3058, +91 265 6133021

sales@indusface.com | indusface.com