INDUSFACE™

2023

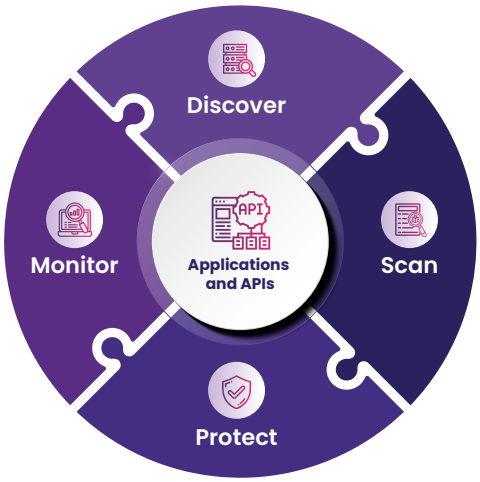
STATE OF APPLICATION SECURITY

ANNUAL REPORT

INDEX

APPTRANA

A unified platform to discover, scan, protect, and monitor your public assets & APIs in real time



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, funded by Tata Capital Growth Fund II, is the only vendor to receive 100% customer recommendation rating three years in a row and is a global customer choice in the Gartner Peer Insights™ Web Application and API Protection (WAAP) Report 2023. Indusface is also a "Great Place to Work" 2022 Winner in the Mid-Size category in India 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 3 CONSECUTIVE YEARS

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

Gartner Peer Insights Customers' Choice 2023

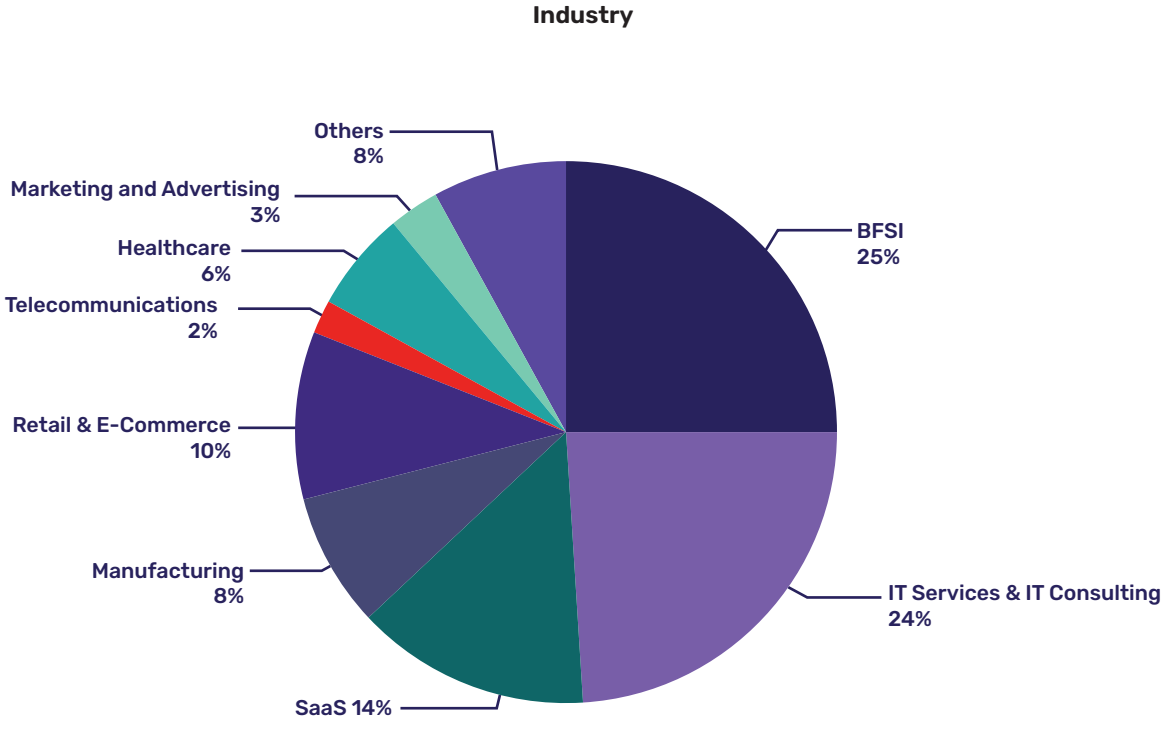
OUR CUSTOMERS

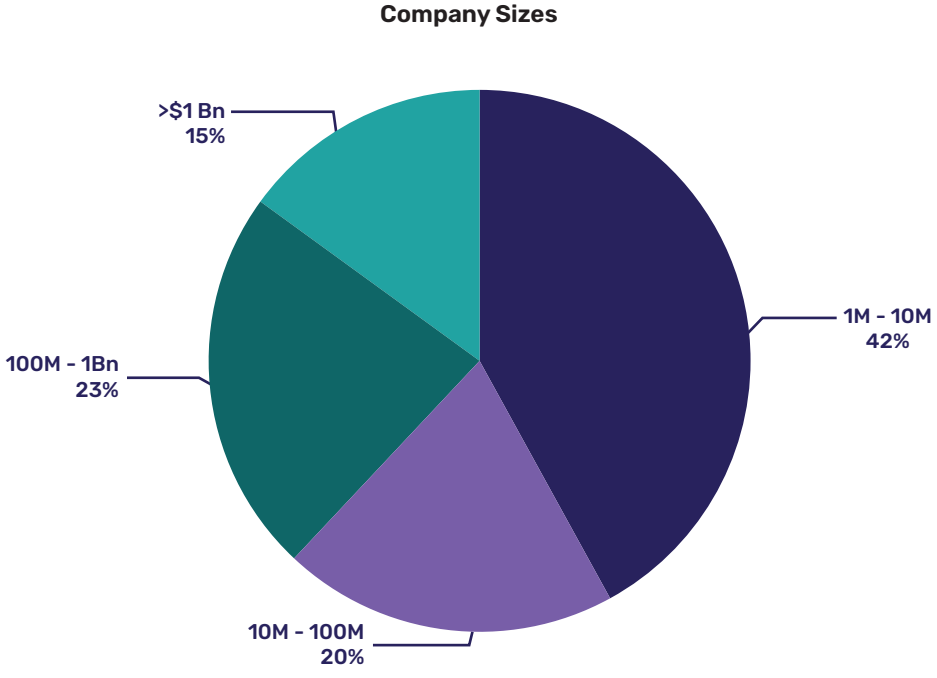
OVERVIEW

The State of Application Security 2023 annual report is based on a sample size of 1400+ websites and applications that were analysed between January 1, 2023, and December 31, 2023.

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





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.

EXECUTIVE SUMMARY

Here are some of the key findings from the report:

- Over 6.8 billion attacks were blocked from 1st Jan 2023 to 31st Dec 2023
- On average, 4.2 million attacks were blocked per website
- 5.14 billion+ attacks were from India - the cyberattacks in India grew on an average of 63% each quarter from Q1 2023 to Q4 2023
- DDoS & bot attacks rose by an average of 46% each quarter:
  - 4.25+ billion DDoS attacks in 2023
  - 467+ million bot attacks in 2023
- 4 out of 10 sites witnessed a DDoS attack, whereas 8 out of 10 sites witnessed a bot attack
- 39% of organizations aren't confident in mitigating a large-scale DDoS attack
- 29K critical and high vulnerabilities were found - 32% of these vulnerabilities were open for 180 days
- Customers are increasingly benefiting from virtual patching at the WAF level. In the last two quarters:
  - 40% of the attacks were blocked by using AppTrana's core rules set
  - 60% of the attacks were blocked using custom rules. This signifies the importance of managed services and custom rules for security teams across the world
- SaaS companies saw a 10X surge in the number of attacks as most of them deal with customer-sensitive information across multiple industries
- Over 90% of banking, finance, and insurance sites witnessed a bot attack throughout the year
- 100% of healthcare sites witnessed a bot attack
- A significant increase in the botnet-driven low-rate HTTP DDoS was seen in 2023, along with carding attacks for retail and e-commerce industries
- The top DDoS attack countries were India, the United States, and the UK
- Other than India, the major countries where bot attacks were observed were the United States, Russia, and the UK.

VULNERABILITY EXPLOITS

Total no. of critical and high vulnerabilities found in the applications: 29K

Top 10 critical and high vulnerability categories found:

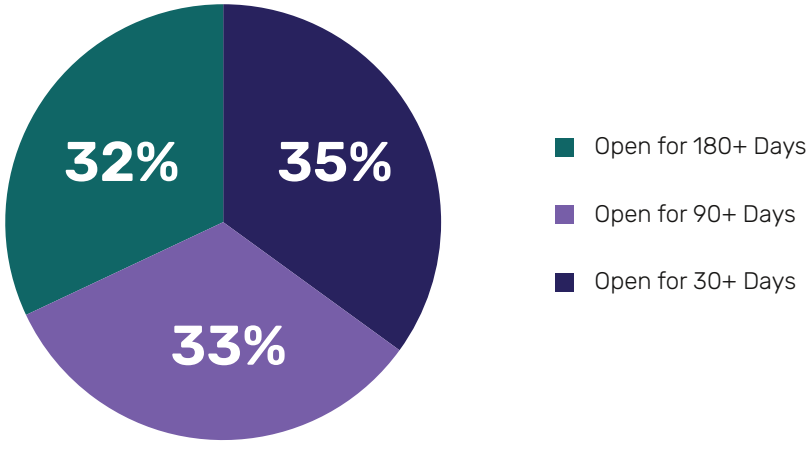
VULNERABILITY TYPE	TOTAL ALERTS FOUND
Malicious Content Found (Software and Data Integrity Failures)	9319
Server-side Request Forgery Detected	2496
Cross-Site Scripting (XSS)	2010
HTML Injection	1615
TLS/SSL Server Certificate Will Expire Soon	1259
Script Source Code Disclosure	418
SQL Injection	261
SSL Certificate Common Name Mismatch	197
Invalid TLS/SSL Server Certificate	181
EPMM Authentication Bypass	124

AGING TREND OF THE WEBSITE/APPLICATION VULNERABILITIES

Over 1400 sites were analysed, and we found 29K critical and high vulnerabilities - around 32% of the critical and high vulnerabilities were open for more than 180 days.

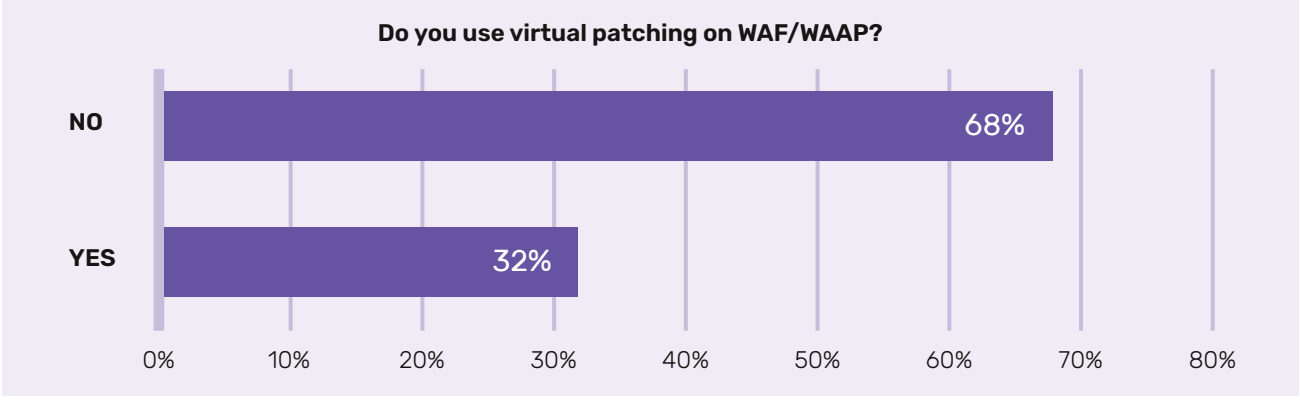
With AppTrana, customers ensured that vulnerabilities were virtually patched immediately, reducing the time to fix them, thereby ensuring that the security team becomes an enabler of business instead of a blocker.

Open Vulnerability in Days



While the benefits of virtual patching 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.

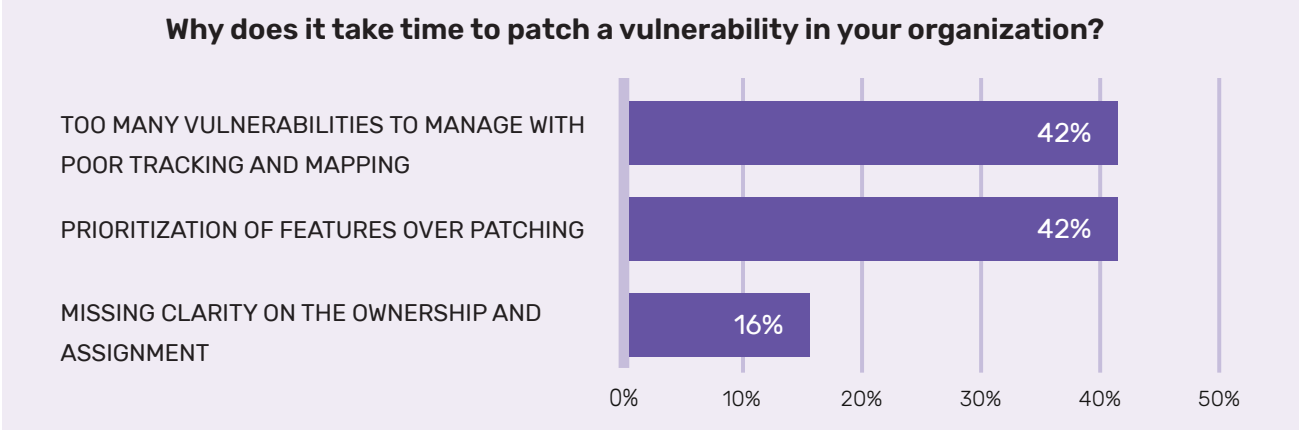


This could be because most of the WAFs/WAAPs don't come with an integrated DAST scanner, which helps the vendors understand how a vulnerability is found before patching it accurately.

And another reason could be because 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 managed services are bundled in our WAAP subscription plans.

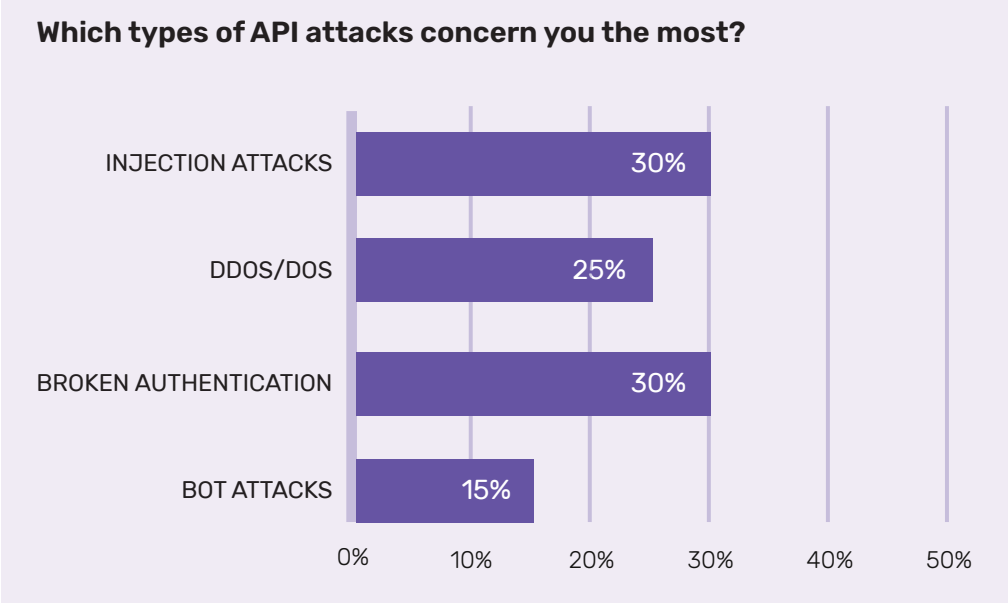
That said, patching these vulnerabilities in code is a major challenge, and the following graph explains these challenges.



Top 10 API vulnerability categories found:

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

Here are the survey answers provided by the security leaders when asked about their challenges related to APIs:



As per the survey, injection attacks and broken authentication attacks are concerning most organizations globally.

Zero Day Vulnerabilities

In the entire year, **3324 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, more than 96% of zero-day vulnerabilities were protected by core rules, while the remaining 4% were safeguarded by custom rules, **resulting in 100% protection from zero-day** vulnerabilities throughout the year.

Top 5 zero-day vulnerability categories in 2023:

Zero-day vulnerability category	Count
Cross-Site Scripting	1480
SQL Injection	915
Command Injection	302
CSRF	224
Local File Inclusion	210

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

Month	Jan		Feb		Mar		Apr		May		Jun	
Total Vulnerabilities	294		311		346		287		314		266	
Parameters	Value	%	Value	%	Value	%	Value	%	Value	%	Value	%
Protected by Core Rules	287	98%	300	96%	346	100%	274	95%	300	96%	248	93%
Protected by Custom Rules	7	2%	11	4%	0	0	12	5%	14	4%	18	7%
Month	**Jul**		**Aug**		**Sep**		**Oct**		**Nov**		**Dec**	
Total Vulnerabilities	266		210		222		251		334		222	
Parameters	Value	%	Value	%	Value	%	Value	%	Value	%	Value	%
Protected by Core Rules	242	91%	195	93%	214	96%	236	94%	334	100%	222	100%
Protected by Custom Rules	24	9%	5	7%	8	4%	15	6%	0	0	0	0

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

- Apache OFBiz Authentication Bypass (CVE-2023-49070 and CVE-2023-51467)
- Apache Struts 2 Vulnerability CVE-2023-50164
- Zimbra Cross-Site Scripting Flaw (CVE-2023-37580)
- HTTP/2 Rapid Reset Attack Vulnerability
- Remote Unauthenticated API Access Vulnerabilities in Ivanti (CVE-2023-35078)
- An actively exploited zero-day vulnerability (CVE-2023-35081) affecting Endpoint Manager Mobile (EPMM)
- Adobe ColdFusion Vulnerabilities (CVE-2023-29300)
- A critical privilege escalation vulnerability in WordPress (CVE-2023-28121).

The exploits targeting these vulnerabilities were mitigated out of the box on AppTrana WAAP.

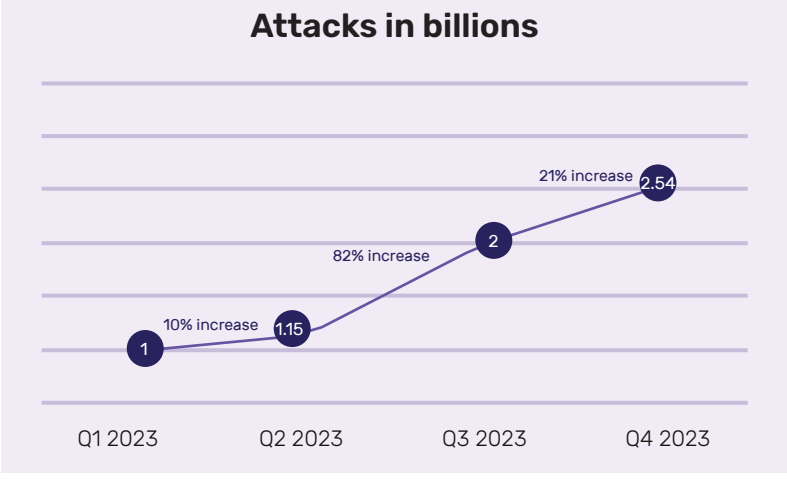
PROTECTION TRENDS

Total Attacks Count

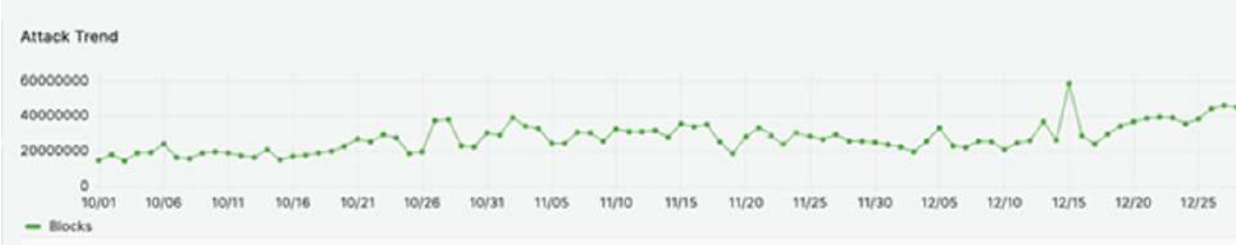
6,869,252,996

We saw over 6.86 billion requests that got blocked across all sites protected by AppTrana. The number of attacks increased by an average of 38% each quarter.

Here is the Q-o-Q visualization on the attack trends from Q1 2023 to Q4 2023:



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

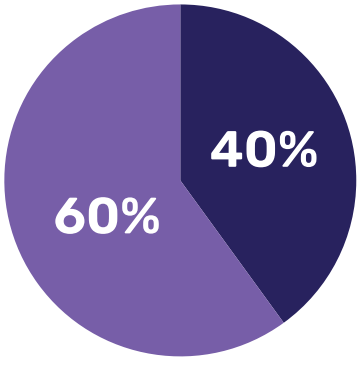


Top 10 Attack Originating Countries

India	215973683
United States	18718472
United Kingdom	3946085
Russian Federation	1975526
Germany	1226703
Singapore	944070
Thailand	907880
France	769779
Australia	744651
Finland	714738

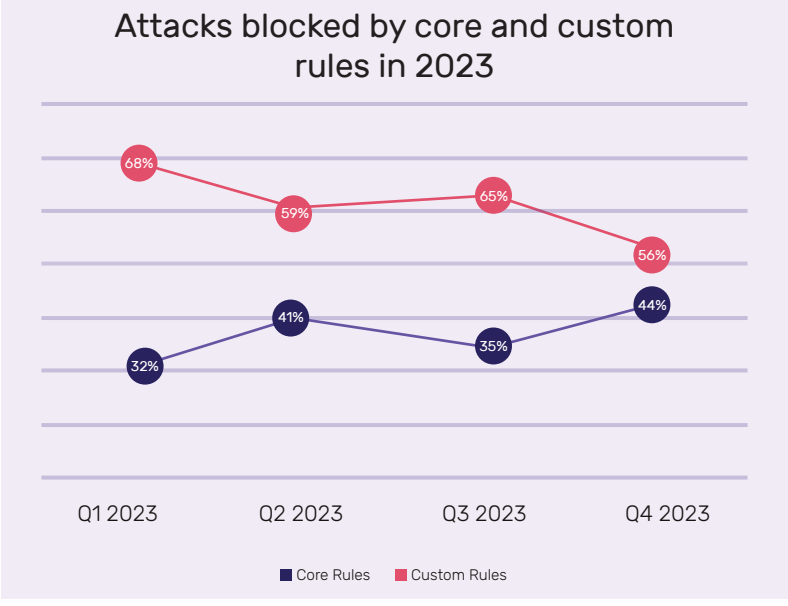
On average, we see about 4.2Mn requests - blocked across all sites protected by AppTrana.

Given most customers' business is targeting Indian markets, many these attacks originate from India. The next major country we see attacks from is the United States, the UK and Russia.



In the last two quarters 40% of requests were blocked by AppTrana's default rule set, and **60% of requests were blocked by custom rules** created based on the specific needs of applications - highlighting the value of managed services that AppTrana provides.

Here is the Q-o-Q visualization on the attack blocked by core and custom rules in each quarter of 2023.



Within core rules, rudimentary attacks are still prevalent, and around 30% of attacks are just getting blocked via malicious user agents and IP rules.

DDOS & BOT ATTACKS

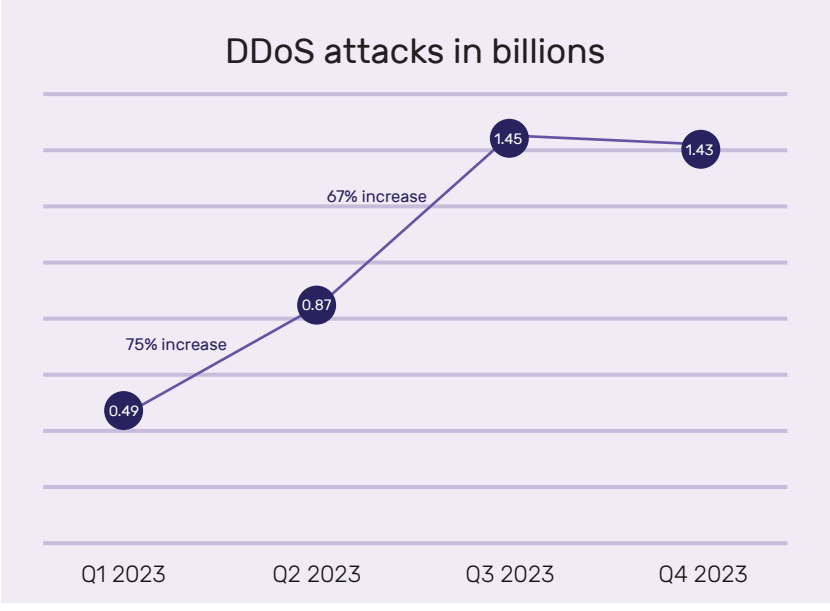
- As new attack trends of DDoS and bot attacks emerge against web applications and APIs, business continuity becomes very important.
  - AppTrana WAAP guarantees zero false positives and ensures 99.99% uptime against layer 3-7 DDoS attacks with behavioural DDoS mitigation, AI-based rate-limiting based 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 behavioural & real-time visibility and 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 2023:

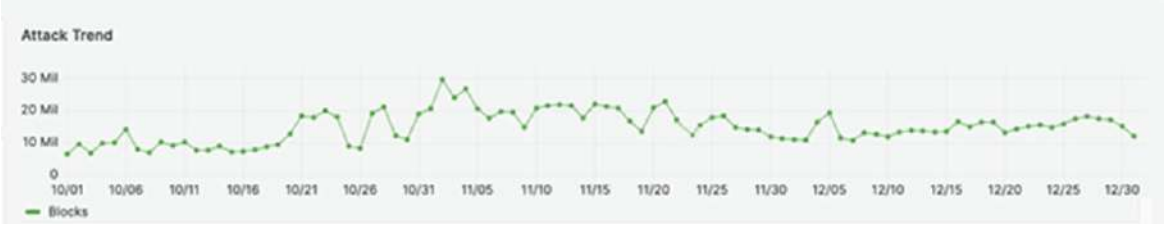
DDoS Attacks

Total Sites Affected by DDoS Attacks	Total DDoS Attacks
709	**4.25+ Billion**

Here is the Q-o-Q visualization on the DDoS attack blocked in each quarter of 2023.



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



Top 10 DDoS Attack Originating Countries

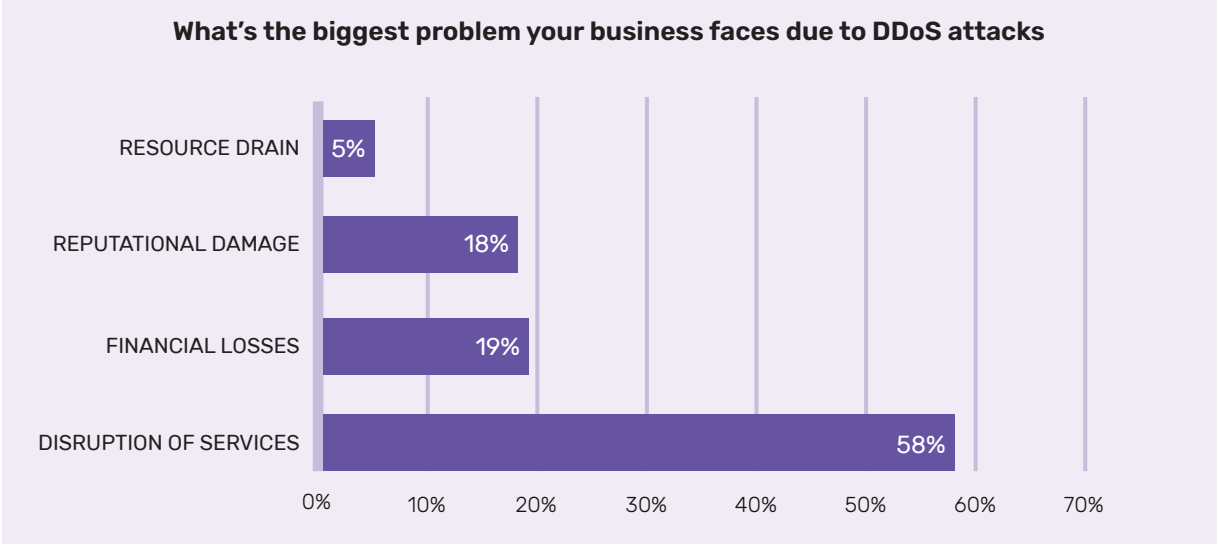
Country	Blocks
India	128951104
United Kingdom	2107517
United States	2107016
Thailand	260003
Singapore	236723
Germany	229757
United Arab Emirates	214979
Netherlands	180958
France	117932
Finland	113415

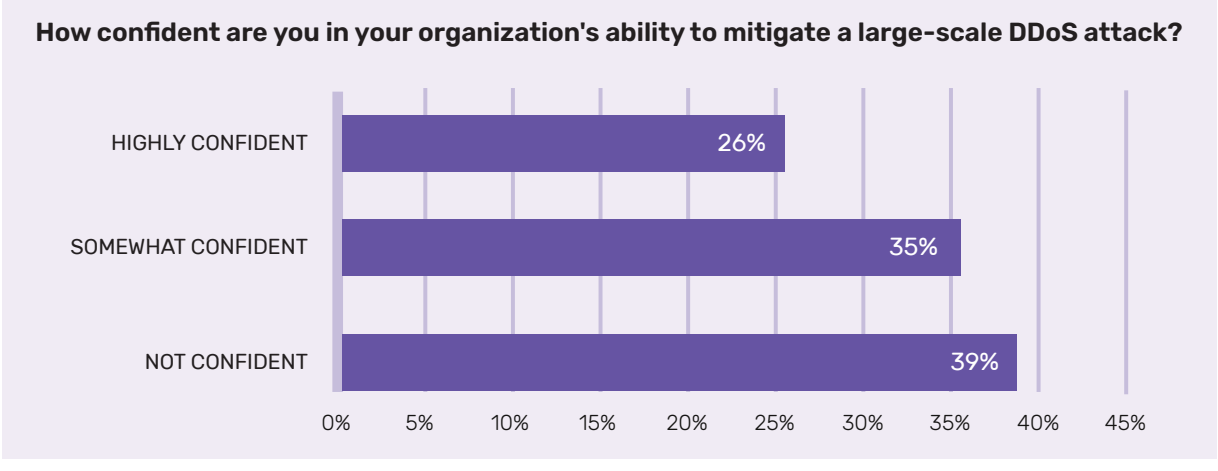
Major countries from where DDoS attacks were observed other than India are the United States, and the UK.

DDoS attacks rose by an average of 46% each quarter, where 4 out of 10 sites witnessed a DDoS attack.

After asking 100+ CISOs, CTOs, and other security leaders outside of our customer base, here's what they had to say about their challenges in managing DDoS attacks.

Here are the survey answers provided by the security leaders after being asked about their challenges with DDoS attacks:



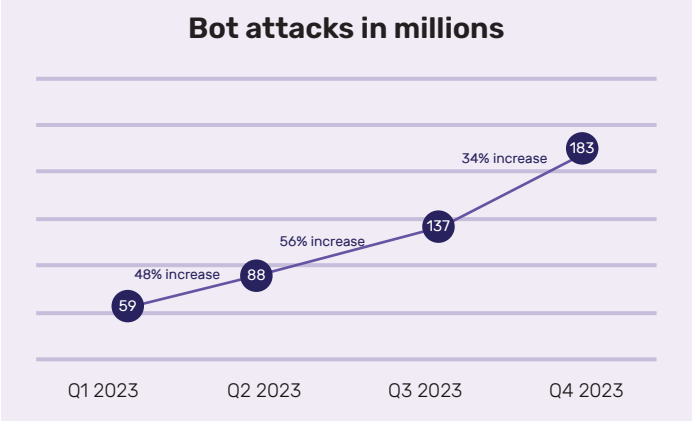


58% of leaders have identified service disruption as the biggest challenge resulting from DDoS attacks. Moreover, only 26% of the surveyed individuals expressed confidence in their WAF/WAAP solutions to safeguard their businesses from large-scale DDoS attacks.

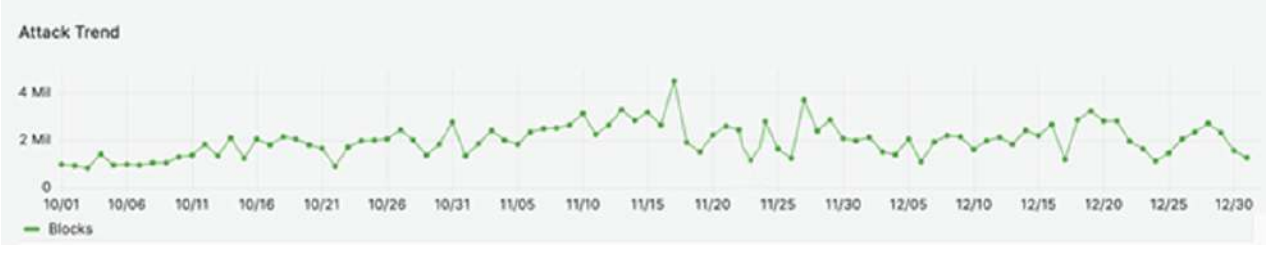
BOT ATTACKS

Total Sites Affected by Bot Attacks	Total Bot Attacks
1348	**467+ Million**

Here is the Q-o-Q visualization on the bot attack blocked in each quarter of 2023.



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



Top 10 BOT Attack Originating Countries

Country	Blocks
India	8744486
United States	4851243
Russian Federation	899702
United Kingdom	795855
Germany	678834
Finland	374566
Hong Kong	254938
France	194646
Netherlands	183368
Canada	149646

Major countries from where bot attacks were observed other than India are the United States, Russia, and the UK.

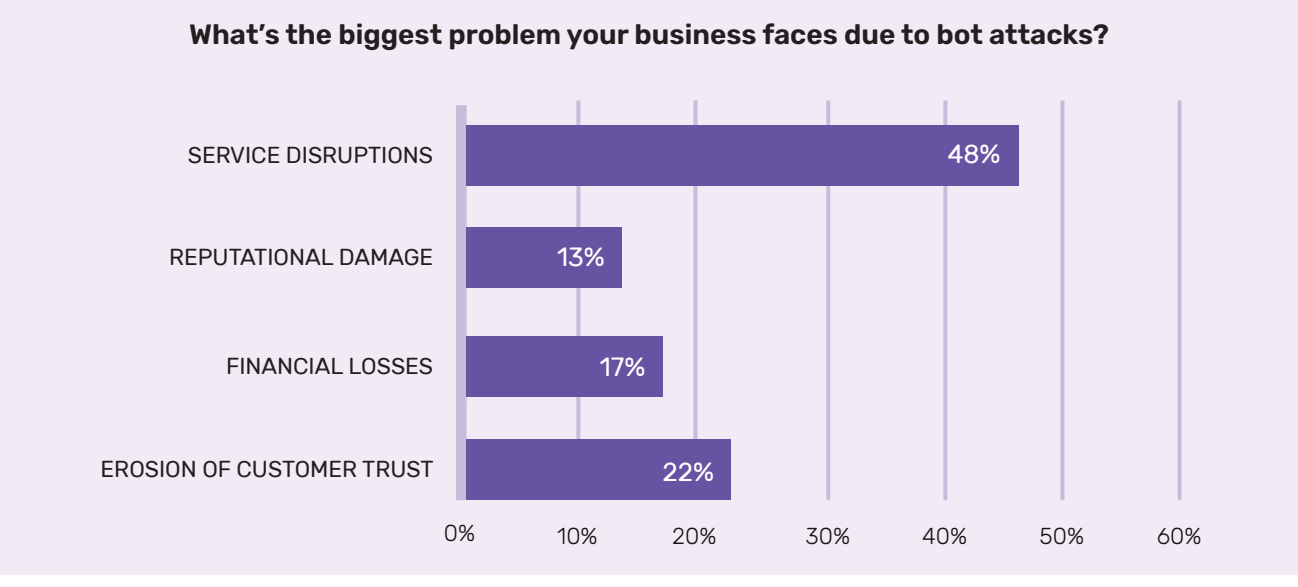
Bot attacks rose by an average of 46% each quarter, where 8 out of 10 sites witnessed a bot attack.

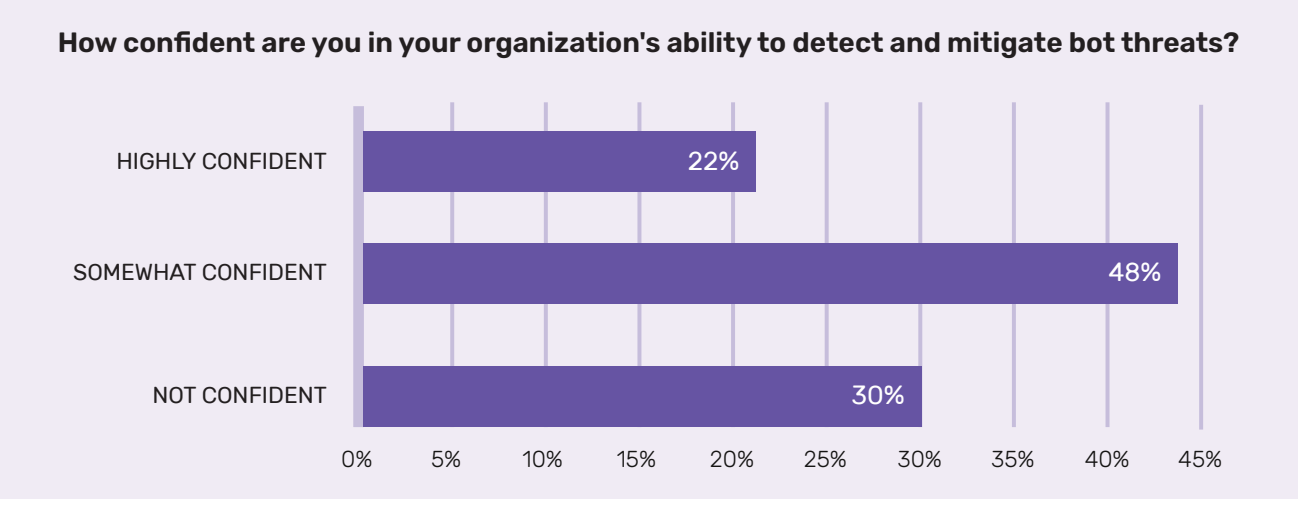
In the year 2023, a significant increase in botnet-driven low-rate HTTP DDoS attacks was witnessed.

These attacks were carried out by using botnets to send a large number of HTTP requests to a target web server/application over a long period of time. These attacks were designed to be stealthy and persistent, with each bot sending requests at a low rate to avoid detection.

AppTrana's custom rules made sure that these attacks were thwarted in a short span of time, ensuring 100% availability of the sites.

Here are the survey answers provided by the security leaders (outside of our customer base) after being asked about their challenges with bot attacks:





According to 48% of leaders, the biggest challenge resulting from bot attacks is service disruption. Only 22% of surveyed individuals expressed confidence in their WAF/WAAP solutions to detect and protect their businesses from various bot attacks.

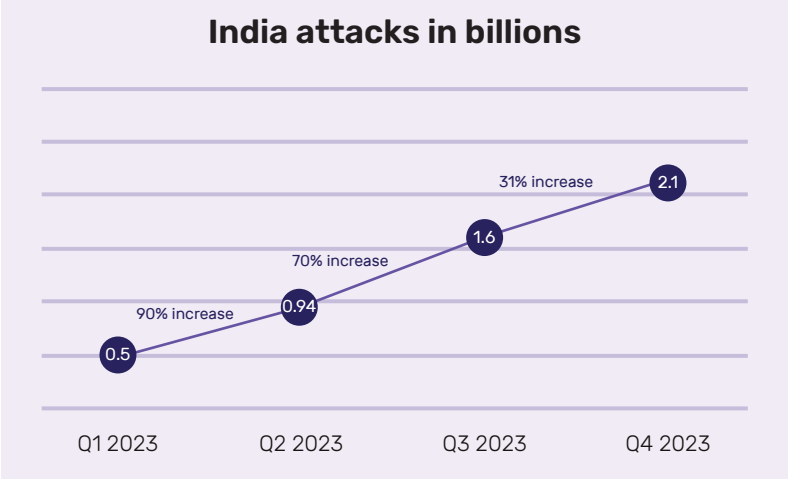
INDIA DATA INSIGHTS

Total Attacks Count - India

5.14 Billion

- Over 5.14 billion attacks were blocked in the year 2023
- The cyberattacks in India grew on an average of 63% each quarter from Q1 2023 to Q4 2023

Here is the Q-o-Q visualization on the India attack trends from Q1 2023 to Q4 2023:



- In the last two quarters, SaaS companies saw a 10X surge in the number of attacks as most of them deal with customer-sensitive information across multiple industries

- Over 90% of BFSI sites witnessed a bot attack throughout the year, and the number of overall attacks increased by an average of 40% each quarter

- In the entire year, the healthcare sector has seen the highest increase (3X growth) in cyberattacks, with 100% of healthcare sites witnessing a bot attack

- A significant increase in the botnet-driven low-rate HTTP DDoS was seen in 2023, along with carding attacks for retail and e-commerce industries

A CUSTOMER ATTACK STORY IN 2023

Mitigating Carding Attacks for a US-Based Leading Jewellery Company

Solution Highlights:

- Carding attacks were carried out from **varying IP addresses**
- Over **16K attack requests** were blocked
- **Human-led** attacks instead of bot-led attacks
- "**Zero**" fake **orders** punched

Key Challenges:

- The customer faced persistent and frequent carding attacks (also known as credit card stuffing/card verification attacks) on their application.
- A carding attack is an attack where attackers **use stolen/fake credit card information** and try to make online purchases.
- Similarly, in this situation, the attacker(s) utilized multiple fake/stolen credit card details along with randomly generated fake email addresses and tried to make a purchase.
- A worrisome concern for the customer was that the attacker could even place around **15 fake orders** from their site by following this process.
- Being in the jewellery business, the customer urgently needed a solution to mitigate these carding attacks quickly, as it posed **substantial financial losses** due to these unauthorized transactions, thereby **impacting their reputation** with third-party payment providers.

Strategy & Recommended Solution:

- The customer contacted the Indusface team and was able to deploy the AppTrana solution within 60 minutes of the request.
- After deployment, the managed services of the Indusface reached out to the customer to identify the attack parameters in detail, and to deploy the necessary solutions.
- A noticeable challenge identified with this carding attack was that it was a **human-based attack** (unique session ID) instead of a bot attack. The attacker carried out all the processes and functions like a regular user, making it hard to identify a normal user vs. a hacker.
- The attacker also used different IP addresses belonging to different countries during each attempt.
- Hence, to tackle this problem, the **managed services team created a pattern of the attacker behaviour** based on all the historical data and tracked for any randomization performed on parameters like BIN (Bank Identification Number), Credit Card details, etc.

The managed services team **deployed custom rules** to track and block any user attempting to edit any standard parameters linked to the carding attack.

- It was also made sure that the IP addresses used to perform the carding attacks were blocked to avoid any more access to those sets of IP addresses for a definite amount of time.
- Furthermore, if the user/attacker belonged to the geolocation where the customer had no scope of doing business, then such requests were blocked immediately with the help of IP filtration.
- All the above rules were deployed within a short time frame, and the carding attacks were reduced significantly making sure that no fake requests were passed to the origin.
- Despite the reduction in the attacks, the 24*7 managed services of Indusface **constantly monitored the incoming traffic** to track any other changing patterns in the behaviour of the incoming traffic and made sure to adjust the defence mechanisms on an ongoing basis.
- Since the deployment of the AppTrana WAAP, the customer has punched **zero fake orders due to carding attacks** over the past year.

Results:

- **Successful mitigation of carding attacks** within a few hours of request
- Significant reduction in fraudulent transactions and **zero fake orders**
- Regained **control over the brand reputation**
- Efficient and **quick response to prevent disruptions** caused by carding attacks

Read the Full Story

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

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.

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.

Dilip Panjwani

Global Head - Cybersecurity Practice & CoE, LTIMindtree

We were looking for a WAF that focuses on attacker behaviour rather than variance signatures to mitigate the risk from application vulnerabilities. We decided to take the leap and partner with Indusface to protect our enterprise application footprint.

INDUSFACE IS THE ONLY CLOUD WAAP (WAF) VENDOR WITH 100% CUSTOMER RECOMMENDATION FOR 3 CONSECUTIVE YEARS

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

Gartner Peer Insights Customers' Choice 2023™

BENGALURU | VADODARA | MUMBAI | NEW DELHI | SAN FRANCISCO

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

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