INDUSFACE™

THE STATE OF APPLICATION SECURITY - Q2, 2023

INDEX

APPTRANA

Fully Managed WAF with Integrated Application Scanner (DAST), API Discovery & Security, DDoS/Bot Protection, 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 5000+ global customers across 90+ countries 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

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

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

Khatabook Business hua Easy | CRISIL An S&P Global Company | AEGON Life | MYn

R. | TATA PLAY | NASSCOM® | YES SECURITIES

EXECUTIVE SUMMARY

The State of Application Security – Q2, 2023 report is based on a sample size of 1400+ applications.

Here are the findings from the study:

- 1.1 billion attacks were blocked during this time
- 900 million+ of them were from India - a 90% growth compared to Q1 where there were 500 million attacks
- DDoS & bot attacks are on the rise.
    - There is a 75% increase in the number of DDoS attacks (Q2, 2023 vs Q1, 2023)
    - We even saw a 48% increase in number of bot attacks. (Q2, 2023 vs Q1, 2023)
- 9 out of 10 sites witnessed a bot attack
- 33K critical, medium, and high vulnerabilities were found
- 31% of vulnerabilities have been open for more than 180 days. This includes 1729 critical and high vulnerabilities.
- Customers are increasingly taking the virtual patching route at the WAF level
    - 41% of the attacks were blocked by using AppTrana's core rules set.
    - 59% of the attacks were blocked using custom rules. This signifies the importance of managed services and custom rules for security teams across the world.
- Banking and insurance faced the highest number of attacks. Over 90% of banking and insurance sites witnessed a bot attack
- 100% of healthcare sites witnessed a bot attack
- The top DDoS attack countries were India, the United States, France and the UK
- Other than India, the major countries from where bot attacks were observed – the United States, the UK and Russia.

VULNERABILITY EXPLOITS

Total no. of vulnerabilities found: 33K

Top 10 vulnerability categories found:

VULNERABILITY TYPE	TOTAL ALERTS FOUND
Cross-Site Scripting (XSS)	13889
HTML Injection	10545
SQL Injection	2959
Web Cache Poisoning Attack	1938
Server Side Request Forgery Detected	1010
SSL Certificate Common Name Mismatch	920
TLS/SSL Server Certificate Will Expire Soon	750
Untrusted TLS/SSL Server Certificate	410
TLS/SSL Server Certificate Expired	384
Script Source Code Disclosure	224

AGING TREND OF THESE VULNERABILITIES:

Over 1400 sites were analyzed. We have found 33K critical, high, and medium vulnerabilities - around 31% of the critical and high vulnerabilities have been open for more than 180 days.

This includes 1729 critical vulnerabilities that have been open for 180+ days. With AppTrana, customers can ensure that vulnerabilities are virtually patched immediately reducing the time to fix ensuring the security team becomes an enabler of business instead of blockers.

Many of our customers leverage the risk-based protection of AppTrana to get vulnerabilities patched in WAF immediately enabling rapid deployment. AppTrana also ensures the detection and protection of zero-day vulnerabilities with more than 94.66% of zero-day vulnerabilities protected by default using AppTrana default rules.

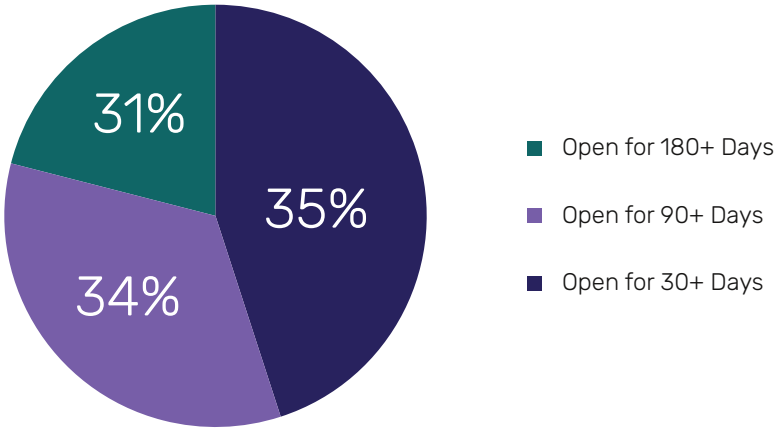
Top 3 vulnerability categories in Q2 2023:

- Cross-Site Scripting (XSS)
- HTML Injection
- SQL Injection

Top 3 vulnerability categories in Q1 2023:

- Cross-Site Scripting (XSS)
- Server Side Request Forgery Detected
- HTML Injection

Amidst known vulnerabilities, we have observed recent vulnerabilities like Moveit SQL 0-day and Adobe ColdFusion RCE. The exploits targeting these vulnerabilities were mitigated out of the box on AppTrana WAAP.



No of vulnerabilities open for 30 days – 35%

No of vulnerabilities open for 90 days – 34%

No of vulnerabilities open for 180 days - 31%

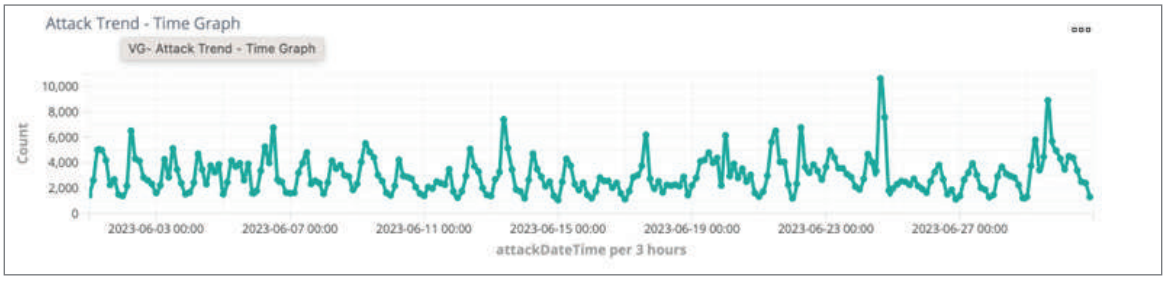
Protection Trends:

Total Attacks Count

1,155,890,271

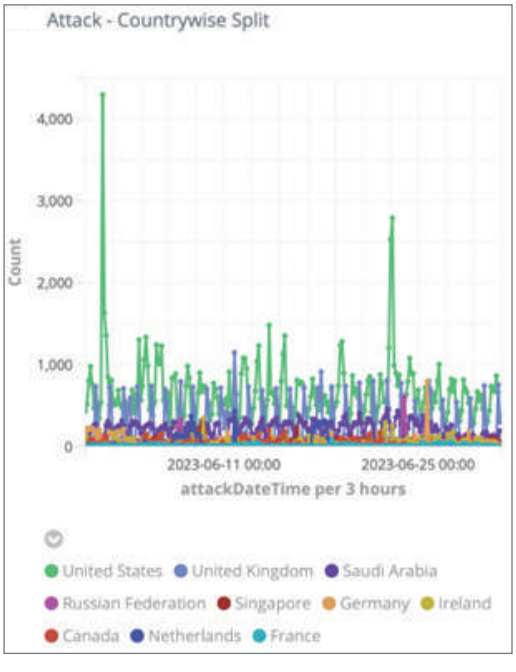
We saw over 1.15 billion requests that got blocked across all sites protected by AppTrana. It's a 10% increase in attacks when compared to the attacks in Q1, 2023.

Past 30-days attacks' trend across all sites:

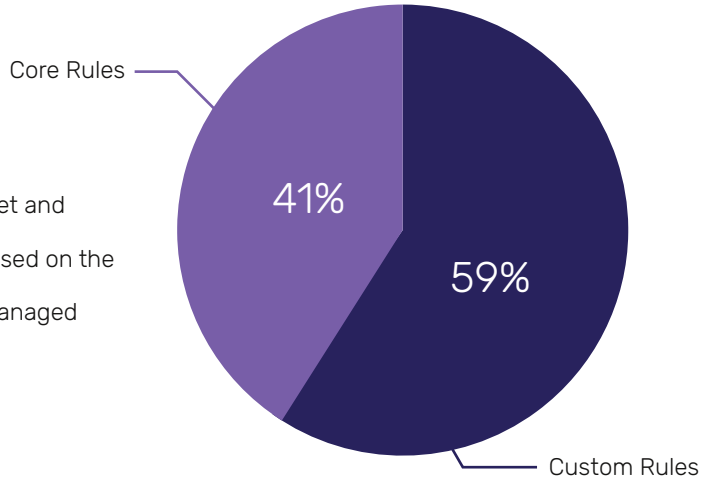


On average, we see about 789K requests that get blocked across all sites protected by AppTrana.

Given majority of customers business is targeting Indian markets, large number of these attacks originate from India. Next major country we see attacks from is the United States followed by the UK.



41% of requests were blocked by AppTrana's default rule set and 59% of requests were blocked by custom rules created based on the specific need of applications - highlighting the value of managed service that AppTrana provides as well.



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 see the following DDoS & Bot trends:

The total number of sites where DDoS & bot Attack trends were observed in the last 180 days are:

Total DDoS Attacks Blocked - Sites	Total DDoS Attacks –
557	**872,105,826**

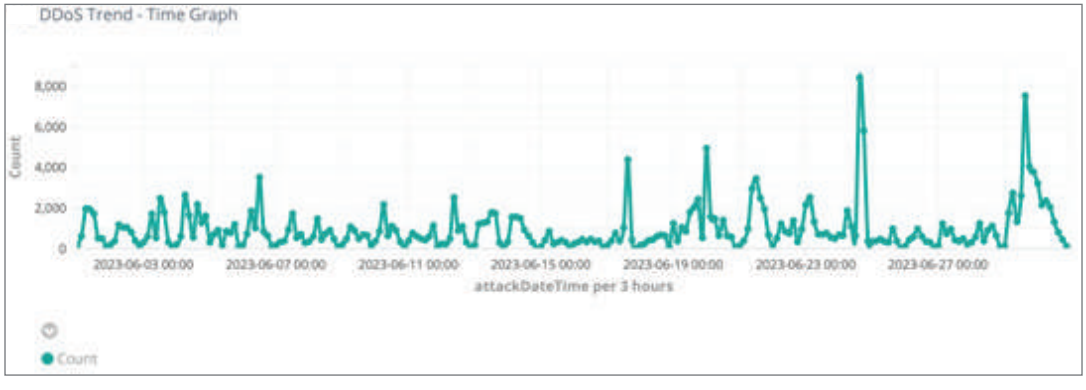
Total Bot Attacks Blocked - Sites	Total Bot Attacks
1304	**88,186,868**

Q2, 2023 vs Q1, 2023 -

- There is a 75% increase in the number of DDoS attacks. 872M vs 498M (Q2, 2023 vs Q1, 2023)
- 38% sites witnessed DDoS attacks compared to 30% in the last quarter.
- There is a 48% increase in number of bot attacks. 88M vs 59M (Q2, 2023 vs Q1, 2023)
- 89% sites witnessed bot attacks compared to 86% in the last quarter.

DDoS & Bot Attacks Trends (Monthly & Country-wise Split)

DDoS attacks trends

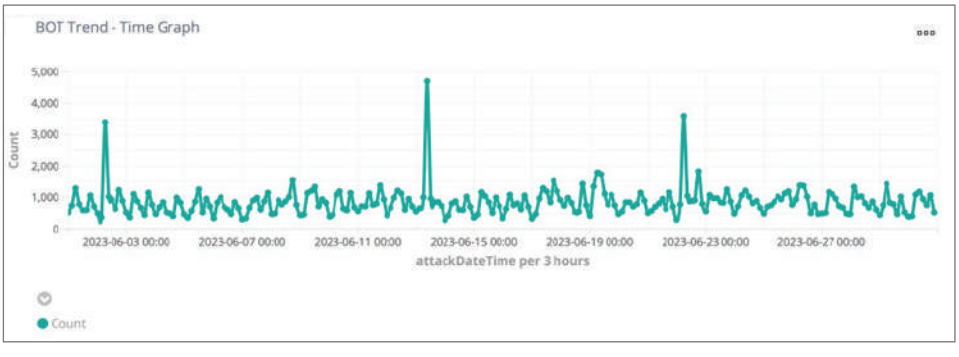


Top 10-DDoS Attack Country

Country	Count
India	39,732,355
United States	3,244,779
France	1,667,643
United Kingdom	615,295
Isle Of Man	264,310
Germany	208,628
Russian Federation	201,729
Thailand	169,101
Seychelles	102,127
Australia	81,885

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

Bot Attack Trends:



Top 10-BOT Attack Country

Country	Count
India	10,607,408
United States	10,388,502
United Kingdom	6,675,747
Russian Federation	2,270,424
Saudi Arabia	1,617,038
Netherlands	939,488
Germany	877,230
Singapore	668,243
France	426,045
Ireland	374,539

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

INDIA DATA INSIGHTS

Total Attacks Count - India

947,830,022

- Over 947 million attacks were blocked during this time.
- There is a 90% increase in the number of attacks in India compared to 500 million in Q1 2023
- Banking and insurance faced the highest number of attacks. Over 90% of banking and insurance sites witnessed a bot attack
- 100% of healthcare sites witnessed a bot attack
- The Banking and Insurance industry relies on custom rules. More than 60% of the attacks were blocked using custom rules.

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

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 6133021 | +1 866 537 8234

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