INDUSFACE™

THE STATE OF
APPLICATION SECURITY

INDEX

APPTRANA

Fully Managed SaaS Based Web Application Security Solution with Integrated Application Scanner, Web Application firewall and CDN

START YOUR FREE TRIAL NOW

ABOUT INDUSFACE

Indusface is a leading application security SaaS company that secures critical Web, Mobile, and API applications of 4000+ global customers using its award-winning fully managed platform AppTrana that integrates web application scanner, web application firewall, DDoS & BOT Mitigation, CDN, and threat intelligence engine.

Indusface has been funded by Tata Capital Growth Fund II, is the only vendor to be named Gartner Peer Insights™ Customers' Choice' in all the 7 segments for Web Application and API Protection Report 2022, is a "Great Place to Work" certified SaaS product company, is PCI, ISO27001, SOC 2, GDPR certified and has been the recipient of many prestigious start-up awards such as the Economic Times Top 25, NASSCOM DSCI Top Security Company, Deloitte Asia Top 100, among others.

INDUSFACE IS THE ONLY VENDOR TO BE NAMED GARTNER® PEER INSIGHTS™ CUSTOMERS' CHOICE IN ALL THE 7 SEGMENTS OF VOICE OF CUSTOMER WAAP 2022 REPORT.

Gartner Peer Insights Customers' Choice 2022™

OUR CUSTOMERS

TATA CONSULTANCY SERVICES · IndusInd Bank · L&T Infotech · ADITYA BIRLA CAPITAL
HDFC ERGO · marico · TITAN · ACT FIBERNET
Khatabook · CRISIL · AEGONLife · MYn
R. · TATA PLAY · NASSCOM® · YES SECURITIES

EXECUTIVE SUMMARY

The report - "The State of Application Security Q4 2022", is based on a sample size of 1400+ applications.

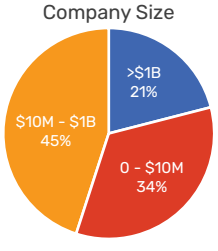
Here are the findings from the study:

- 829,833,298 attacks were blocked during this time
- These attacks were blocked despite having 61,713 open vulnerabilities in the applications
- 30% of vulnerabilities have been open for more than 180 days. This includes 1745 critical and high vulnerabilities
- Customers are increasingly taking the route of "virtual patching" to protect applications at the Web Application Firewall level
- 60% of attacks were blocked using custom rules. Security teams are increasiningly relying on managed services and custom rules to get more value out of WAF deployments
- On an average, each customer deploys 48 custom rules
- 32% of apps have had a DDoS attack in the last 60 days. DDoS as a % of total attacks has increased to 10% in Q4 from 7.5% in Q3
- URI-specific rate limiting is preventing 47% of DDoS attacks
- 743 websites experienced a bot attack but were successfully blocked by AppTrana
- Most of the bot attacks originated from Russia

CUSTOMER SEGMENTS AND ANALYSIS

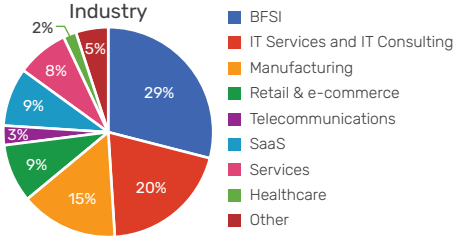
Before we go into the report, here is the segmentation of the 1400+ websites analysed for this study.

As per revenue, the largest segment belonged to the mid-market, with 45% of companies having revenues between $10 Million to $1 Billion, 21% of the companies are large enterprises with more than one billion in revenue, and small businesses made up the remaining 34%.

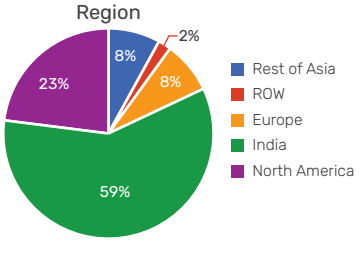


Now coming to the industry split, Banking, Insurance, and other finance companies, followed by IT services and manufacturing companies, are the top three segments.

SaaS/IT products and Retail/e-commerce also have a decent representation of 9% each.



Finally, as far as the region is concerned, 59% of the websites are in India, followed by 23% in US and Canada.



VULNERABILITY EXPLOITS

- Total no. of vulnerabilities found: 61K

Top 10 vulnerability categories found:

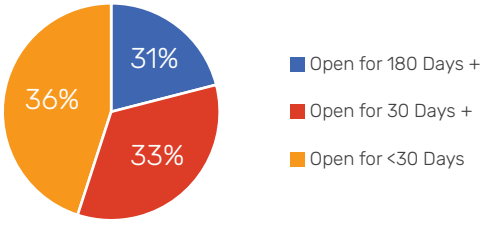
VULNERABILITY TYPE	TOTAL VULNERABILITIES
Unset/Insecure X-Permitted-Cross-Domain-Policies Header	13003
Possible Slow Response Time Detected	4842
Insecure Content Security Policy (CSP)/X-Frame-Options	4293
Application Error Message	3697
Email Address Disclosure	2944
Cookie Overly Broad Path Detected	2702
Running Service (Port:80/TCP)	2533
HTML Form Without Anti-CSRF Token Detected	2486
Content Injection	1949
Web Server Version Disclosure	1921

AGING TREND OF THESE VULNERABILITIES:

Across the sample size of 1400+ sites analyzed; we have found 61K open vulnerabilities. This is an average of about 30 vulnerabilities/site and around 31% have been open for more than 180 days. This includes 1700+ critical and high vulnerabilities that have been open for 180+ days.

Security and dev teams are increasingly adopting the "virtual patching" capabilities on WAF to block attacks. This gives them time to fix these vulnerabilities on the applications.

With AppTrana, security teams are increasingly leveraging the built-in scanner and penetration testing support to find vulnerabilities regularly. Then they leverage the managed services team to patch these vulnerabilities on the firewall near real-time.



No of vulnerabilities open for 30 days – 36%

No of vulnerabilities open for 90 days – 33%

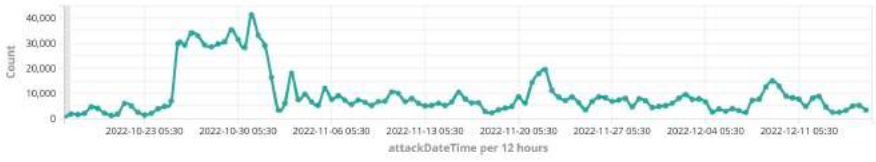
No of vulnerabilities open for 180 days - 31%

Protection trends:

No. of attacks blocked

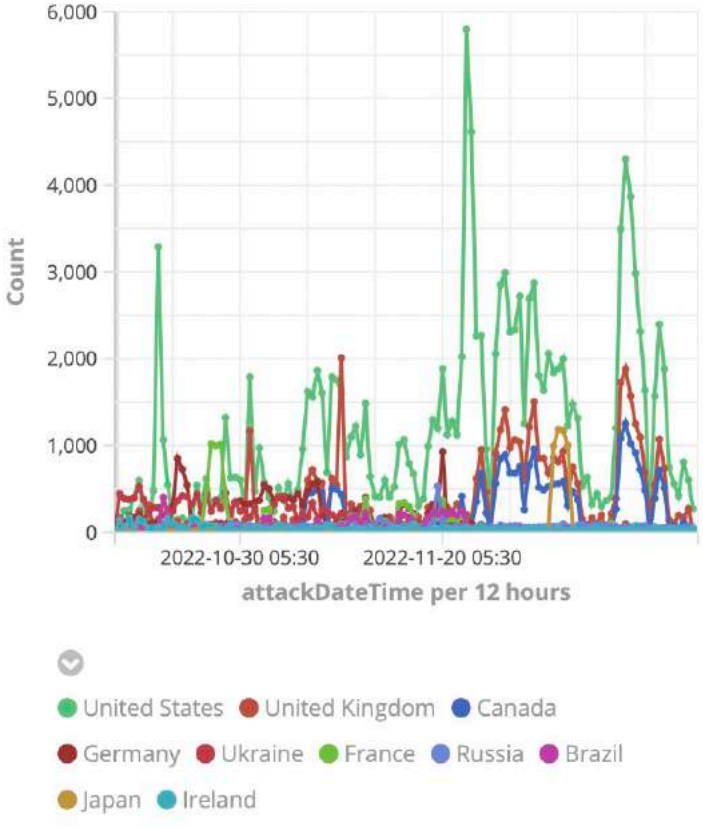
829,833,298

Attacks' trend across all sites:



On average, we see about 829M requests that get blocked across all sites protected by AppTrana.

Given majority of customers business is targeting Indian markets, large number of these attacks originate from India. Outside India, we see attacks from the US, the UK & Canada.



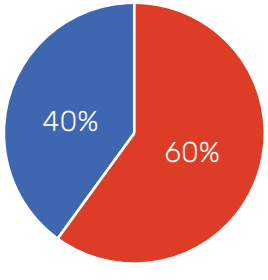
No. of blocks by the core rules set

188,164,757

No. of blocks by custom rules

295,571,861

40% of requests are blocked by AppTrana's default rule set and 60% of requests blocked by custom rules created based on the specific need of applications highlighting the value of managed service that AppTrana provides.



DDoS & BOT ATTACKS

As new attack trends of DDoS and BOT attacks emerge, business continuity becomes very important.

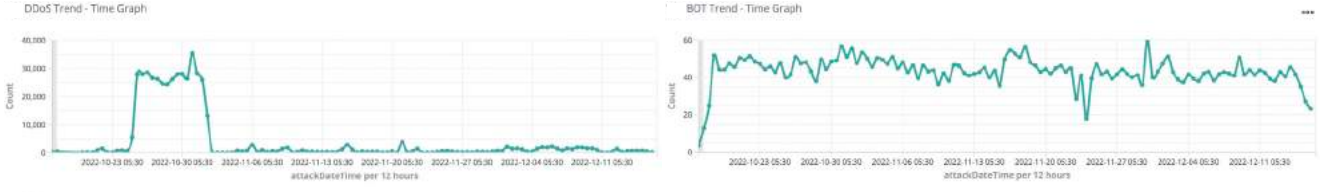
- AppTrana ensures round-the-clock availability of your application by mitigating DDoS and Bot attacks with its inbuilt DDoS scrubber.
- It helps you go beyond static rate limits and customize rules based on the behavior of inbound traffic received by host, IP, URI, and Geography.

We see the following DDoS & Bot trends:

336 million DDoS request and 3.7 million bot attackes are blocked on 405 and 743 application respectively

DDoS Attack blocked - Sites	BOT Attack blocked - Sites
405	**743**
No. of Sites Where Block Happened	No. of Sites Where Block Happened

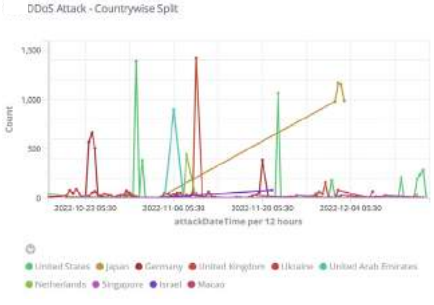
Attack trend



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

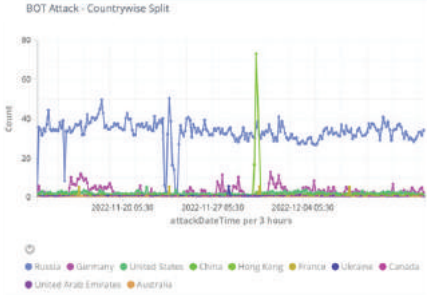
DDoS as a % of total attacks has increased to 10% in Q4 from 7.5% in Q3.

URI-specific rate limiting is preventing 47% of DDoS attacks. Also, Geofencing and IP blacklisting are the other weapons that customers choose for protection against DDoS attacks



Bot trend across major countries:

Similar to Q3, bot attacks majorly originated from Russia.



AppTrana enables CISOs to ensure business continuity with round-the-clock protection against DDoS and BOT attacks through sophisticated behaviour-based models.

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 Web sites. 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 that occurs when a user is able to control an input point and is able to 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 cyber-attack 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

CISO & IT Controller, LTI (Larsen & Toubro Infotech)

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 VENDOR TO BE NAMED GARTNER® PEER INSIGHTS™ CUSTOMERS' CHOICE IN ALL THE 7 SEGMENTS OF VOICE OF CUSTOMER WAAP 2022 REPORT.

Gartner Peer Insights Customers' Choice 2022

INDUSFACE™

BENGALURU | VADODARA | MUMBAI | NEW DELHI | SAN FRANCISCO

Contact Us - +91 265 6133021 | +1 866 537 8234

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