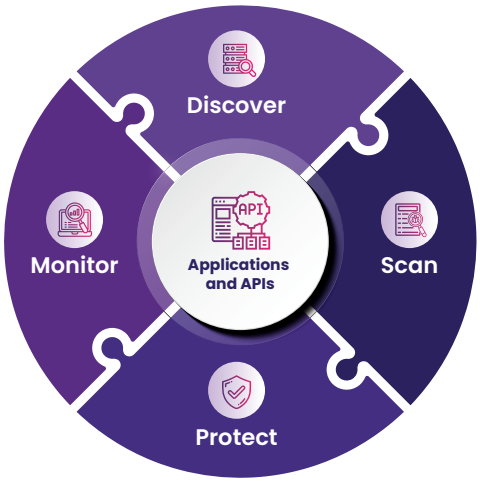
INDUSFACE™

THE STATE OF APPLICATION SECURITY - Q3, 2023

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

EXECUTIVE SUMMARY

The State of Application Security – Q3, 2023 report is based on a sample size of 1400+ applications.

Here are the findings from the study:

- Over 2 billion attacks were blocked during this time
- 1.6 billion+ of them were from India - a 70% growth compared to Q2, where there were 947 million attacks
- DDoS & bot attacks are on the rise.
    - There is a 67% increase in the number of DDoS attacks (Q3, 2023 vs Q2, 2023)
    - We even saw a 56% increase in number of bot attacks. (Q3, 2023 vs Q2, 2023)
- 8 out of 10 sites witnessed a bot attack
- 46K critical and high vulnerabilities were found
- 32% of vulnerabilities have been open for more than 180 days. This includes 14794 critical and high vulnerabilities.
- Customers are increasingly taking the virtual patching route at the WAF level.
    - 35% of the attacks were blocked by using AppTrana's core rules set.
    - 65% of the attacks were blocked using custom rules. This signifies the importance of managed services and custom rules for security teams across the world
- In this quarter, SaaS and Conglomerate companies saw a 10X surge in the number of attacks as they deal with customer-sensitive information across multiple industries
- A significant increase in the botnet-driven low-rate HTTP DDoS attacks was witnessed in Q3 2023
- URI-based rate limiting prevented over 50% of DDoS attacks in the Banking and Financial sectors
- 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, Germany and the UK
- Other than India, the major countries where bot attacks were observed were the United States, the UK, Russia and Singapore.

VULNERABILITY EXPLOITS

Total no. of vulnerabilities found: 46K

Top 10 vulnerability categories found:

VULNERABILITY TYPE	TOTAL ALERTS FOUND
Malicious Content Found (Software and Data Integrity Failures)	9373
Server Side Request Forgery Detected	897
Cross-Site Scripting (XSS)	633
HTML Injection	540
TLS/SSL Server Certificate Will Expire Soon	248
Script Source Code Disclosure	118
SQL Injection	111
SSL Certificate Common Name Mismatch	101
Invalid TLS/SSL Server Certificate	72
EPMM Authentication Bypass	44

AGING TREND OF THESE VULNERABILITIES:

Over 1400 sites were analyzed. We have found 46K critical and high vulnerabilities - around 31% of the critical and high vulnerabilities (i.e., 14794) have been open for more than 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 a blocker

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 93.33% of zero-day vulnerabilities protected by default using AppTrana default rules.

Top 3 vulnerability categories in Q3 2023:

- Malicious Content Found (Software and Data Integrity Failures)
- Server Side Request Forgery Detected
- Cross-Site Scripting (XSS)

Top 3 vulnerability categories in Q2 2023:

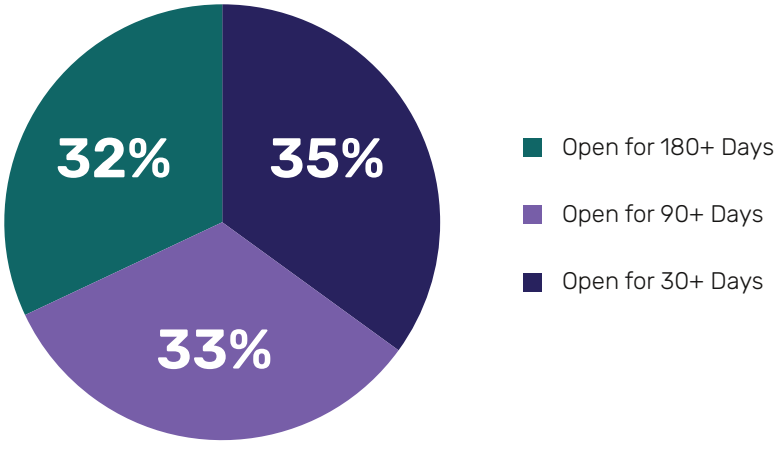
- Cross-Site Scripting (XSS)
- HTML Injection
- SQL Injection

Zero-Day vulnerabilities identified in the quarter:

	July	**August**	**September**
Zero-Day Vulnerabilities Identified	266	210	222
Zero-day vulnerabilities **blocked through AppTrana**	**Total - 100%** Core rules – 91% Custom rules - 9%	**Total - 100%** Core rules – 93% Custom rules - 7%	**Total - 100%** Core rules – 96% Custom rules - 4%

Amidst known vulnerabilities, we observed several critical zero-day vulnerabilities such as Ivanti 0-day (CVE-2023-35078), an actively exploited zero-day vulnerability (CVE-2023-35081) affecting Endpoint Manager Mobile (EPMM), and a critical privilege escalation vulnerability in WordPress (CVE-2023-28121).

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



No of vulnerabilities open for 180 days - 32%

No of vulnerabilities open for 90 days – 33%

No of vulnerabilities open for 30 days – 35%

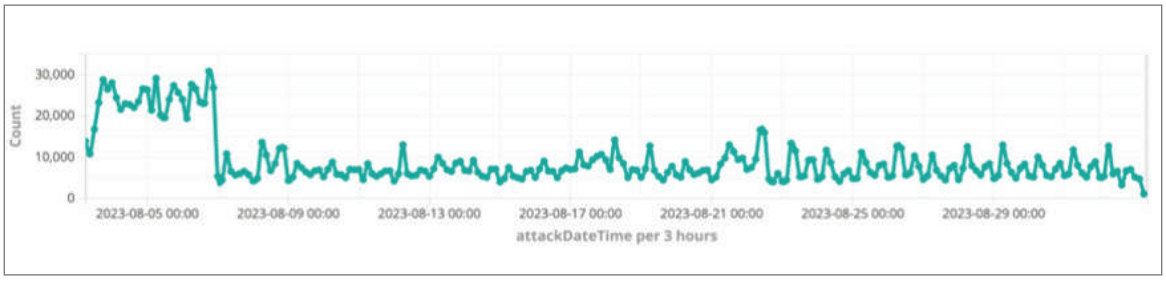
Protection Trends:

Total Attacks Count

2,098,484,247

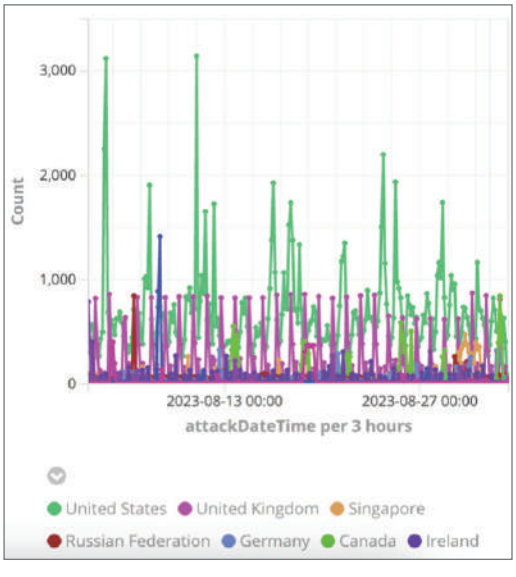
We saw over 2.09 billion requests that got blocked across all sites protected by AppTrana. It's an 82% increase in attacks when compared to the attacks in Q2, 2023.

A view of 30-day attacks' trend across all sites:

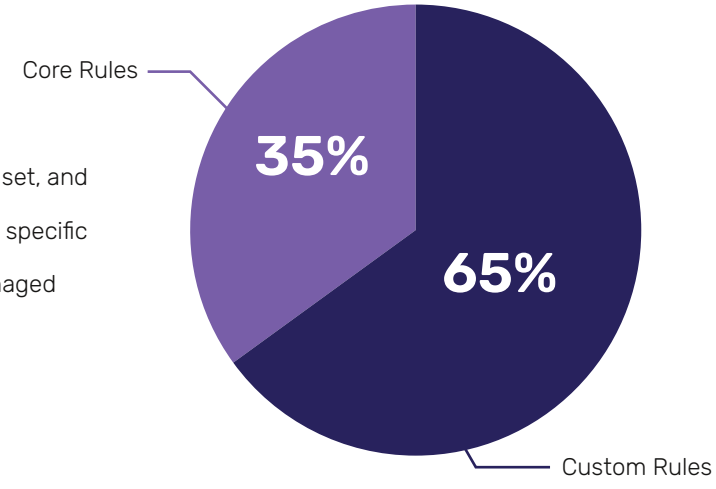


On average, we see about 1.43Mn requests that get blocked across all sites protected by AppTrana.

Given the majority of customer's business is targeting Indian markets, a large number of these attacks originate from India. The next major country we see attacks from is the United States, followed by the UK.



35% of requests were blocked by AppTrana's default rule set, and 65% were blocked by custom rules created based on the specific needs of applications - highlighting the value of the managed service that AppTrana provides.



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 Sites Affected by DDoS Attacks	Total DDoS Attacks
607	**1.45+ Bn**

Total Sites Affected by Bot Attacks	Total Bot Attacks
1348	**137+ Mn**

Q3, 2023 vs Q2 2023

- There is a 67% increase in the number of DDoS attacks compared to Q2 2023
- 41% of the sites witnessed a DDoS attack.
- There is a 56% increase in the number of bot attacks as compared to Q2 2023
- 81% of the sites witnessed a bot attack.

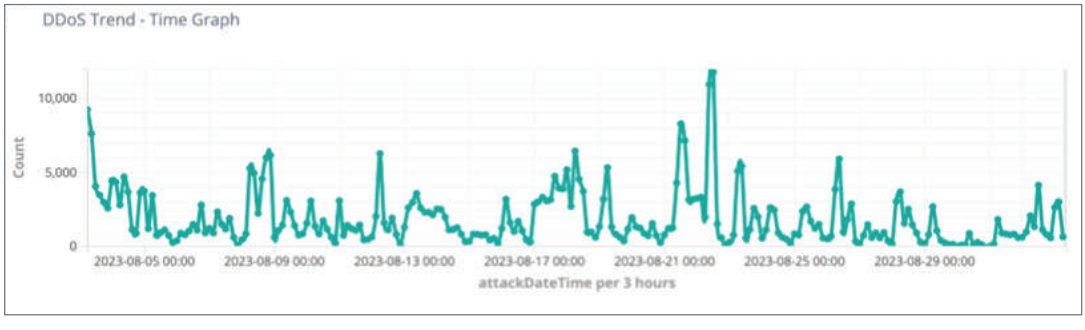
A significant increase in the botnet-driven low-rate HTTP DDoS attacks was witnessed.

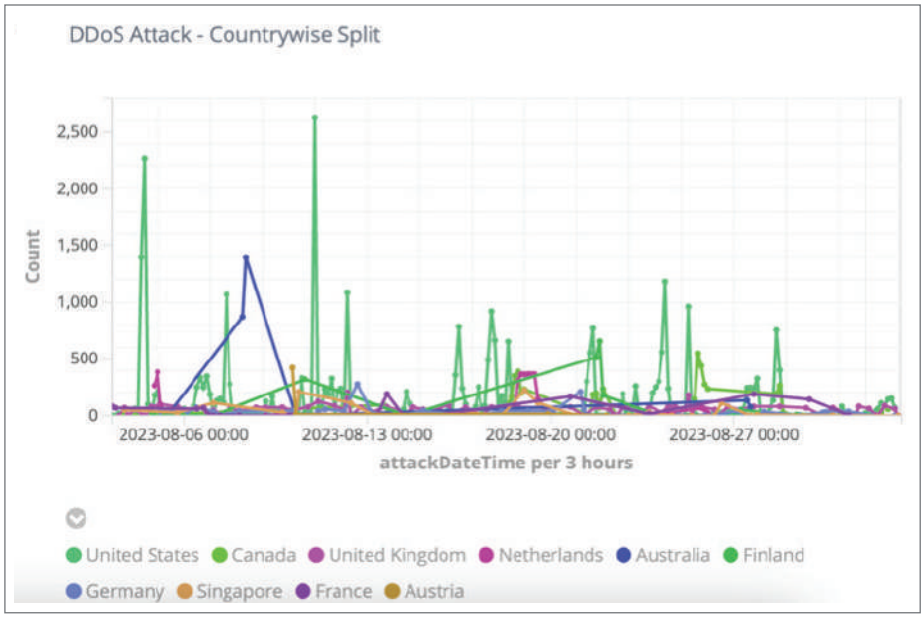
These attacks were carried out by using botnets to send a large number of HTTP requests to a target web server/application over a long period of time. These attacks were designed to be stealthy and persistent, with each bot sending requests at a low rate to avoid detection.

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

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

DDoS attacks trends



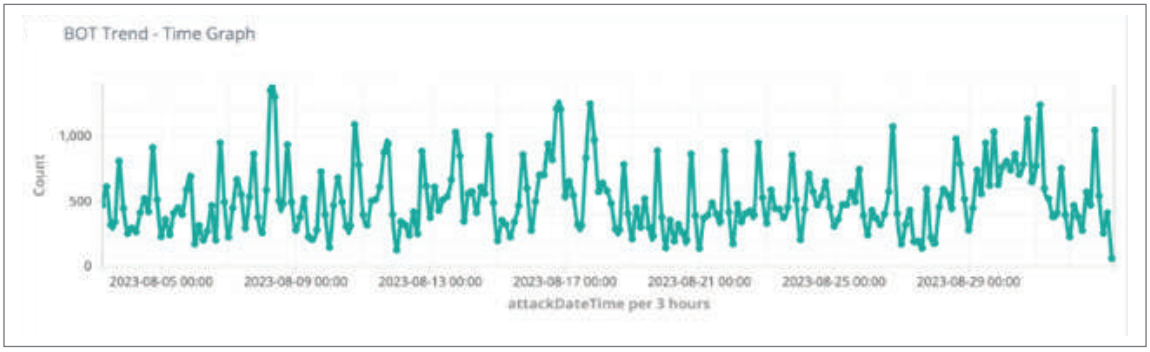


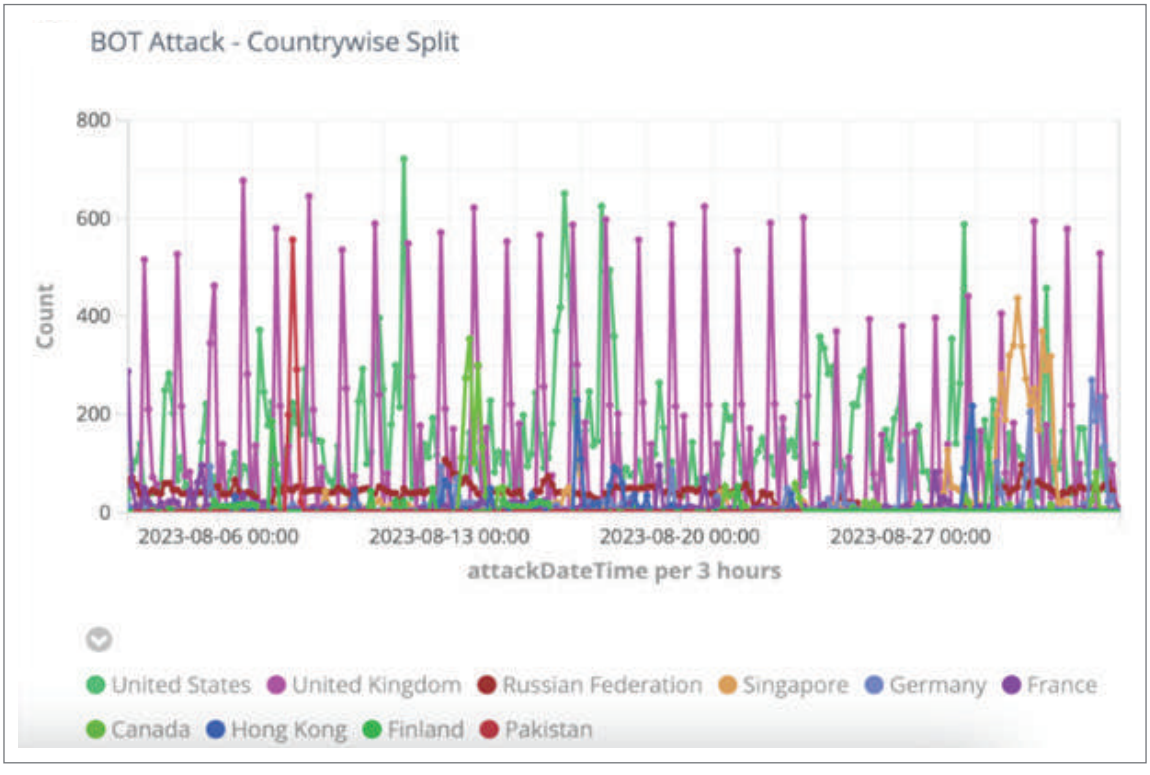
Top 10-DDoS Attack Country

Country	Count
India	135,421,050
United States	111,079,293
Germany	1,951,739
United Kingdom	1,490,138
Singapore	469,202
Ireland	354,577
Canada	274,322
Netherlands	239,810
France	132,553
Philippines	127,321

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

Bot Attack Trends:





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

INDIA DATA INSIGHTS

Total Attacks Count - India

1.6+ Bn

- Over 1.6 billion attacks were blocked during this time
- There is a 70% increase in the number of attacks in India compared to Q2 2023
- SaaS and Conglomerate companies saw a 10X surge in the number of attacks primarily because they deal with customer-sensitive information across multiple industries
- Over 90% of banking and insurance sites witnessed a bot attack
- 100% of healthcare sites witnessed a bot attack
- URI-based rate limiting prevented over 50% of DDoS attacks in the Banking and Financial sectors

CUSTOMER CYBER ATTACK STORY OF THE QUARTER

Mitigating a Botnet-Driven DDoS Attack on a Fortune 500 Company

Solution Highlights:

- DDoS attacks were carried out from 8 million unique IPs for 14 days
- The DDoS attack traffic ranged from 3000X – 14000X, the usual daily traffic
- 100% availability ensured while saving thousands of dollars in additional bandwidth expenditure

About The Customer:

The customer is a Fortune 500 company with a presence in over 30 countries and has been running its businesses in a wide range of sectors for over 5+ decades.

Key Challenges:

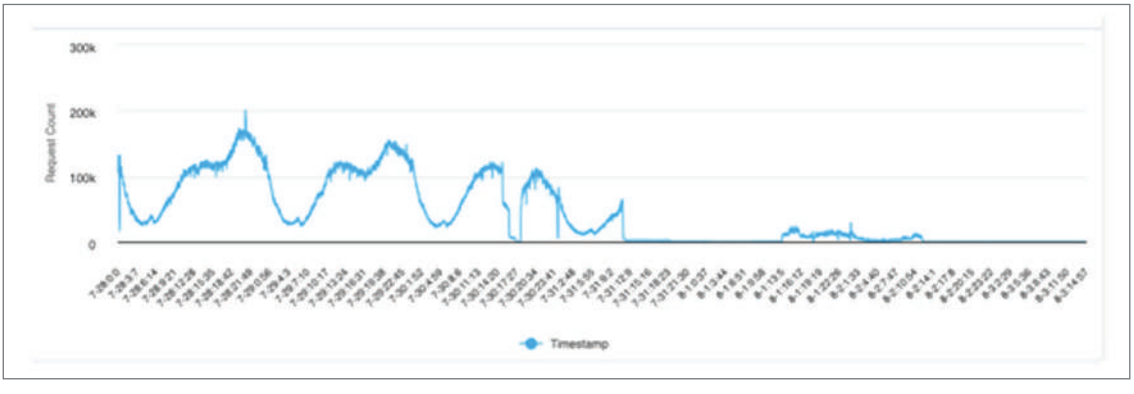
- A targeted Distributed Denial-of-Service (DDoS) attack was launched by Botnets by flooding a series of HTTP requests against their application
- The volume of this HTTP Flooding attack was 3000X – 14000X higher than the usual requests/min received on the site, and the attack used around 8 million unique IPs for 14 days.
- Some IPs were sending only one request per minute, which was too low

Solution Deployed:

- URI Blacklisting Policy
- Rate-Limiting Rules
- Custom rules to allow requests only from the browsers & to block anonymous proxy
- Geo-Fencing Rules
- Increased Tolerance for Bot modules

Results:

- Successfully blocked all the bot traffic at the WAF level, and valid business users were forwarded to the application server.
- No lag in the website's usage and zero service disruptions.
- Saved thousands of dollars in additional bandwidth expenditure



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 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 6133000 | +1 866 458 3058

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