INDUSFACE™

STATE OF APPLICATION SECURITY

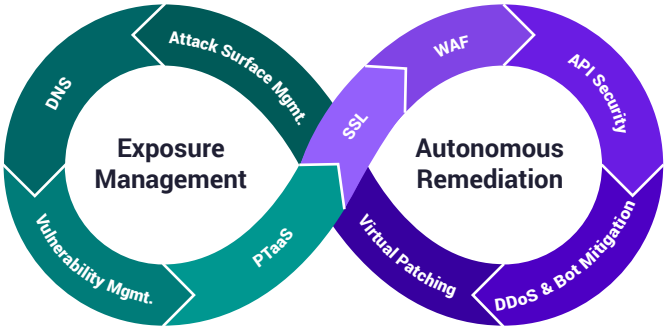
H1 2025

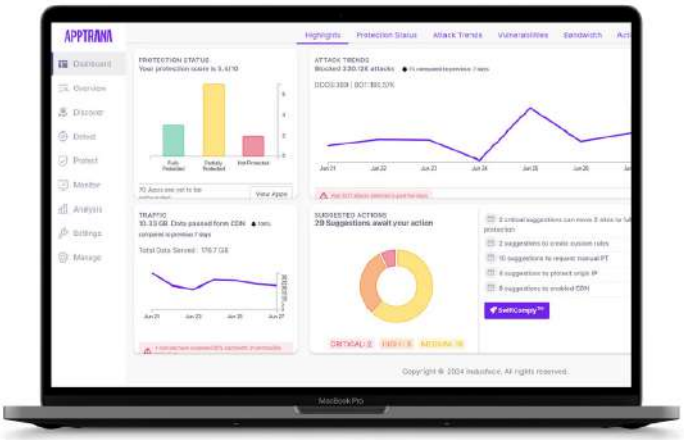
INDEX

APPTRANA

AI-Powered, Fully Managed Application and API Protection

AI-Powered, Continuous Compliance for Web Apps and APIs





START YOUR FREE TRIAL NOW

ABOUT INDUSFACE

Indusface is a leading application security SaaS company, securing over 5,000 customers across 95 countries with its award-winning platform. Funded by institutional investors, it has been a category leader in Gartner Peer Insights™ for the past three years.

The industry's only AI-powered, all-in-one AppSec platform helps businesses discover, detect, remediate, and protect web applications and APIs at internet scale, backed by a 100% uptime guarantee.

INDUSFACE IS THE ONLY CLOUD WAAP (WAF) VENDOR WITH 100% CUSTOMER RECOMMENDATION FOR 4 CONSECUTIVE YEARS

A CUSTOMERS' CHOICE FOR 2024, 2023 AND 2022 GARTNER® PEER INSIGHTS™

Gartner Peer Insights Customers' Choice 2024

OUR CUSTOMERS

EXECUTIVE SUMMARY

H1 2025 vs H1 2024: Attackers Are Now Focusing More on Exploiting Vulnerabilities and APIs

In the first half of 2025, attacks on websites and APIs continued to rise across industries. The biggest shift this year is in how attackers operate. Instead of relying heavily on broad automated methods, they are now focusing more on **targeted attacks that exploit vulnerabilities on websites and APIs.**

This change is most likely being driven by a few key factors:

- AI & LLM tools like ChatGPT have made it easier for attackers to perform sophisticated attacks
- APIs are often less protected and harder to manage at scale, making them easier targets
- At the same time, better bot detection and declining success rates from basic automation may be quietly pushing attackers toward more effective methods. This includes a noticeable rise in DDoS and vulnerability attacks on APIs, as these endpoints are often loosely documented, less monitored, and critical to application availability and data access

Here are the attack trends seen in H1 2025 as compared to H1 2024:

Website Attacks

- The number of attacks per website in India increased by **14%**, while **DDoS attacks** rose by **15%**
- **Vulnerability attacks** grew by **27%**, and **custom rule-based attack mitigations** increased by **47%**, indicating a rise in targeted and evasive attack patterns that required tailored defenses

API Attacks

Attackers are now putting far more focus on APIs than on websites. In H1 2025, **API attacks increased by 104%**, with a sharp rise in both **vulnerability exploitation** and **DDoS attacks.**

- **Vulnerability attacks on APIs grew 13X**, while **DDoS attacks rose by 30%**
- In terms of DDoS, **API hosts experienced 388% more attacks per site**
- **Targeted attacks blocked by positive security policies grew by 12X,** highlighting the importance of enforcing strict security controls for effective API protection

Total Value Delivered by AppTrana:

In the last one year, AppTrana delivered measurable business value/ROI per app, ranging from **$5.1M to $14.32 in the US and ₹79 lakhs to ₹1.2 Cr in India.**

Here is a breakdown off the total ROI:

US applications:

Parameters	Per App Value/ROI Range
Operational Savings	$56K to $57K
Risk Mitigation Savings from Managed WAAP	$5.08M to $14M
Total Value Delivered	$5.1M to $14.32

India applications:

Parameters	Per App Value/ROI Range
Operational Savings	₹21.42 lakhs to ₹21.75 lakhs
Risk Mitigation Savings from Managed WAAP	₹58 lakhs to ₹99 lakhs
Total Value Delivered	₹79 lakhs to ₹1.2 Cr

The ROI values vary by industry in the above given range and are calculated using actual enforcement references with a conservative risk adjustment. For complete details on the calculation, please refer to the ROI section on the page 22.

INDUSTRY-SPECIFIC TRENDS (H1 2025 VS H1 2024)

BANKING & FINANCIAL SERVICES

- 14% increase in overall attacks
- 46% increase in vulnerability attacks
- 95% of BFS sites witnessed a bot attack
- 172% rise in DDoS attacks during Operation Sindoor.

INSURANCE

- 309% increase in overall attacks
- 350% increase in DDoS attacks
- Vulnerability attacks grew by 10X

HEALTHCARE

- Attacks blocked by custom rules grew by 247%
- 100% of healthcare sites faced a bot attack

MANUFACTURING

- 311% increase in overall attacks
- 427% increase in DDoS attacks
- Vulnerability attacks grew by 459%

RETAIL & E-COMMERCE

- 420% higher DDoS attacks
- 127% increase in vulnerability attacks
- Carding, credential stuffing, & fake account abuse marked widespread bot activity

SMBS

- 202% more website attacks than enterprises
- 74X more API attacks and 121X higher DDoS attacks on APIs compared to enterprises

PROTECTION TRENDS

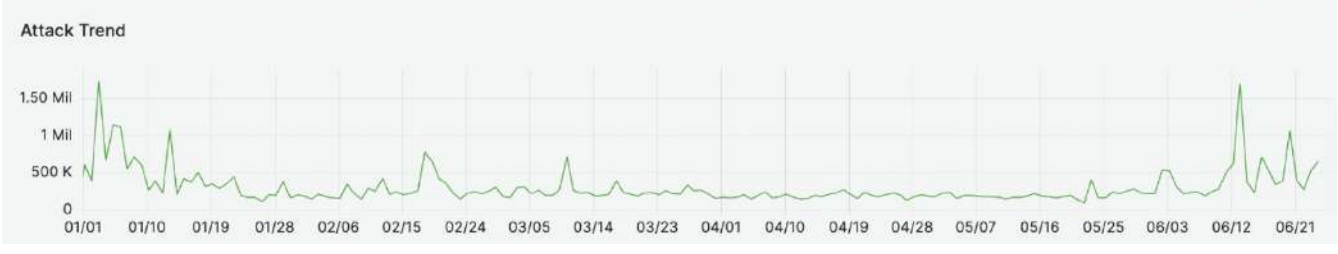
Total Attacks Count

4.8 Billion

We saw over 4.8 billion requests that got blocked across all sites protected by AppTrana.

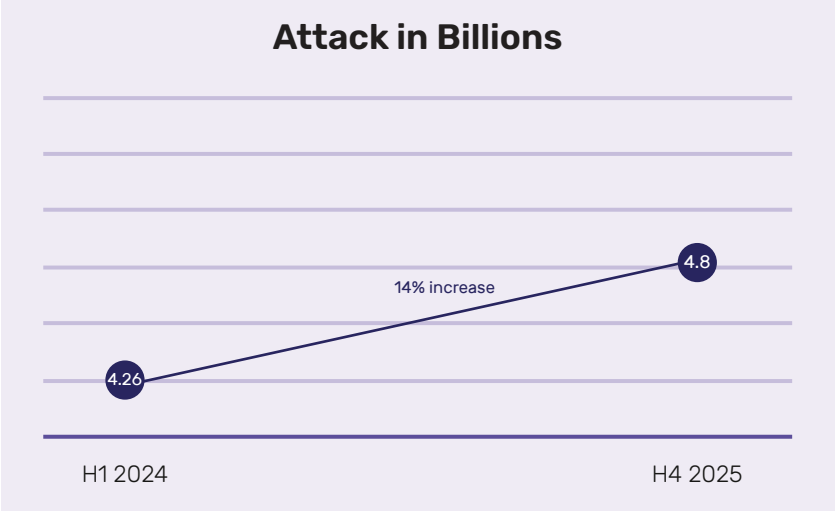
On average, each site witnessed over 3.48 million attacks in the year.

A view of the last 180-day attack trend across all the sites:



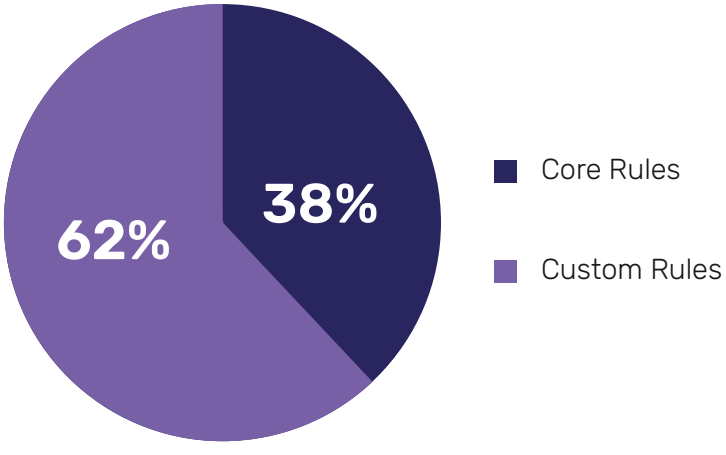
Top 10 Attack Originating Countries

Country	Blocks
India	3270263149
United States	338619112
France	181728661
Singapore	90244012
Germany	62312096
United Kingdom	57006585
Brazil	19194174
Italy	17294828
Australia	11255452
Malaysia	9830168



The cyberattacks grew by 14% in the H1 of 2025 compared to H1 of 2024

Most of attacks originated from India, followed by United States, France, Singapore, and Germany.



In the H1 2025, approximately 38% of requests were blocked by AppTrana's default rule set, while 62% were blocked by custom rules tailored to the specific requirements of each application. This highlights the value of the managed services provided by AppTrana.

ROI HIGHLIGHT

US (per app): $5.1M – $14.32M

India (per app): ₹79 lakhs – ₹1.2 Cr

The ROI values vary by industry in the above given range and are calculated using actual enforcement references with a conservative risk adjustment. For complete details on the ROI calculation, kindly refer to the ROI section on page number 22.

DDoS & BOT ATTACKS

As new DDoS and bot attack trends emerge against web applications and APIs, business continuity becomes very important.

- AppTrana WAAP guarantees zero false positives and ensures 100% uptime against layer 3-7 DDoS attacks with AI-driven behavioral DDoS mitigation and rate-limiting based on URI, IP, host, and geo. Click here to learn more
- Against bot attacks such as account takeover, credential stuffing, and scraping, AppTrana WAAP provides protection from day zero with AI-driven behavioral bot protection, real-time analysis of bot traffic, correlated risk scoring, anomaly detection, and custom controls. Click here to know more.

We saw the following DDoS and Bot trends in the year:

DDoS Attacks

Total Sites Affected by DDoS Attacks	Total DDoS Attacks –
70%	**1.52+ Billion**

Here is a view of the last 180-day DDoS attack trend across all sites:

Major countries from where DDoS attacks originated apart from India, were the United States, the UK, and France.

7 out of 10 websites experienced a DDoS attack.

During the week of Operation Sindoor, when tensions rose between India and Pakistan, the Banking and Financial Services sector saw a 172% spike in DDoS attacks. This surge highlights how geopolitical events can trigger targeted cyberattacks on critical infrastructure, especially in sectors like BFS that are essential to national stability.

Approximately 40% of these DDoS attacks were successfully blocked by static URI-based rate-limiting measures. However, the remaining 60% were neutralized by AI-driven behavioral models on AppTrana WAAP, even in the cases where attackers used millions of IP addresses to conduct low-rate attacks.

After surveying over 300+ CISOs, CTOs, and other security leaders outside our customer base, we gathered insights regarding their challenges in managing DDoS attacks. Here are the responses shared by these security leaders regarding their difficulties with DDoS attacks:

of leaders identify service disruption as the biggest challenge posed by DDoS attacks

leaders are not confident in their existing WAF/WAAP solutions to protect their businesses against large-scale DDoS attacks

Bot Attacks

Total Sites Affected by Bot Attacks	Total Bot Attacks
90%	**64 Million**

Here is a view of the last 180-day Bot attack trend across all sites:

Major countries from where bot attacks originated apart from India, were the United States, France and Singapore.

9 out of 10 websites experienced a bot attack.

of industry leaders cite service disruption as the primary challenge posed by bot attacks

leaders are not confident in their Web Application Firewall (WAF) solutions for protecting their businesses against bot attacks

API Attacks

Total API Attacks

1.36+ Billion

A view of the last 180-day API attack trend across all sites:

- Average attacks per API host were 72% higher compared to attacks per website.

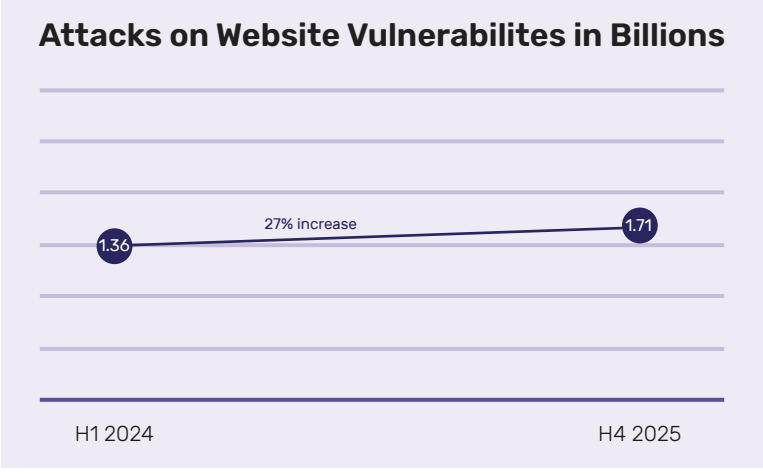
- APIs are experiencing over 388% more DDoS attacks compared to websites. This trend is particularly concerning for organizations that rely solely on API gateways for security. API gateways are often unable to provide sufficient protection against advanced DDoS attacks and have limited defenses against bot attacks, zero-day vulnerabilities, and other related threats.

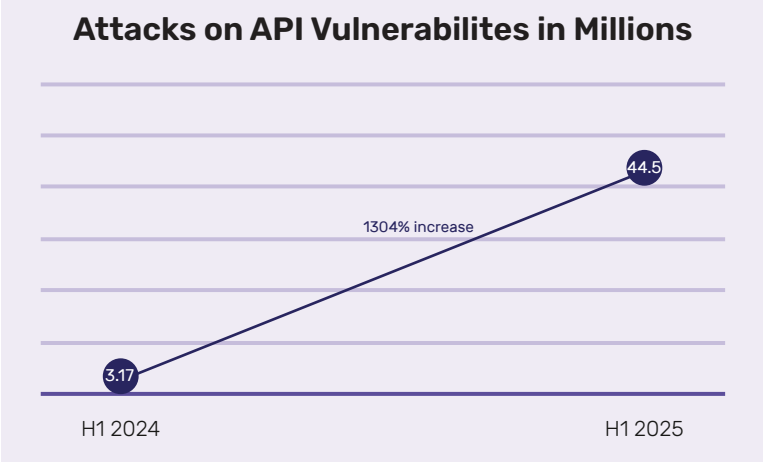
- **Targeted attacks blocked by positive security policies (custom rules) grew by 12X,** highlighting the importance of enforcing strict security controls for effective API protection. AppTrana offers automated API discovery and one-click protection, which saves organizations time in documenting APIs and provides tailored protection for each API without requiring extensive manual intervention.

VULNERABILITY EXPLOITS

Attacks on website vulnerabilities increased by 27%, while attacks on API vulnerabilities skyrocketed by 13X from H1 2024 to H1 2025. A significant factor in this rise may be the widespread use of large language model (LLM) tools like ChatGPT, which allow novice hackers to easily discover and use scripts that exploit open vulnerabilities.

In addition, APIs often expose sensitive functions and data directly to the internet and are frequently updated without thorough security testing, making them a prime target. This accessibility and growing attack surface have lowered the barrier to entry for cybercriminals, leading to an unprecedented surge in the exploitation of vulnerabilities.





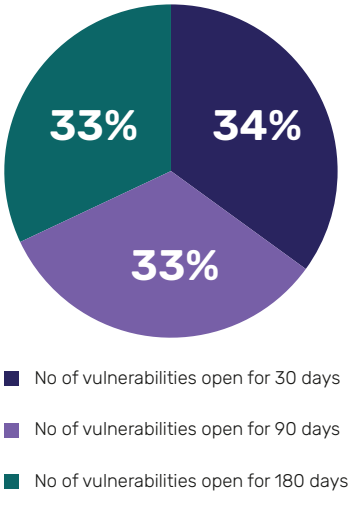
Total no. of critical and high vulnerabilities found in the applications: **18K**

Top 5 critical and high vulnerability categories found in web applications:

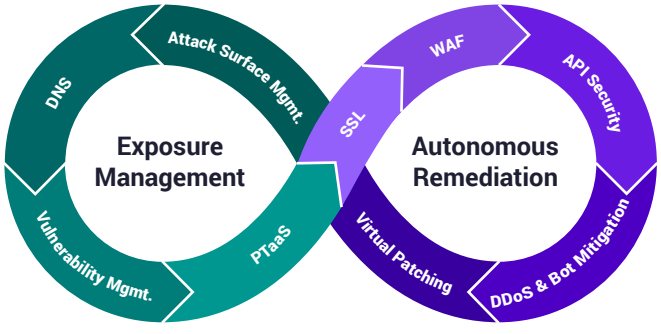
#	Vulnerability Type
1	PHP Object Injection
2	File Upload Vulnerability (MIME Type Validation)
3	Server Side Request Forgery Detected
4	DOM Location Manipulation
5	Blind SQL Injection

We identified 18K critical and high vulnerabilities, with 33% of these remaining open for 180+ days.

With AppTrana, our customers were able to virtually patch these vulnerabilities immediately, significantly reducing the time needed to resolve them. This allows the security team to function as an enabler of business rather than a blocker.



AI-Powered, Continuous Compliance for Web Apps and APIs



No false positives. No open vulnerabilities. AI-powered WAAP with human verification ensures every app and API is protected against all known threats-remediated within 72 hours, an industry only capability.

Top OWASP API vulnerability categories found:

#	API Vulnerability Type
1	A5: Security Misconfiguration
2	A3: Injection
3	A6: Security Misconfiguration
4	A7: Identification and Authentication Failures
5	A2: Cryptographic Failures

of organizations do not scan their APIs

organizations use automated DAST scanners to scan their APIs

While performing penetration testing is considered a best practice, it is often costly, time-consuming, and typically done only once a year.

Indusface's DAST scanner for APIs typically identifies over 90% of the vulnerabilities found in manual penetration testing and completes scans in just a couple of hours. Notably, around 95% of the identified API vulnerabilities were patched using application-specific Positive/Negative security models.

Another useful feature is CI/CD integration, which allows for automatic triggering of scans upon code check-in and enables the assignment of open vulnerabilities to the development team for timely patching.

Zero Day Vulnerabilities

In H1 2025, 3508 zero-day vulnerabilities were identified for the websites protected by the AppTrana WAAP. In H1 2024, the number of zero-day vulnerabilities was 1,265, showing a consistent trend of increasing zero-day vulnerabilities.

All AppTrana customers have benefited from risk-based protection, which effectively detects and safeguards against zero-day vulnerabilities. By default, approximately 98% of these vulnerabilities were protected by core rules, while the remaining 2% were covered by custom rules. **Resulting in 100% protection from zero-day** vulnerabilities throughout the year.

Zero Day Vulnerabilities

In H1 2025, 3508 zero-day vulnerabilities were identified for the websites protected by the AppTrana WAAP. In H1 2024, the number of zero-day vulnerabilities was 1,265, showing a consistent trend of increasing zero-day vulnerabilities.

All AppTrana customers have benefited from risk-based protection, which effectively detects and safeguards against zero-day vulnerabilities. By default, approximately 98% of these vulnerabilities were protected by core rules, while the remaining 2% were covered by custom rules. **Resulting in 100% protection from zero-day** vulnerabilities throughout the year.

A view of the Zero-Day vulnerabilities identified in the year:

Month	Jan 25		Feb 25		Mar 25		Apr 25		May 25		Jun 25	
Total Vulnerabilities	275		473		667		1103		463		527	
Parameters	Value	%	Value	%	Value	%	Value	%	Value	%	Value	%
Protected by Core Rules	248	90%	466	99%	666	99%	1103	100%	463	100%	527	100%
Protected by Custom Rules	27	10%	7	1%	1	1%	0	0%	0	0%	0	0%

Amidst known vulnerabilities, we observed several critical zero-day vulnerabilities, such as:

- Cryptocurrency Mining Attack Exploiting PHP Vulnerabilities
- Credential Coercion Vulnerabilities in Ivanti Endpoint Manager
- CVE-2024-4577 – PHP-CGI RCE Exploitation in Windows Servers
- CVE-2025-24813 – Apache Tomcat Vulnerability Under Active Exploitation
- CVE-2017-12637: Exploitation of SAP NetWeaver Directory Traversal Vulnerability

INDUSTRY-SPECIFIC TRENDS (H1 2025 VS H1 2024):

Banking and Financial Services (BFS):

The Banking and Financial Services sector continues to face consistent and focused targeting by attackers. In H1 2025, overall attacks increased by 14%, but more importantly, 78% of all attacks in this sector were aimed at exploiting vulnerabilities. It suggests attackers are focusing more on finding real entry points, not just testing the surface through trial and error.

- **Vulnerability attacks increased by 46%**
- Among targeted exploit attempts, **54% were blocked using custom rules,** indicating that attackers are increasingly spending time crafting targeted, sophisticated attacks, largely because of the **high-value data, real-time transactional systems, and deeper access opportunities** that BFS applications provide
- **95% of BFS sites witnessed a bot attack,** with most attacks focused on login abuse, scraping, and transaction manipulation
- **Financial services SaaS platforms** reported the highest volume of API attacks across all the sectors
- **During the week of Operation Sindoor, when tensions rose between India and Pakistan,** the Banking and Financial Services sector saw a **172% spike in DDoS attacks and 35% increase in overall attacks.** This surge highlights how geopolitical events can trigger targeted cyberattacks on critical infrastructure, especially in sectors like BFS that are essential to national stability.

INSURANCE

In H1 2025, the Insurance sector experienced a sharp escalation in cyberattacks, with overall attack volumes rising by 309% compared to H1 2024. The sector is facing growing pressure from attackers who aim not only to breach systems but also to disrupt service availability.

- **DDoS attacks rose by 350%,** targeting critical times like claim processing and policy renewals
- **Vulnerability attacks grew 10X,** as attackers focused on exploiting unpatched vulnerabilities and insecure functionalities across web portals
- **92% of insurance websites were hit by bots,** often used to abuse login flows or submit fake claims
- With increasing digitization and large volumes of customer data, insurers continue to be high-value targets for both disruption and exploitation

MANUFACTURING

The Manufacturing sector experienced a significant rise in attacks, with overall attacks increasing by 331% compared to H1 2024. Attackers focused on disrupting operations and accessing proprietary systems.

- **DDoS attacks grew by 427%,** targeting internal tools like timesheet portals, documentation systems, and production dashboards to interrupt routine processes
- **Vulnerability attacks increased by 459%,** with many attempts aimed at systems that store intellectual property including design files, product specs, and engineering data
- **13% more attacks were blocked via custom rules,** suggesting that while most attacks remain opportunistic, the trend is gradually shifting. Manufacturers cannot afford to overlook the need for custom protections as their data and systems become more exposed

HEALTHCARE

The Healthcare sector remained a target for attackers with most threats aiming to access sensitive data.

- **Attacks blocked via custom rules grew by 247%,** reflecting a rise in targeted exploit attempts on systems like EMRs, test result dashboards, and online consultation platforms
- **100% of healthcare websites** faced bot attacks, often abusing login portals, appointment systems, and patient data forms
- With highly sensitive patient data and the high price it commands on the dark web, healthcare continues to face persistent threats across applications and APIs.

RETAIL & E-COMMERCE

The real-time nature of Retail and E-Commerce, combined with payment data, high traffic, and uptime sensitivity, continues to make the sector one of the top priorities for attackers.

- **DDoS attacks rose by 420%,** aimed at disrupting order flows and user experience, with downtime increasingly used as leverage in ransom-driven attacks
- **Vulnerability attacks increased by 127%,** targeting payment flows, checkout logic, and third-party scripts for Magecart-style and formjacking attacks
- **Bot attacks remained widespread,** including carding, credential stuffing, and fake account abuse to commit fraud at scale
- With growing reliance on third-party services running in the browser, attackers are also exploiting client-side vulnerabilities that often go undetected by server-side defenses

SMALL AND MID-SIZED BUSINESSES (SMBS)

While large enterprises remain high-value targets, attackers are increasingly turning their attention to SMBs, where security coverage is often fragmented and response times are slower.

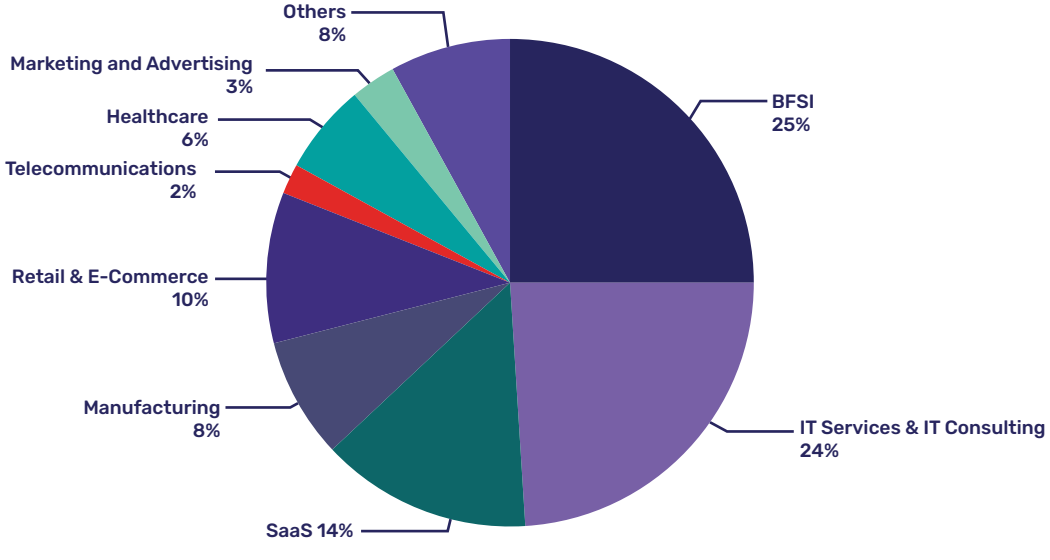
- SMBs faced **202% more attacks per site** compared to enterprises, with **14X higher DDoS attacks per site**
- Talking about APIs, the SMBs experienced **74X more API attacks and nearly 121X higher DDoS attacks on APIs** with respect to enterprises
- **API vulnerability attacks almost doubled,** driven by gaps in visibility and protection
- SMBs mostly have fewer than five people managing both infrastructure and security, often without 24/7 monitoring or dedicated protection. This likely makes DDoS the most exploited attack vector, with attackers using downtime to disrupt services or pressure businesses into paying ransom.

STATE OF APPLICATION SECURITY H1 2025 - RESEARCH OVERVIEW

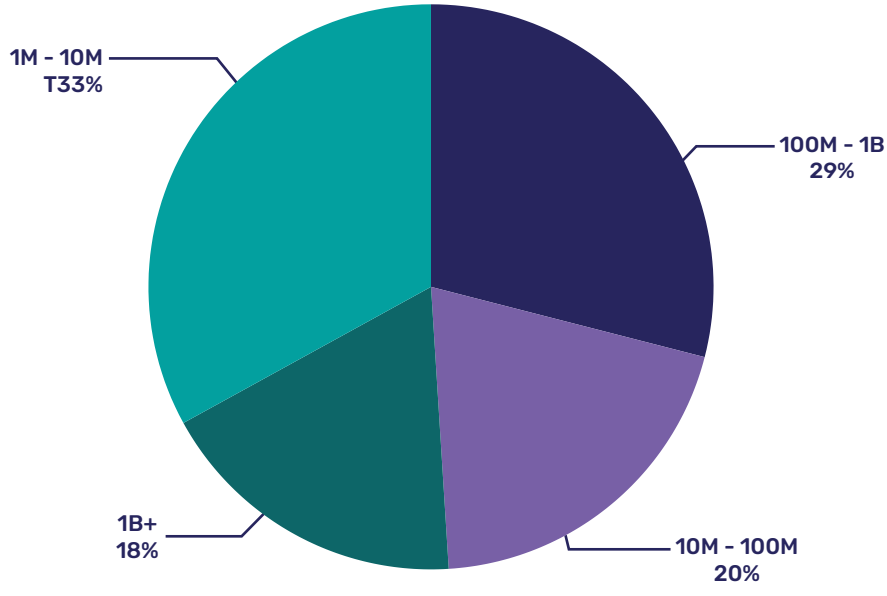
The State of Application Security H1 2025 report is based on a sample size of 1400+ global websites and applications that were analyzed between Jan 1st, 2025, and June 30th, 2025.

During this period, various enterprise, government, and SME websites were analyzed. The below figure illustrates the diversity of industries represented in this report.

Industries Analysed



Company Sizes



Apart from the above-mentioned analysis of the sites, Indusface also surveyed over 300 CISOs, CTOs, and other security leaders to understand their pain points related to application security concerns and challenges faced due to DDoS, Bot, and API attacks.

ROI ANALYSIS OF MANAGED WAF – OPERATIONAL SAVINGS AND RISK MITIGATION

The key question: what ROI do our customers achieve. While there are many parameters that could be used for this calculation, our methodology here uses the below two aspects:

1. Operational Savings from Managed WAAP
2. Risk Mitigation Savings from Managed WAAP

1. Operational Savings from Managed WAAP

This section evaluates the cost savings achieved through AppTrana's Managed WAAP in two operational areas: DDoS monitoring and patch cycle avoidance. These savings are direct, measurable, and arise from the elimination of time spent to handle these functions.

1.1 Patch Cycle Avoidance

The biggest benefit of having a managed WAAP includes speeding up the patch cycles through virtual patches, which are compensatory controls accepted by all major regulators and compliance bodies.

1.1.1 Cost of Deploying an Application in Block Mode

To leverage virtual patching effectively, a WAAP must first be deployed in block mode with origin server protection enabled by default. AppTrana's SOC team takes responsibility for false positive testing and ensures that every deployment is moved into block mode.

Without such a managed onboarding process, in-house teams bear the cost of enabling block mode themselves. Industry benchmarks indicate that best-in-class vendors can deploy an application in approximately three days. When handled internally, however, this timeline is typically closer to six days per application due to false positive tuning, stakeholder coordination, and validation.

Even this is a conservative estimate as most industry studies state that three to six months deployment time is standard. This is largely due to false-positive tuning, stakeholder coordination, and impact validation.

	US	India
Developer	$75	₹2,800
SOC Engineer	$80	₹3,500

Table 1: Resource costs

Using the estimates above for per-hour costs, for block mode onboarding, the cost is

- **US:** 48 × $80 = **$3,840**
- **India:** 48 × ₹3,500 = **₹168,000**

1.1.2 Cost of Patching Vulnerabilities on Code

Industry studies indicate that nearly half of all WAF deployments operate in monitoring mode, which forces application teams to patch every vulnerability directly in code.

Even when applications are deployed in block mode, there is still a gap: DAST scanners and WAAPs rarely integrate, and responsibility often falls across different teams. This lack of visibility means application teams still end up carrying a heavy code patching burden.

According to Edgescan's report, an average application enters production with 10–60 open vulnerabilities. For this analysis, we take a mid-range estimate of 35 vulnerabilities per application. With AppTrana, every application is deployed in block mode, ensuring that approximately 70% of vulnerabilities are automatically protected. Our managed services team then develops custom rules that address most of the remaining cases, leaving just 1–2 vulnerabilities per application requiring code-level fixes.

Industry research from IBM and Veracode shows that patching a single vulnerability requires 12–30 hours for root cause analysis, code changes, unit and integration testing, and QA/regression testing. Using an average of 21 hours, the total cost of code patching is calculated as:

- **US:** 33 × 21 × $75 =**$51,975**
- **India:** 33 × 21 × ₹2,800 =**₹19,40,400**

1.2 DDoS Monitoring Cost Avoidance

The next parameter is the cost avoided by preventing downtime associated with a DDoS or a bot attack.
Based on historical data, below is a table that shows the probability of a DDoS attack across various industries:

Industry	Probability serious DDoS/year
Banking & FS	40%
Insurance	35%
Healthcare	30%
Retail	25%
SaaS / Tech	20%

Table 2: Estimated probabilities of a DDoS attack across various industries

Then we multiply the above probabilities with the time it takes to recover from a DDoS attack. Usually, it is about 12 hours for monitoring, analysis, and mitigation time.

Industry	Hours/year/app
Banking & FS	4.8 hours
Insurance	4.2 hours
Healthcare	3.6 hours
Retail	3.0 hours
SaaS / Tech	2.4 hours

Table 3: Estimated time spent on attack mitigation

Then cost savings is a simple multiplication on $/hour. Based on industry data, the cost for a senior security engineer in the US is $80/hour and India is $42/hour.

Cost savings per app per year for app across industries includes:

Industry	Hours/year/app	US$/app/year	₹/app/year
Banking & FS	4.8	$384	₹16,800
Insurance	4.2	$336	₹14,700
Healthcare	3.6	$288	₹12,600
Retail	3.0	$240	₹10,500
SaaS / Tech	2.4	$192	₹8,400

Table 4: Estimated cost savings on DDoS attack mitigation

Finally, irrespective of whether an incident occurs, SOC team needs to spend time on:

1. **Monitoring dashboards for** signs of attacks
2. **Fine-tuning thresholds** and updating playbooks
3. **Running detection & response drills**
4. **Shift handovers** and status briefings
5. **Tool upkeep**(signatures, integrations, reporting)
6. **False positive investigations**
7. **Coordinating with ISPs / upstream providers** even when there is no active incident

In SOC terms, this is called "coverage factor", "operational readiness overhead", or "staffing multiplier".

In SOC staffing models, this is often expressed as:

$$\text{Total SOC Hours/year} = \text{Incident Hours/year} \times \text{Coverage Factor}$$

Where:

- **Coverage factor** accounts for **continuous monitoring + preventive work**
- Typical range in industry: **3X to 6X**(depending on maturity and tooling)

As per SANS SOC Staffing Guide, NIST SP 800-61, and Gartner SOC TCO models, most SOC teams spend 60–80% of their time on readiness and preventive work rather than live incident handling. A multiplier of 4X, therefore, reflects realistic operational effort while staying conservative.

The updated numbers are:

Industry	Hours/year/app (incident)	Hours/year/app (with 4X Coverage Factor)	US$/app/year	₹/app/year
Banking & FS	4.8	19.2	$1,536	₹67,200
Insurance	4.2	16.8	$1,344	₹58,800
Healthcare	3.6	14.4	$1,152	₹50,400
Retail	3.0	12.0	$960	₹42,000
SaaS / Tech	2.4	9.6	$768	₹33,600

Table 5: Final estimated cost savings on DDoS attack monitoring and mitigation

Total Operational Savings from Managed WAAP

Industry	US$/app/year	₹/app/year
Banking & FS	$1,536 + $51,975 + $3,840 = **$57,351**	₹67,200 + ₹1,940,400 + ₹168,000 = ₹2,175,600
Insurance	$1,344 + $51,975 + $3,840 = **$57,159**	₹58,800 + ₹1,940,400 + ₹168,000 = ₹2,167,200
Healthcare	$1,152 + $51,975 + $3,840 = **$56,967**	₹50,400 + ₹1,940,400 + ₹168,000 = ₹2,158,800
Retail	$960 + $51,975 + $3,840 = **$56,775**	₹42,000 + ₹1,940,400 + ₹168,000 = ₹2,150,400
SaaS / Tech	$768 + $51,975 + $3,840 = **$56,583**	₹33,600 + ₹1,940,400 + ₹168,000 = ₹2,142,000

Table 6: Total operational savings from AppTrana WAAP

1. Risk Mitigation Savings from Managed WAAP

This section evaluates the cost savings achieved through AppTrana's Managed WAAP in two operational areas: DDoS monitoring and patch cycle avoidance. These savings are direct, measurable, and arise from the elimination of time spent to handle these functions.

1.1 Patch Cycle Avoidance

The biggest benefit of having a managed WAAP includes speeding up the patch cycles through virtual patches, which are compensatory controls accepted by all major regulators and compliance bodies.

1.1.1 Cost of Deploying an Application in Block Mode

To leverage virtual patching effectively, a WAAP must first be deployed in block mode with origin server protection enabled by default. AppTrana's SOC team takes responsibility for false positive testing and ensures that every deployment is moved into block mode.

Without such a managed onboarding process, in-house teams bear the cost of enabling block mode themselves. Industry benchmarks indicate that best-in-class vendors can deploy an application in approximately three days. When handled internally, however, this timeline is typically closer to six days per application due to false positive tuning, stakeholder coordination, and validation.

Even this is a conservative estimate as most industry studies state that three to six months deployment time is standard. This is largely due to false-positive tuning, stakeholder coordination, and impact validation.

	US	India
Developer	$75	₹2,800
SOC Engineer	$80	₹3,500

Table 1: Resource costs

Using the estimates above for per-hour costs, for block mode onboarding, the cost is

- **US:** 48 × $80 = **$3,840**
- **India:** 48 × ₹3,500 = ₹**168,000**

1.1.2 Cost of Patching Vulnerabilities on Code

Industry studies indicate that nearly half of all WAF deployments operate in monitoring mode, which forces application teams to patch every vulnerability directly in code.

Even when applications are deployed in block mode, there is still a gap: DAST scanners and WAAPs rarely integrate, and responsibility often falls across different teams. This lack of visibility means application teams still end up carrying a heavy code patching burden.

According to Edgescan's report, an average application enters production with 10–60 open vulnerabilities. For this analysis, we take a mid-range estimate of 35 vulnerabilities per application. With AppTrana, every application is deployed in block mode, ensuring that approximately 70% of vulnerabilities are automatically protected. Our managed services team then develops custom rules that address most of the remaining cases, leaving just 1–2 vulnerabilities per application requiring code-level fixes.

Industry research from IBM and Veracode shows that patching a single vulnerability requires 12–30 hours for root cause analysis, code changes, unit and integration testing, and QA/regression testing. Using an average of 21 hours, the total cost of code patching is calculated as:

- **US:** 33 × 21 × $75 = **$51,975**
- **India:** 33 × 21 × ₹2,800 = **₹19,40,400**

1.2 DDoS Monitoring Cost Avoidance

The next parameter is the cost avoided by preventing downtime associated with a DDoS or a bot attack.

Based on historical data, below is a table that shows the probability of a DDoS attack across various industries:

Industry	Probability serious DDoS/year
Banking & FS	40%
Insurance	35%
Healthcare	30%
Retail	25%
SaaS/Tech	20%

Table 2: Estimated probabilities of a DDoS attack across various industries

Then we multiply the above probabilities with the time it takes to recover from a DDoS attack. Usually, it is about 12 hours for monitoring, analysis, and mitigation time.

Industry	Hours/year/app
Banking & FS	4.8 hours
Insurance	4.2 hours
Healthcare	3.6 hours
Retail	3.0 hours
SaaS/Tech	2.4 hours

Table 3: Estimated time spent on attack mitigation

Then cost savings is a simple multiplication on $/hour. Based on industry data, the cost for a senior security engineer in the US is $80/hour and India is $42/hour.

Cost savings per app per year for app across industries includes:

Industry	Hours/year/app	US$/app/year	₹/app/year
Banking & FS	4.8	$384	₹16,800
Insurance	4.2	$336	₹14,700
Healthcare	3.6	$288	₹12,600
Retail	3.0	$240	₹10,500
SaaS / Tech	2.4	$192	₹8,400

Table 4: Estimated cost savings on DDoS attack mitigation

Finally, irrespective of whether an incident occurs, SOC team needs to spend time on:

1. **Monitoring dashboards** for signs of attacks
2. **Fine-tuning thresholds** and updating playbooks
3. **Running detection & response drills**
4. **Shift handovers** and status briefings
5. **Tool upkeep** (signatures, integrations, reporting)
6. **False positive investigations**
7. **Coordinating with ISPs / upstream providers** even when there is no active incident

In SOC terms, this is called "coverage factor", "operational readiness overhead", or "staffing multiplier".

In SOC staffing models, this is often expressed as:

Total SOC Hours/year = Incident Hours/year × Coverage Factor

Where:

1. **Coverage factor** accounts for **continuous monitoring + preventive work**
2. Typical range in industry: **3X to 6X** (depending on maturity and tooling)

As per SANS SOC Staffing Guide, NIST SP 800-61, and Gartner SOC TCO models, most SOC teams spend 60–80% of their time on readiness and preventive work rather than live incident handling. A multiplier of 4X, therefore, reflects realistic operational effort while staying conservative.

The updated numbers are:

Industry	Hours/year/app (incident)	Hours/year/app (with 4X Coverage Factor)	US$/app/year	₹/app/year
Banking & FS	4.8	19.2	$1,536	₹67,200
Insurance	4.2	16.8	$1,344	₹58,800
Healthcare	3.6	14.4	$1,152	₹50,400
Retail	3.0	12.0	$960	₹42,000
SaaS / Tech	2.4	9.6	$768	₹33,600

Table 5: Final estimated cost savings on DDoS attack monitoring and mitigation

Total Operational Savings from Managed WAAP

Industry	US$/app/year	₹/app/year
Banking & FS	$1,536 + $51,975 + $3,840 = **$57,351**	₹67,200 + ₹1,940,400 + ₹168,000 = **₹2,175,600**
Insurance	$1,344 + $51,975 + $3,840 = **$57,159**	₹58,800 + ₹1,940,400 + ₹168,000 = **₹2,167,200**
Healthcare	$1,152 + $51,975 + $3,840 = **$56,967**	₹50,400 + ₹1,940,400 + ₹168,000 = **₹2,158,800**
Retail	$960 + $51,975 + $3,840 = **$56,775**	₹42,000 + ₹1,940,400 + ₹168,000 = **₹2,150,400**
SaaS / Tech	$768 + $51,975 + $3,840 = **$56,583**	₹33,600 + ₹1,940,400 + ₹168,000 = **₹2,142,000**

Table 6: Total operational savings from AppTrana WAAP

2. Risk Mitigation Savings from Managed WAAP

In addition to operational savings, AppTrana delivers significant value through breach avoidance. By blocking exploit attempts on open vulnerabilities, the platform reduces the likelihood of successful breaches that can result in regulatory penalties, legal costs, and reputational damage. These estimates are based on conservative breach probability figures and industry-specific penalty benchmarks from both US and India.

In our analysis, we focused only on attacks targeting open vulnerabilities — what we call exploits. This data is directly available to customers through our Exploit Analytics feature.

Across the observed sample, each application saw more than 3 million total attacks, but the number of exploit attempts averaged 14,600 per app.

To estimate breach risk, we referred to the Verizon DBIR, which places the exploit-to-breach success rate at around 0.02%. For the ROI calculation, we halved that figure and used a 0.01% breach success rate. This translates to 1.46 expected breaches per app, per year.

Estimating breach cost

For breach costs, we looked at:

- US: IBM's 2024 Cost of a Data Breach report, which provides industry-specific breach costs including legal, remediation, notification, and downtime.
- India: Recent public enforcement actions, such as:
  - Star Health fined ₹24 crore by IRDAI (2024)
  - Kotak Mahindra Bank fined ₹1.3 crore by RBI (2023)
  - DPDPA provisions with a ₹250 crore ceiling (not yet fully enforced)

To remain conservative, we estimated India breach costs using available fines and then applied a 1/5th risk-weighting to account for infrequent enforcement and underreporting.

For SaaS/Tech, we further toned down the assumption: while IBM pegs the average cost of a breach in India at ₹19.5 crore, we believe that level of exposure would be financially unrealistic for most SaaS firms. Instead, we assumed a ₹50 lakh (₹0.5 crore) breach cost per incident. This represents reputational impact, legal fees, and customer churn without assuming regulatory penalties.

Then we looked at penalties imposed in the US and in India, where majority of world's GCCs are located. For estimates of penalties, we looked at median value if available or the latest penalty levied. Since a lot of penalties are not publicly reported, we divided the penalty found in the industry by a factor of 5.

Below is our final estimate based on breach cost/penalties avoidance per industry.

Industry	US ROI/app (US$ M)	India ROI/app (₹ crore)	Source Notes
Banking & FS	$8,880,000	₹88,00,000	RBI enforcement on Kotak and IBM databreach data for the US; conservative factor 1/5
Insurance	$8,610,000	₹99,00,000	IBM databreach data for the US and Star Health IRDAI fine (₹24 Cr) scaled down
Healthcare	$14,270,000	₹69,00,000	IBM India average breach cost (₹19.5 Cr) × 1/5
Retail	$5,080,000	₹58,00,000	DPDPA penalty assumption (₹10 Cr) scaled
SaaS / Tech	$6,800,000	₹73,00,000	Assumed ₹50L cost per breach; excludes regulatory penalties

Table 7: Breach cost avoidance per app

Even with modest assumptions:

- The **US per-app savings range from $5M to $14M,** depending on industry.
- In **India**, per-app savings range from **₹58 lakhs to ₹99 lakhs,** using actual enforcement references with a conservative risk adjustment.
- For **SaaS,** we further toned down the breach cost estimate to reflect the financial reality of smaller firms — yet even then, the ROI remains significant.
- This validates that **blocking exploit attempts,** especially those targeting open vulnerabilities, is a measurable cost-saving lever and not just a technical necessity.

3. Total Value Delivered

When operational savings and risk mitigation savings are combined, the total annual ROI per app provides a comprehensive view of the value delivered by AppTrana's Managed WAF.

For industries with higher regulatory exposure, breach-related savings represent a significant share of the total ROI. For others, operational savings alone may justify adoption.

Industry	US$/app/year	₹/app/year
Banking & FS	$8,937,351	₹10,975,600
Insurance	$8,667,159	₹12,067,200
Healthcare	$14,326,967	₹9,058,800
Retail	$5,136,775	₹7,950,400
SaaS / Tech	$6,856,583	₹9,442,000

- The **US per-app total value delivered** ranges from **$5.1M to $14.32M,** depending on industry.

- In **India,** per-app total value delivered ranges from **₹79 lakhs to ₹1.2 Cr,** using actual enforcement references with a conservative risk adjustment.

Key Assumptions

1. Patch Cycle Avoidance:

- 35 open vulnerabilities per application.
- 33 to be protected on the WAAP and 2 need fix in code
- Uses $75/hr for developers, $80/hr for SOC in US; 2,800/hr for developers, 3,500/hr for SOC in India.

2. DDoS Monitoring Savings:

- Based on lean SOC coverage model with 4× readiness multiplier (SANS/NIST benchmarks).
- 70% of apps see DDoS traffic; serious outages modeled at much lower percentage.

3. Breach Avoidance:

- Based on 0.01% breach probability applied to median/reduced penalty values from real-world cases (Kotak Mahindra, Star Health, HIPAA settlements, FTC rulings).
- SaaS/Tech penalties reduced for sustainability (most cannot absorb very high fines).

NECESSARY DEFINITIONS:

- **Cross-Site Scripting –**
    - XSS or CSS is a web application attack used to gain access to private information by delivering malicious code to end-users via trusted websites. Typically, this type of attack is successful due to a web application's lack of user input validation, allowing users to supply application code in HTML forms instead of normal text strings.
- **HTML Injection -**
    - A type of injection vulnerability occurs when a user can control an input point and can inject arbitrary HTML code into a vulnerable web page. This vulnerability leads to many consequences, like disclosure of a user's session cookies that could be used to impersonate the victim, or it can allow the attacker to modify the page content seen by the victims.
- **DDoS Attack –**
    - A distributed denial of service (DDoS) is a type of cyberattack where target web applications/ websites are slowed down or made unavailable to legitimate users by overwhelming the application/ network/ server with fake traffic.
- **Bot Attack –**
    - A botnet is the collection of malware-infected computers and networked devices (IoT, smart devices, etc.) that work together under the control of a single malicious actor or an attack group. Such a network is also known as a zombie army, and each infected device is called a bot/ zombie.

INDUSFACE™

CUSTOMER TESTIMONIALS

Kiran Belsekar

Executive Vice President - CISO & IT Governance, Bandhan Life

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

Mayuresh Purandare

Head – IT Infrastructure and Cyber Security, Marico

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.

Biswa Prasad Chakravorty

CIO, IndusInd Bank

With Indusface, we have worked together on a model that looks at different types of risks in the bank and this model scales on demand and at the same time effectively mitigate risks.

INDUSFACE IS THE ONLY CLOUD WAAP (WAF) VENDOR WITH 100% CUSTOMER RECOMMENDATION FOR 4 CONSECUTIVE YEARS

A CUSTOMERS' CHOICE FOR 2024, 2023 AND 2022 GARTNER® PEER INSIGHTS™

Gartner Peer Insights Customers' Choice 2024

INDUSFACE™

BENGALURU | VADODARA | MUMBAI | NEW DELHI | DALLAS

Contact Us - +91 265 6133000 | +1 866 458 3058

Email - sales@indusface.com | Website - www.indusface.com