INDUSFACE™

THE STATE OF APPLICATION SECURITY

INDEX

APPTRANA

START YOUR FREE TRIAL NOW

ABOUT INDUSFACE

Indusface is a leading application security SaaS company that secures critical Web, Mobile, and API applications of 3000+ 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

TCS TATA CONSULTANCY SERVICES | IndusInd Bank | L&T Infotech | ADITYA BIRLA CAPITAL

HDFC ERGO Take it easy! | marico | TITAN | ACT FIBERNET

CRISIL An S&P Global Company | Flipkart Health+ | AEGONLife | MYn

R. | TATA PLAY | NASSCOM® | YES SECURITIES

EXECUTIVE SUMMARY

The report - "The State of Application Security", is based on the analysis of 1200+ websites and 12 billion+ requests on the AppTrana network from August 2022 – September 2022.

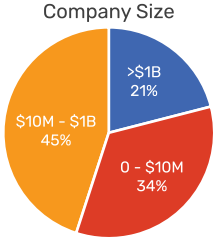
Here are the findings from the study:

- 418,583,338 attacks were blocked during this time
- These attacks were blocked despite having 40,756 open vulnerabilities in the applications
- 30% of vulnerabilities have been open for more than 180 days. This is in line with industry averages where, on an average, vulnerabilities are fixed in 250 odd days
- Customers are increasingly taking the route of "virtual patching" to protect applications right at the Web Application Firewall level
- 234 websites experienced DDoS attacks, but all of them were blocked by AppTrana
- Outside India, AppTrana detected the DDoS attempts from the UK and Ukraine
- 695 websites experienced a bot attack but were successfully blocked by AppTrana
- Most of the bot attacks originated from Russia

CUSTOMER SEGMENTS AND ANALYSIS

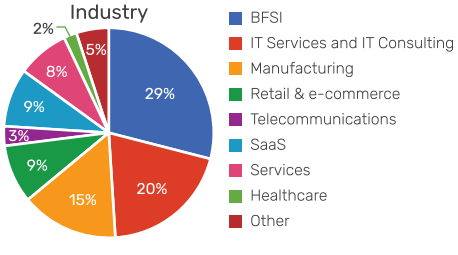
Before we go into the report, here is the segmentation of the 1200+ websites analysed for this study.

As per revenue, the largest segment belonged to the mid-market, with 46% of companies having revenues between $10 Million to $1 Billion, 31% of the companies are large enterprises with more than one billion in revenue, and small businesses made up the remaining 34%.

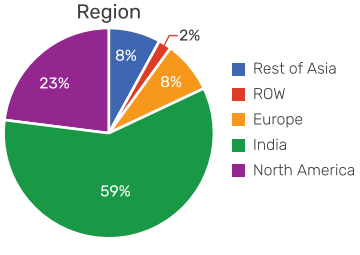


Now coming to the industry split, Banking, Insurance, and other finance companies, followed by IT services and manufacturing companies, are the top three segments.

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

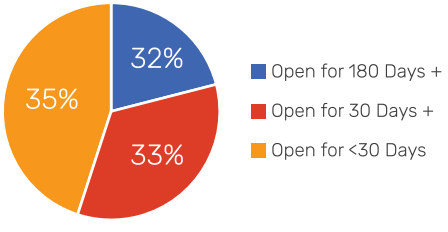
- Total no. of vulnerabilities found: 41K
- Top 10 vulnerability categories found

VULNERABILITY TYPE	TOTAL VULNERABILITIES
Insecure Content Security Policy (CSP)/X-Frame-Options	9002
Application error message	7720
Cookie Overly Broad Path Detected	4044
HTML Form Without CSRF Protection	4042
Email Address Disclosure	3818
Sensitive HTML Form Fields With auto-complete Enabled	3796
Web server version disclosure	2336
Cross-Site Scripting (XSS)	2288
Browser Cache Enabled	1882
HTML injection	1828

AGING TREND OF THESE VULNERABILITIES:

Across 1200+ sites analysed, we have found 41K vulnerabilities, averaging about 40 vulnerabilities/site, and around 30% are open for more than 180 days.

That said, these sites had zero reports of security breaches despite receiving 400 million+ attacks.

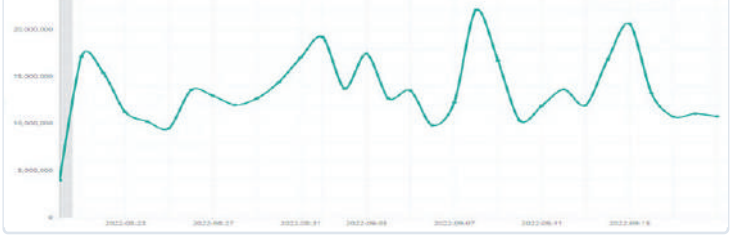


No. of blocks in 30 days

Total Attack Count

418,583,338

30 days Trend of attacks across all sites



On average, every day, we see about 14M attacks targeting open vulnerabilities that get blocked across all sites protected in AppTrana.

So, how do these companies stay protected while having so many open vulnerabilities?

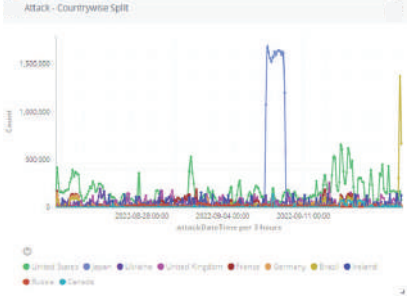
It is not like these teams don't want to fix vulnerabilities. There are factors outside the control of the company, such as dependency on third-party code, unavailability of developers, and so on.

With AppTrana, our customers have chosen to virtually patch these vulnerabilities on the firewall, thereby ensuring real-time protection.

Since detection of vulnerabilities and protection through virtual patches happen on the same product, our customers are always on top of vulnerabilities. They have the capability even to run daily scans and request virtual patches through our fully managed web application firewall.

CISOs are thereby at the forefront of enabling digital transformation without compromising security.

AppTrana also ensures the detection and protection of zero-day vulnerabilities, with more than 95% of zero-day vulnerabilities protected by default without needing any virtual patches.



Now coming to the origin of these attacks, most of our customers service the Indian market. Therefore, many of these attacks originate from India. The next major country we see attacks from is the United States, followed by Japan and Ukraine.

Trend of attacks from Ukraine increased with changing geo-political situations.

Blocks by AppTrana's default configuration in 30 days across sites.	Blocks by on-demand virtual patches across the sites
218,602,321	167,901,255

AppTrana's default configuration blocks 60% of requests, and on-demand virtual patches block 40% of requests. These have been created based on the specific need of the security teams by highlighting the value of managed service that AppTrana provides.

DDoS & BOT ATTACKS

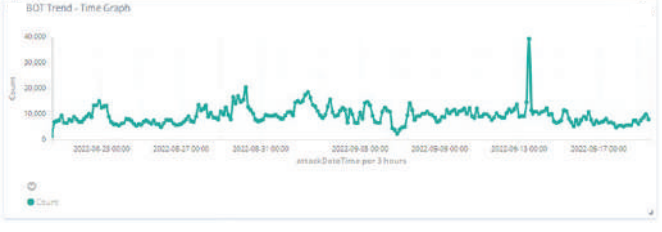
Business continuity is at a huge risk, given the rise in DDoS and Bot Attacks.

We see the following DDoS & Bot trends:

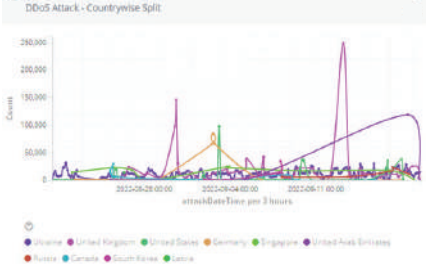
The total number of sites where the DDoS & BOT attack trends were observed (in the last 30 days) are:

DDoS Attack blocked - Sites	BOT Attack blocked - Sites
234	**695**
No. of Sites Where Block Happened	No. of Sites Where Block Happened

ATTACK TREND

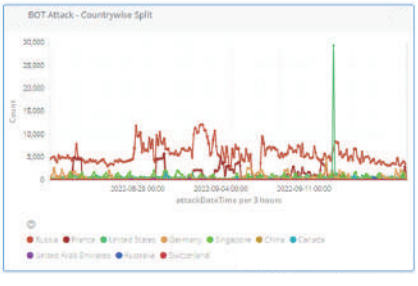


Major countries where DDoS attacks were observed other than India are Ukraine, the UK, and the United States. These trends are in line with the changes in the geopolitical situation.



Major Countries' Bot Trend:

Bot Trends were a bit surprising, with major requests seen from Russia.



CISOs ensure business continuity with round-the-clock protection against DDoS and BOT attacks through AppTrana's sophisticated Behavioural-based models.

- Go beyond static rate limits and customize blocking behaviors based on the trends of inbound traffic received by the host, IP, URI, and Geography
- AppTrana ensures round-the-clock availability of your application by mitigating DDoS and Bot attacks with its inbuilt DDoS scrubber.

GLOSSARY

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.

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 attack is successful due to a web application's lack of user input validation, allowing users to supply application code in HTML instead of normal text strings.

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.

HTML Injection -

- A type of injection vulnerability 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.

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 we managed services and the Indusface team is the SOC for AppSec 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

BENGALURU | VADODARA | MUMBAI | NEW DELHI | SAN FRANCISCO

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

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