INDUSFACE™

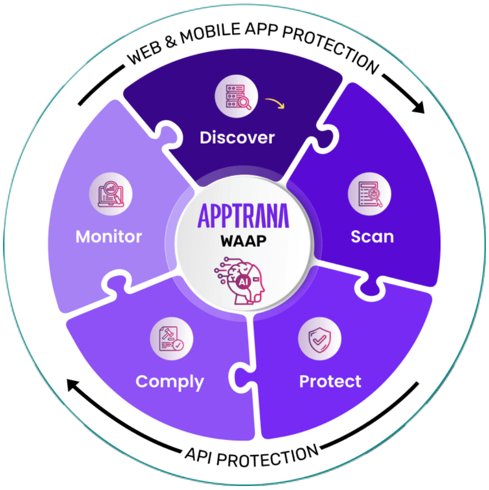
STATE OF APPLICATION SECURITY

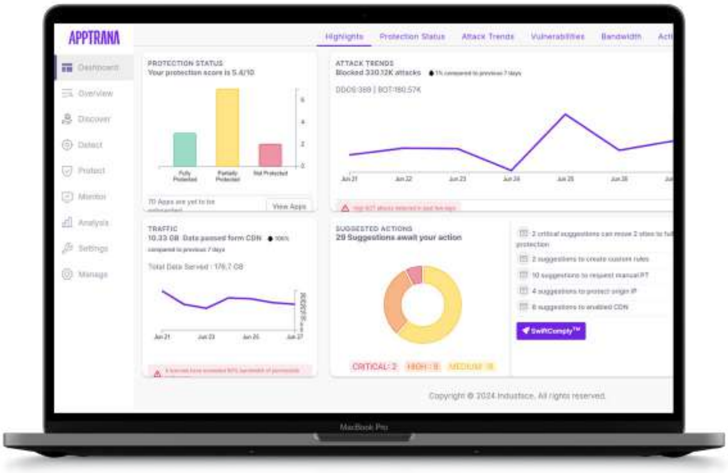
Q3 2024

INDEX

APPTRANA

AI-Powered, Fully Managed Application and API Protection





PROTECTION STATUS
Your protection score is 5.4/10

70 Apps are yet to be onboarded

ATTACK TRENDS
Blocked 330.12K attacks ● 1% compared to previous 7 days

DDOS:388 | BOT:180.57K

TRAFFIC
10.33 GB Data passed form CDN ● 100% compared to previous 7 days

Total Data Served : 176.7 GB

SUGGESTED ACTIONS
20 Suggestions await your action

2 critical suggestions can move 2 sites to full protection

2 suggestions to create custom rules

10 suggestions to request manual PT

4 suggestions to protect origin IP

6 suggestions to enabled CDN

Copyright © 2024 Indusface. All rights reserved.

START YOUR FREE TRIAL NOW

ABOUT INDUSFACE

Indusface is a leading application security SaaS company that secures critical Web, Mobile, and API applications of 5000+ global customers using its award-winning fully managed platform that integrates web application scanner, web application firewall, DDoS & BOT Mitigation, CDN, and threat intelligence engine.

Indusface, an institutionally funded firm, is the only vendor to receive 100% customer recommendation rating four years in a row and is a global customer choice in the 2024 Gartner Peer Insights™ Web Application and API Protection (WAAP) Report. Indusface is also a “Great Place to Work” 2024 certified and is PCI, ISO27001, SOC 2, GDPR certified and has been the recipient of many prestigious start-up awards.

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

Here are some of the key findings from the report:

- Over 1.26 billion attacks were blocked from 1st July 2024 to 30th Sept 2024
- On average, 903K attacks were blocked per website
- Cyberattacks grew by 26% in the Q3 of 2024 compared to the Q3 of 2023
- 271+ million API attacks in Q3 2024, where each API witnessed over 3000% higher DDoS attacks as compared to the DDoS attacks per website
- Bot attacks rose by 145% in Q3 2024 compared to Q3 2023:
    - 215+ million bot attacks in Q3 2024
    - 377+ million DDoS attacks in Q3 2024
- 6 out of 10 sites witnessed a DDoS attack, whereas 9 out of 10 sites witnessed a bot attack
- 19K critical and high vulnerabilities were found - 33% of these vulnerabilities were open for 180+ days
- Attacks on vulnerabilities grew by 124% in Q3 2024 compared to Q3 2023. A big part of this could be because of the widespread use of LLM tools such as ChatGPT enabling novice hackers to easily find and deploy scripts that could exploit open vulnerabilities
- The cyberattacks in India grew by 92% in the Q3 of 2024 compared to the Q3 of 2023
- The Small and Medium Businesses (SMB) globally faced over 354 million attacks across a sample of 500+ websites in Q3 2024
    - DDoS is the #1 attack vector for SMBs, where each website/app sees 175% higher no of DDoS attacks compared to the enterprise apps. This could be because DDoS attack monitoring requires either a managed WAAP or a specialised, 24x7 security operations centers (SOC) and SMBs can ill-afford them
- Power and energy companies faced up to 4X higher number of attacks than the industry average. This could be less regulated industries are softer targets
- SQL injection attack is the top vulnerability attack in the Banking, Financial Services, Insurance, Retail, and SMB sectors thereby reinforcing the importance of protecting critical customer data, including PII, credit card information and others that these applications host

- The banking, financial services and insurance sectors witnessed 2X higher bot attacks compared to the industry average
- 100% of healthcare sites witness a bot attack

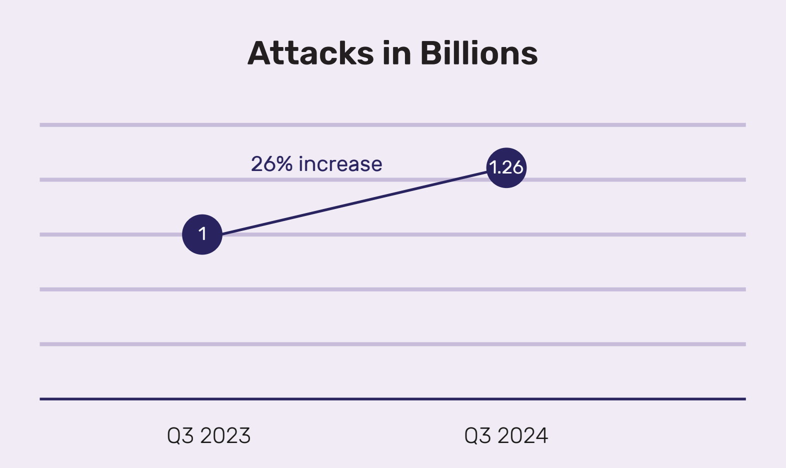
PROTECTION TRENDS:

Total Attacks Count

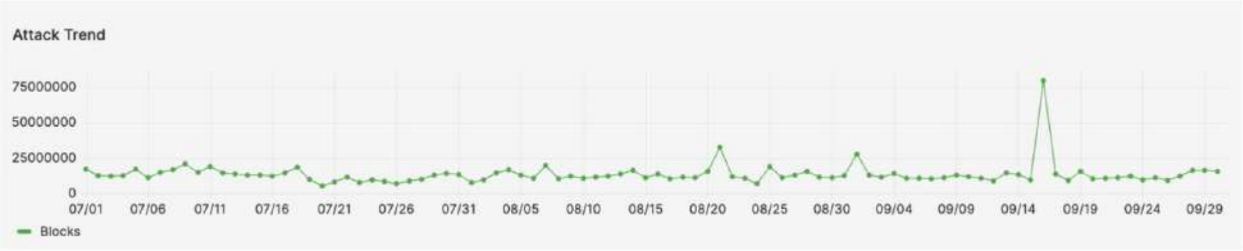
1.26+ Billion

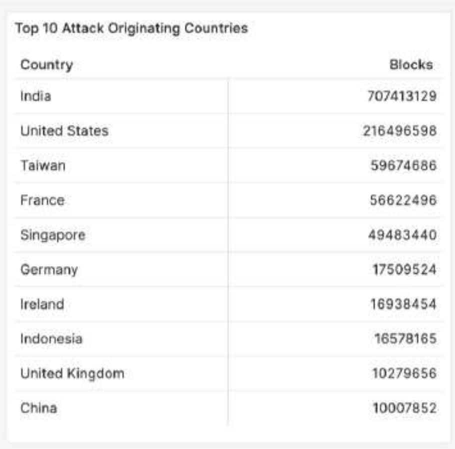
We saw over 1.26 billion requests that got blocked across all sites protected by AppTrana.

The number of attacks increased by 26% in Q3 2024 compared to Q3 2023.



A view of the last 90-day attacks' trend across all sites:

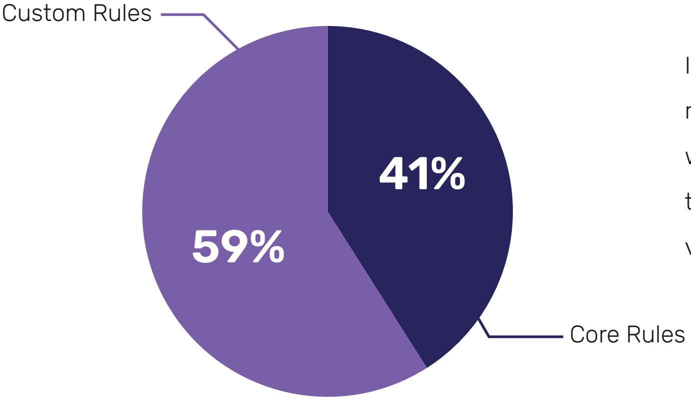




Top 10 Attack Originating Countries

Country	Blocks
India	707413129
United States	216496598
Taiwan	59674686
France	56622496
Singapore	49483440
Germany	17509524
Ireland	16938454
Indonesia	16578165
United Kingdom	10279656
China	10007852

Given most customers' business target the Indian market, many of these attacks originate within India. The next major countries from which we see attacks are the United States, Taiwan, and France.



In Q3 2024, just like last year, approximately 41% of requests were blocked by AppTrana's default rule set, while 59% were blocked by custom rules tailored to the specific needs of applications—highlighting the value of the managed services provided by AppTrana.

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 behavioural DDoS mitigation and rate-limiting based on URI, IP, host, and geo. Click here to know more
- Against bot attacks such as account takeover, credential stuffing, and scraping, AppTrana WAAP provides protection from day zero with AI-driven behavioural 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 Q3 2024:

DDoS Attacks

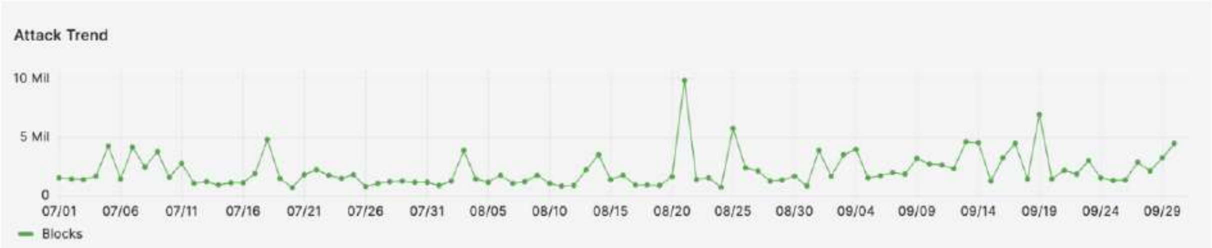
Total Sites Affected by DDoS Attacks

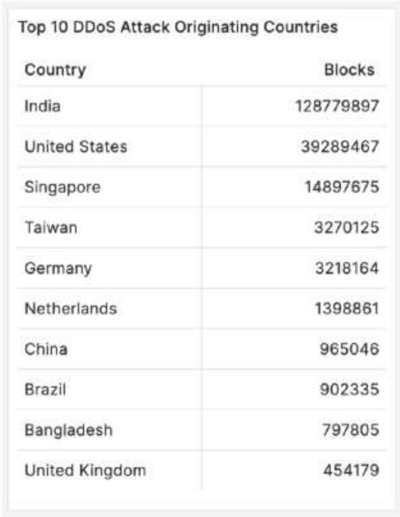
60%

Total DDoS Attacks

377+ Million

Here is a view of the last 90-day DDoS attack trend across all sites:





Top 10 DDoS Attack Originating Countries

Country	Blocks
India	128779897
United States	39289467
Singapore	14897675
Taiwan	3270125
Germany	3218164
Netherlands	1398861
China	965046
Brazil	902335
Bangladesh	797805
United Kingdom	454179

Major countries from where DDoS attacks were observed other than India are the United States, Singapore and Taiwan.

In Q3 2024, 6 out of 10 sites witnessed a DDoS attack.

Bot Attacks

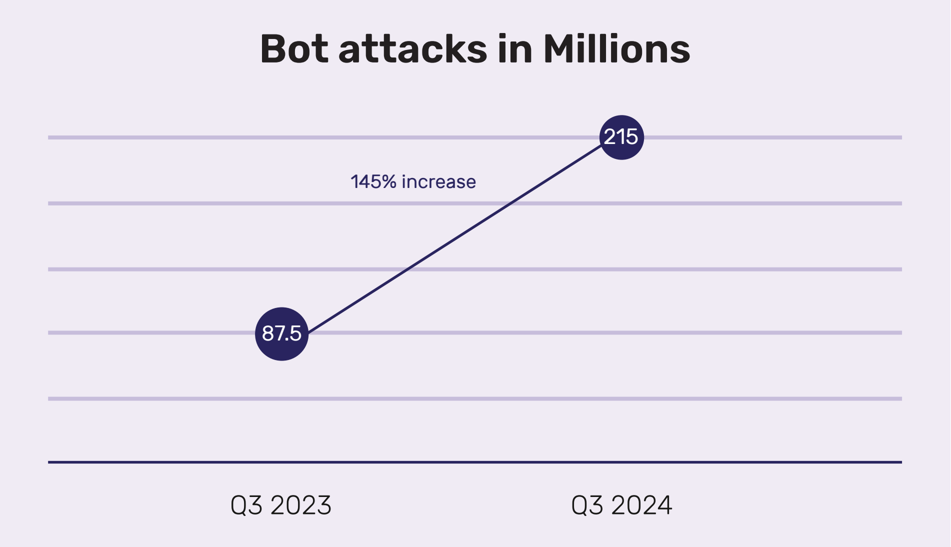
Total Sites Affected by Bot Attacks

90%

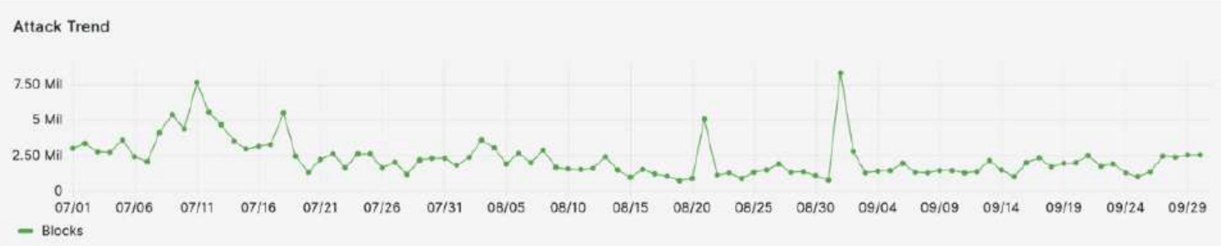
Total Bot Attacks

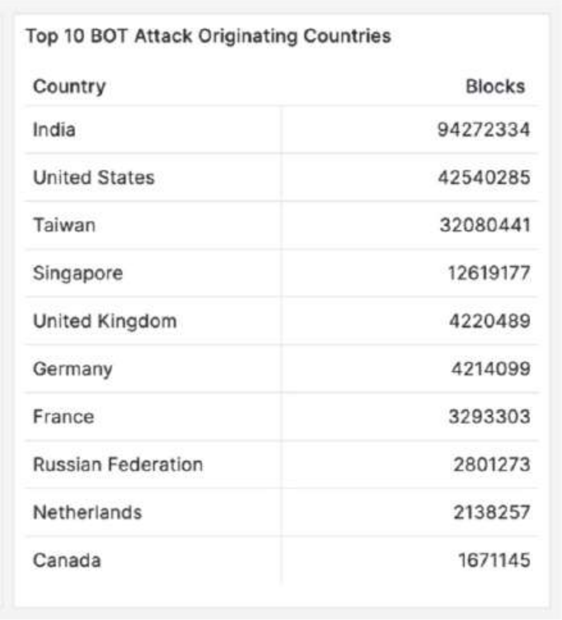
215+ Million

Here is the Q-o-Q visualisation of the bot attacks blocked in Q3 2024 vs. Q3 2023.



A view of the last 90-day bot attack trend across all sites:





Top 10 BOT Attack Originating Countries

Country	Blocks
India	94272334
United States	42540285
Taiwan	32080441
Singapore	12619177
United Kingdom	4220489
Germany	4214099
France	3293303
Russian Federation	2801273
Netherlands	2138257
Canada	1671145

Major countries from where bot attacks were observed other than India are the United States, Taiwan, Singapore and United Kingdom.

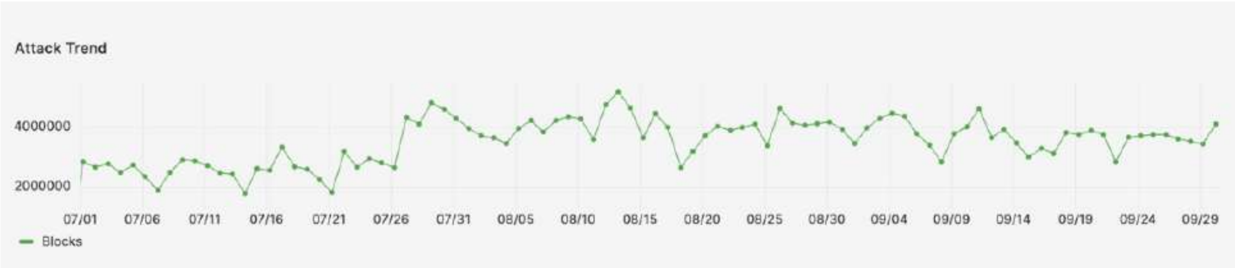
Bot attacks rose 145% compared to Q3 2023, whereas 9 out of 10 sites witnessed a bot attack

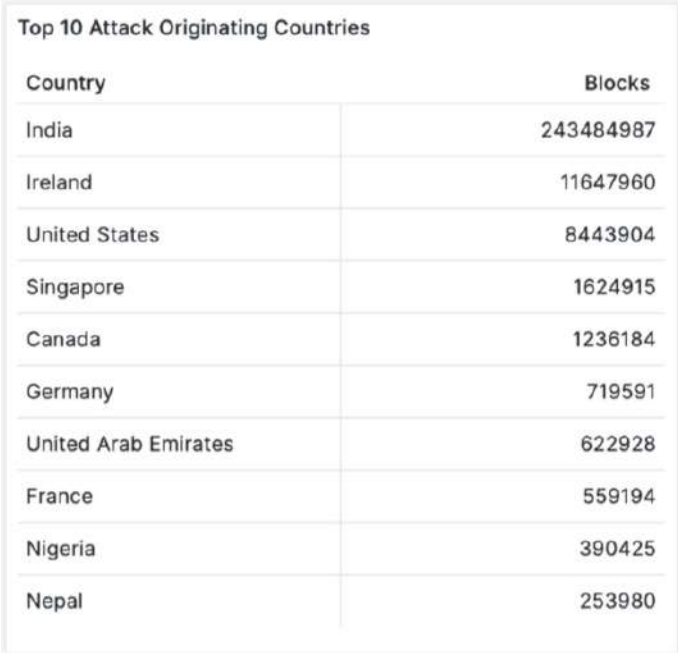
API ATTACKS

Total API Attacks

271+ Million

A view of the last 90-day API attack trend across all sites:





Top 10 Attack Originating Countries

Country	Blocks
India	243484987
Ireland	11647960
United States	8443904
Singapore	1624915
Canada	1236184
Germany	719591
United Arab Emirates	622928
France	559194
Nigeria	390425
Nepal	253980

Major countries from where API attacks were observed other than India are Ireland, the United States, Singapore and Canada.

DDoS Attacks on APIs

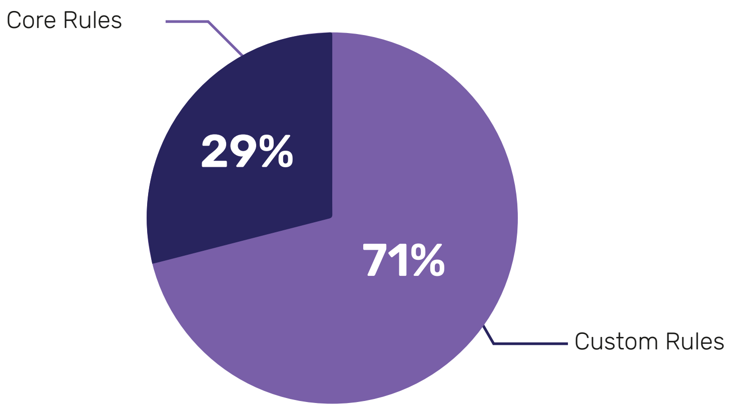
237 Million

Bot Attacks on APIs

8.9 Million

- Average Attacks witnessed per API is 85% higher compared to that of attacks per/website.
- APIs face over 3000% higher DDoS attacks compared to websites. This is alarming, especially for organizations that rely solely on API gateways for API security. As API gateways cannot provide adequate protection against advanced DDoS attacks and have weak protection measures in place against bot, zero days, and vulnerability-related attacks.
- Along with that, Custom Rules (Positive/Negative Security Policies) on APIs prove effective, as 71% of attacks are blocked via these Custom Rules. AppTrana, with its automated API discovery and one-click protection, not only saves time for organizations in documenting APIs but also provides tailored protection for each API without the need for extensive manual intervention.

Attacks Blocked - APIs



VULNERABILITY EXPLOITS

Attacks on vulnerabilities surged by **125% in Q3 2024.** A big part of this could be because of the widespread use of LLM tools such as ChatGPT, which enable novice hackers to easily find and deploy scripts that could exploit open vulnerabilities. This accessibility has lowered the barrier to entry for cybercriminals, resulting in an unprecedented rise in vulnerability exploitation.

Total no. of critical and high vulnerabilities found in the applications in Q3 2024: **19K**

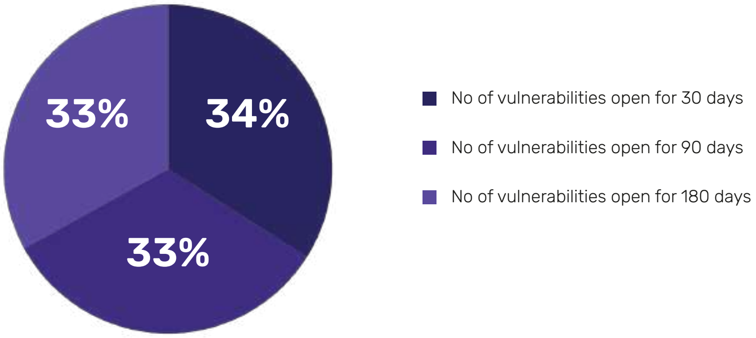
Top 5 critical and high vulnerability categories found in web applications:

#	Vulnerability Type
1	Possible Blind SQL Injection
2	Server Side Request Forgery Detected
3	HTML Injection
4	Cross-Site Scripting (XSS)
5	SQL Injection

Ageing trend of the website/application vulnerabilities

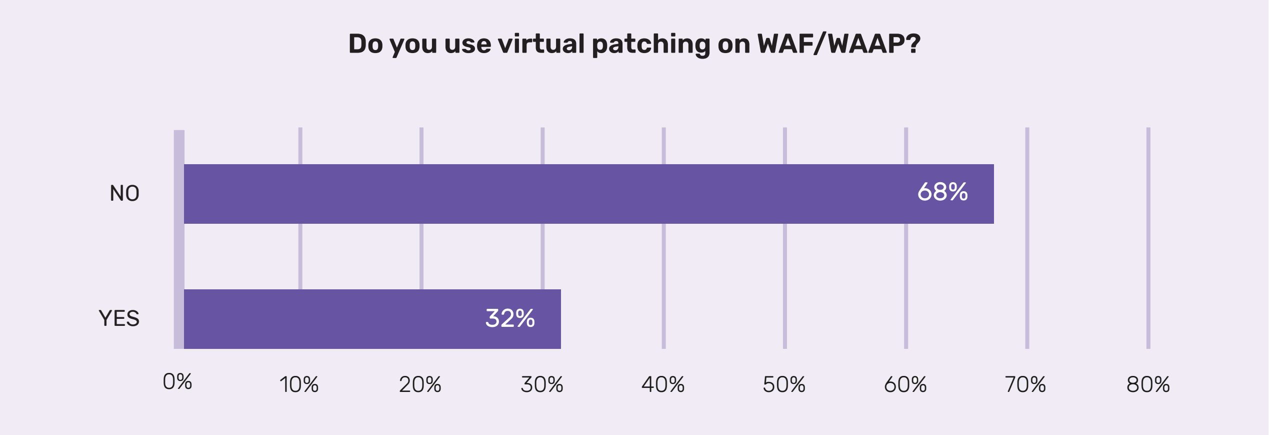
Over 1400 sites were analysed, and we found 19K critical and high vulnerabilities - around 33% of the critical and high vulnerabilities were open for more than 180 days.

Over 60% of sites with open vulnerabilities subscribed to AppTrana, faced an onslaught of over 5 million hacking attempts against these vulnerabilities. We were able to successfully mitigate these using our SwyftComply feature. In the absence of our solution, these attacks could have potentially led to losses in the billions of dollars for our customers



While the benefits of virtual patching via our SwyftComply feature are a given, we were curious to understand the adoption of this feature across the industry.

When we surveyed 300+ CISOs, CTOs, and other security leaders, a majority of whom were not our customers, it was surprising to learn that only 32% of the survey respondents used virtual patching.



This could be because most WAFs/WAAPs don't come with an integrated DAST scanner, which helps vendors understand how a vulnerability is found before patching it accurately.

Another reason could be that most of these companies do not opt for managed services, where the WAAP vendor writes the rules and removes false positives.

In contrast, we see a near 100% adoption of virtual patching among our customers, mainly because false positive testing is done by managed services that are bundled in AppTrana subscription plans.

That said, prioritising which vulnerabilities to patch and fixing the vulnerabilities in code is a major challenge for organisations and the below graph explains the same:

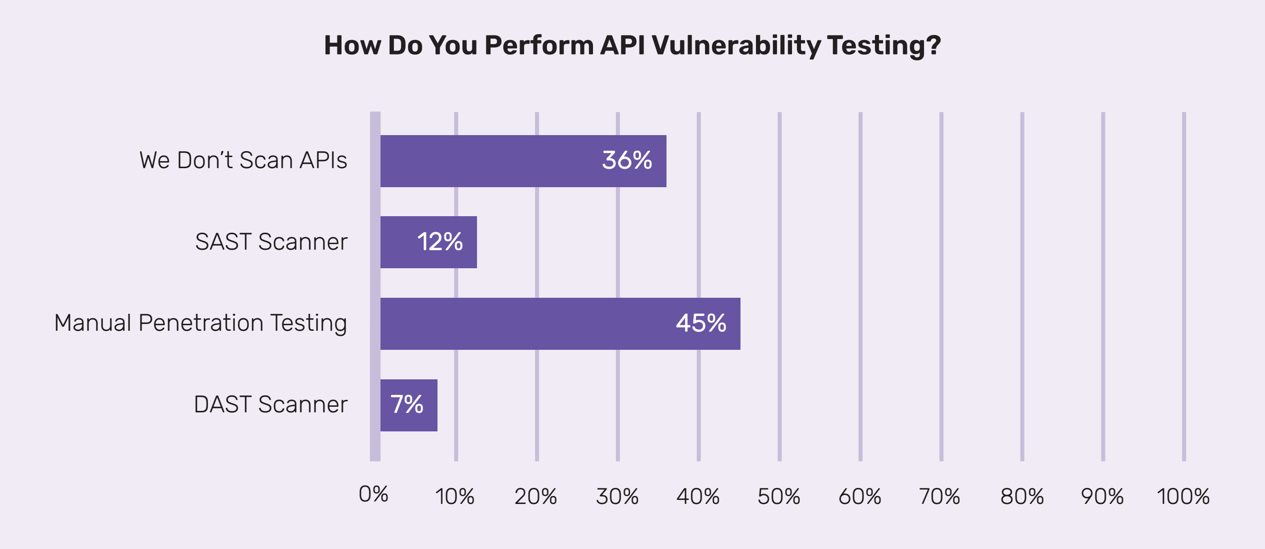
Top OWASP API vulnerability categories found:

#	API Vulnerability Type
1	A5: Security Misconfiguration
2	A7: Identification and Authentication Failures
3	A3: Injection
4	A2: Cryptographic Failures
5	A1: Broken Access Control

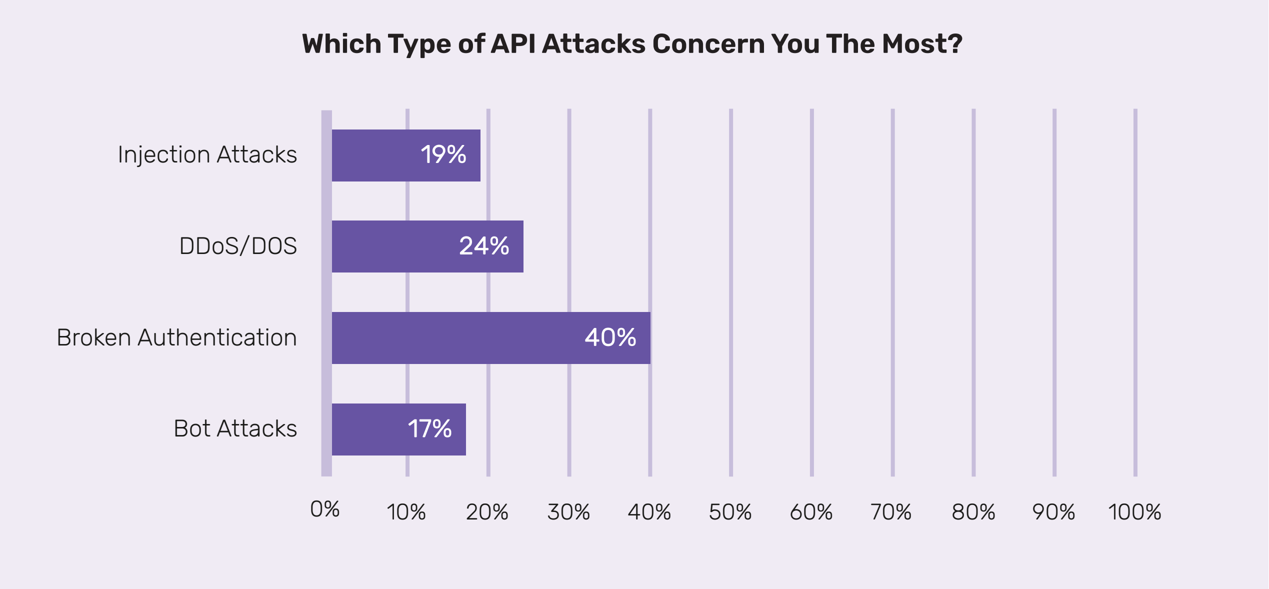
We asked the security leaders to understand what types of testing methods they perform to protect against API-specific vulnerabilities. It was surprising to know that around 36% of organizations don't even scan APIs, and only 7% of them utilize automated DAST scanners, which may be one of the easiest ways to scan APIs for vulnerabilities.

While performing penetration testing is a best practice, it is often expensive, time-taking and mostly done once a year.

Indusface's DAST scanner for APIs typically finds 90%+ vulnerabilities found in manual penetration testing and completes in a couple of hours. The other nifty feature is CI/CD integration, with which you can automatically trigger a scan with code-check-in and assign open vulnerabilities to the dev team to patch them on time.



We also tried to understand which types of API attacks concern the security leaders the most, and broken authentication emerged as the top attack vector across organizations.

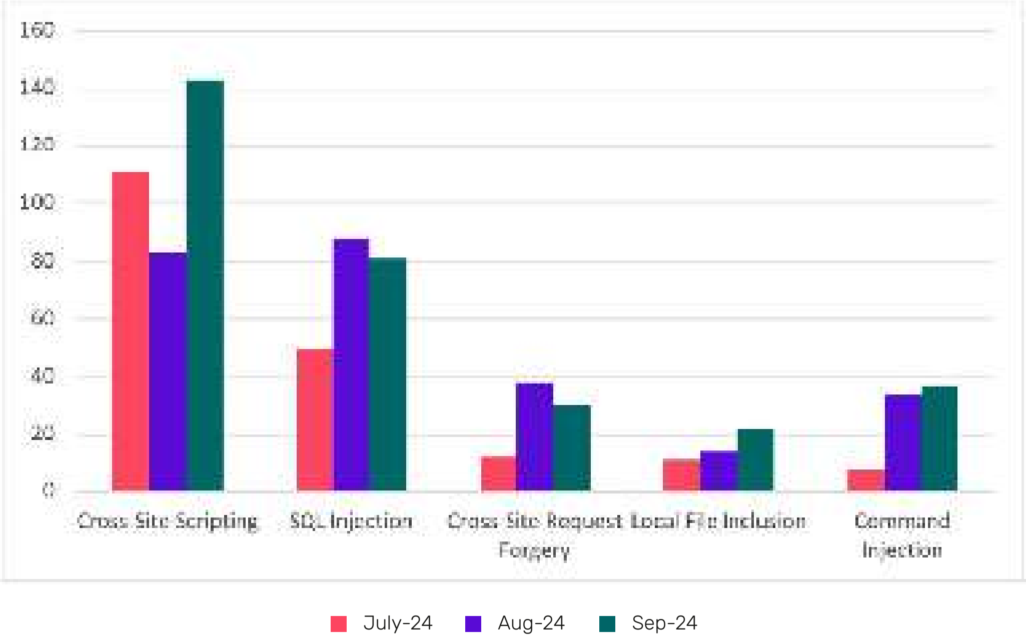


Zero Day Vulnerabilities

In Q3 2024, **779** zero-day vulnerabilities were identified for the websites protected by the AppTrana WAAP.

Most of our customers have utilized the risk-based protection of AppTrana, which has ensured the detection and protection of zero-day vulnerabilities. By default, around 98% of zero-day vulnerabilities were protected by core rules, while the remaining 2% were safeguarded by custom rules, **resulting in 100% protection from zero-day** vulnerabilities throughout the year.

Top 5 zero-day vulnerability categories in Q3 2024:



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

Month	July		Aug		Sep	
Parameters	Value	Percentage	Value	Percentage	Value	Percentage
Total Vulnerabilities	200		266		313	
Protected by Core Rules	189	96%	258	97%	313	100%
Protected by Custom Rules	11	4%	8	3%	0	0%

In Q3 2024, CVE-2024-38856, CVE-2024-36104 and CVE-2024-32113 (Incorrect Authorization vulnerability leading to RCE in Apache OFBiz) were the top targeted zero-day's.

GLOBAL SMALL AND MEDIUM BUSINESS (SMB) ATTACK INSIGHTS

Total SMB Sites Analysed

550+

Total Attacks Count – Global SMBs

354+ Million

- Over 354 million attacks were blocked in Q3 2024
- On average, 625K attacks were blocked for SMBs per site
- 71+ million DDoS attacks and 24.3+ million bot attacks are witnessed in the SMB sector in Q3 2024
- Compared to enterprises, SMBs see 198% higher number of overall attacks and 175% higher number of DDoS attacks per website

DDoS mitigation is complex, and it is mostly mitigated by maintaining continuous, 24/7 monitoring for application attacks. This is especially difficult for SMBs as security is mostly a part-time responsibility that falls on the tech or DevOps teams.

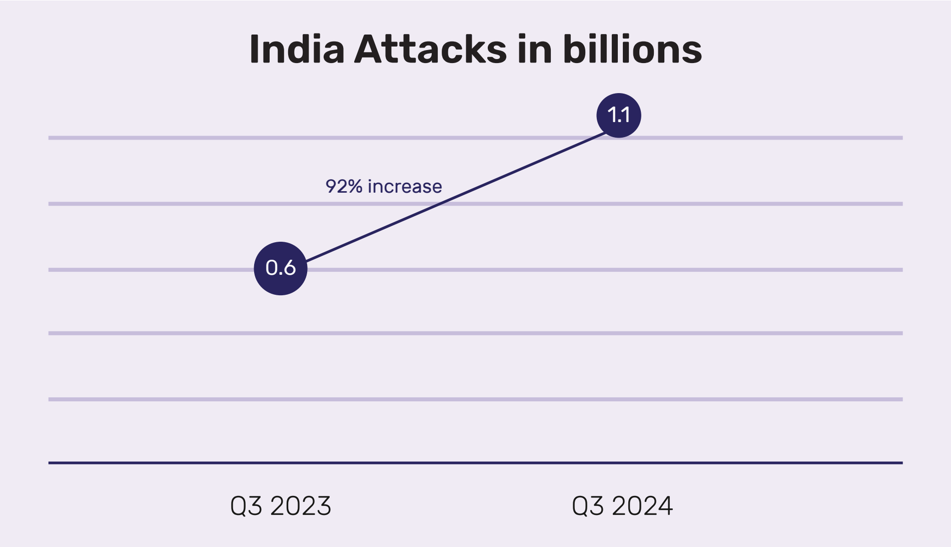
AppTrana offers a fully managed WAAP solution that is very affordable, even for SMBs. This helps them with DDoS monitoring, reduces issues related to alert fatigue, and provides support for virtual patching of open vulnerabilities.

INDIA DATA INSIGHT

Total Attacks Count - India

1.15+ Billion

- Over 1.1 billion attacks were blocked in Q3 2024
- The cyberattacks in India grew by 92% in the Q3 of 2024 compared to the Q3 of 2023



- While the DDoS attacks in India was similar to the last year, there was a huge growth in the bot and vulnerability attacks in India
- Bot attacks in India have gone up by 217% in Q3 2024 vs Q3 2023
- And attacks on vulnerabilities in India have increased by 171%. This could again be correlated with the widespread use of LLM tools, as discussed above.

Industry-Wise Data Trends

BFSI:

- The BFSI sector sees 2X higher attacks per site compared to the global average
- SQL injection attack is the top vulnerability attack in the Banking, Financial Services, and Insurance sectors thereby reinforcing the importance of protecting critical customer data, including PII, credit card information, and others that these applications host
- The BFSI sector also witnessed 2X higher bot attacks per site than the average. The highly regulated nature of these sectors means that the applications already have a robust infrastructure for cybersecurity. This could be one reason why they are targeted by bots more than other attack vectors such as DDoS. Bots are tougher to detect and could be used for a variety of exploits, including vulnerability scanning, account takeover, credit card scams, and so on
- BFSI sees the highest number of attacks blocked via Custom Rules as compared to other industries, i.e. 135 Mn+

Healthcare:

- 100% of healthcare sites witness a bot attack
- The healthcare sector sees the highest dependency on custom rules i.e. over 80% of requests are blocked by application-specific custom rules

Retail & E-Commerce:

- Retail industries face 50% more bot and vulnerability attacks as compared to DDoS attacks
- The most common bot attacks on retail and e-commerce sites are credential stuffing and carding. Both these bots essentially try to place orders and commit purchase fraud

Power & Energy:

- Power & Energy sees 4X higher attacks per website compared to the average, with an average of 1.9 million attacks per site
- This is due to hackers now seeking ransom opportunities and targeting less regulated industries with strong revenue streams.

Manufacturing:

- Manufacturing industries mainly were targeted to disrupt their internal functions such as supply chain management, spares, QA and production functions & other ERP-specific activities.
- Unlike BFSI and healthcare, which typically host sensitive PII and other data, the manufacturing industry has less sensitive data that could be exploited for ransom. Hence, hackers are finding ways to disrupt the operations significantly and making ways for them to demand a ransom.

CUSTOMER ATTACK STORY OF THE QUARTER

Mitigating Targeted Browser-Based Bot Submission Attacks

Summary:

- Over **200,000** false **insurance claim submissions were blocked**
- **Bot attacks from 100,000+ IPs/Day and browser-based automated tools**
- Deployed AI-recommended, time-based rate-limiting measures to block hackers from submitting forms at **abnormal rates**

About the Customer:

The customer is a decade-old firm based in California, USA, specializing in legal, fiduciary, and administrative services. They specialize in Corporate Restructuring, Mass Tort, Settlement Administration, and Trustee and Fiduciary Services.

Key Challenges:

- The behavioural AI model found anomalies with the "Insurance Settlement Administration" page, where a hacker was persistently submitting bot-driven insurance claims
- This was relayed out to the customer in real-time to check the veracity of the findings. The customer confirmed and noted that this could have resulted in hundreds of thousands of claim submission requests flooding the system in a short time, making it difficult for employees to process claims and identify legitimate requests
- The hacker had carefully designed the bots to mimic human behavior, filling out all required details on the claim page accurately
- Additionally, identifying the bots was challenging because they were deployed through browser-based automated tools rather than command-line interface (CLI) tools
- The hacker utilized over 100,000 IP addresses, submitting more than 200,000 claims
- The attack evolved every day and the rules had to be tuned regularly while eliminating false positives

Solution:

The customer already used the behavioural bot module on AppTrana WAAP.

Once the anomaly alert triggered, the 24/7 SOC team took a quick confirmation from the customer and deployed the mitigation mechanisms.

The summary of the mitigation approach includes:

- Deploy a very low tolerance for requests per URI. Any URI exceeding this threshold was blocked
- Any signs of malicious bot activity—regardless of tools, geography, or device—were met with CAPTCHA or tarpit challenges first, and if suspicious behaviour persisted, users were blocked for extended periods
- Accept traffic solely from the geographical locations where insurance claims were permitted, blocking requests from all other locations
- Deploy time-based rate-limiting rules to block any user who filled out the form at a significantly faster rate, calculated by the behavioural AI model, than normal or submitted multiple forms within a specified time-frame

- Prevent the exploitation of any business logic vulnerabilities in the claim process, ensuring that user input—from insurance numbers to other details—was more specific and unique

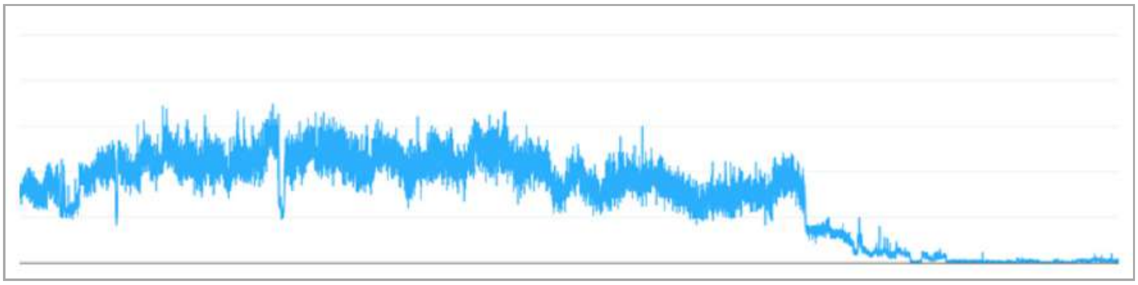
The AI model on AppTrana WAAP continuously evolved with the hackers' methods and the attacks stopped within a couple of days.

This is a classic case of human (Indusface 24/7 SOC and customer's DevOps team) and AI (behavioural bot module) working together to ensure that attacks are thwarted with minimal false positives.

AppTrana successfully blocked over 2 million targeted attacks, leading zero cases of false claims registered on the customer's site.

Results:

- Over 2 million attacks blocked in a couple of days
- Prevented potential losses of hundreds of hours and thousands of dollars lost in processing fraudulent claims
- Achieved zero false claim submissions with AppTrana WAAP
- Strengthened security measures, reducing vulnerability to future attacks

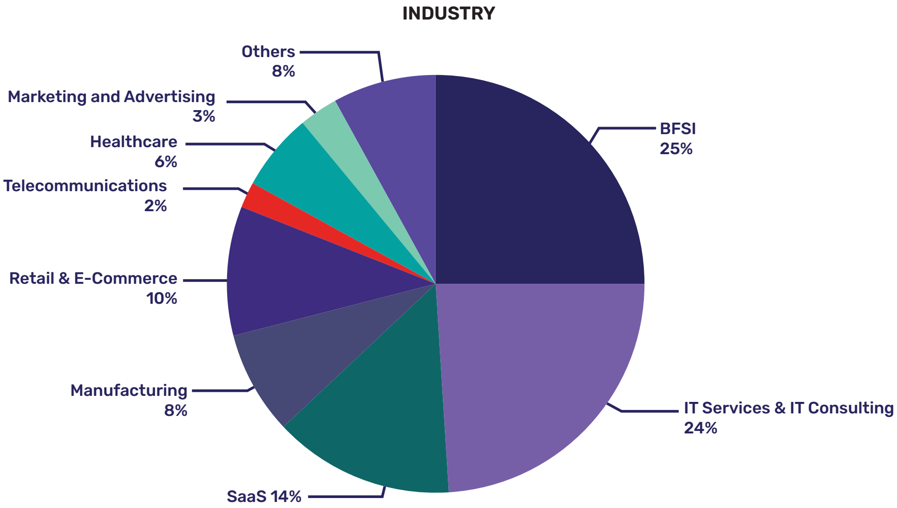


Q3 2024 RESEARCH OVERVIEW

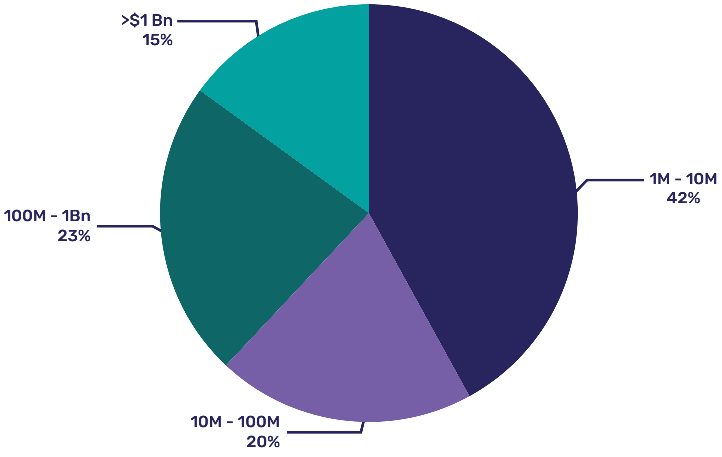
The State of Application Security Q3 2024 annual report is based on a sample size of 1400+ websites and applications that were analysed between July 1, 2024, and September 30, 2024.

During this period, various enterprise, government, and SME websites were analysed. 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.

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.

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