INDUSFACE™

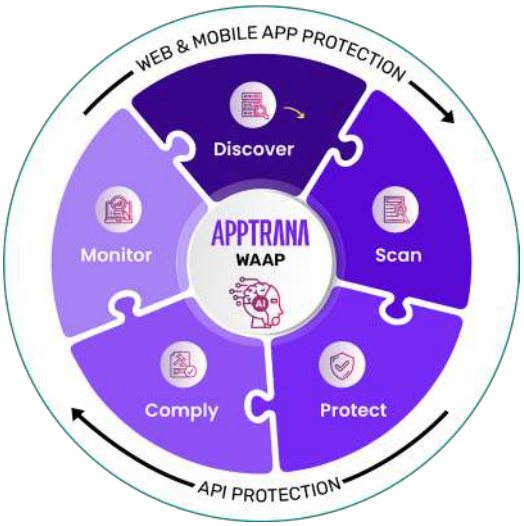
STATE OF APPLICATION SECURITY

Q1 2024

INDEX

APPTRANA

AI-Powered, Fully Managed Application and API Protection



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, an institutionally funded firm, is the only vendor to receive 100% customer recommendation rating four years in a row and is a global customer choice in the 2024 Gartner Peer Insights™ Web Application and API Protection (WAAP) Report. Indusface is also a "Great Place to Work" 2024 certified 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 4 CONSECUTIVE YEARS

A CUSTOMERS' CHOICE FOR 2024, 2023 AND 2022 GARTNER® PEER INSIGHTS™

Gartner Peer Insights Customers' Choice 2024

OUR CUSTOMERS

EXECUTIVE SUMMARY

Here are some of the key findings from the report:

- Over 1.89 billion attacks were blocked from 1st Jan 2024 to 31st March 2024
- On average, 800K attacks were blocked per website
- Cyberattacks grew by 76% in the Q1 of 2024 compared to the Q1 of 2023
- Bot attacks rose by 147%, and DDoS attacks rose by 76% compared to last year Q1 2023:
    - 147+ million bot attacks in Q1 2024
    - 875+ million DDoS attacks in Q1 2024
- 6 out of 10 sites witnessed a DDoS attack, whereas 9 out of 10 sites witnessed a bot attack
- 17K critical and high vulnerabilities were found - 32% of these vulnerabilities were open for 180+ days
- The cyberattacks in India grew by 261% in the Q1 of 2024 compared to the Q1 of 2023
- Customers are increasingly benefiting from autonomous patching at WAAP. In the last two quarters:
    - 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
- Power and energy companies faced up to 500x higher number of attacks than the industry average. This is because hackers are now finding options for ransom and targeting less regulated industries
- Banking and Finance sectors face 4x higher encoding attacks where hackers are using evasion techniques to bypass security measures and probe into sensitive data
- Manufacturing industry is increasingly targeted with Local File Injection(LFI) attacks, where hackers try to access protected folders by manipulating inputs
- 100% of healthcare sites witnessed a bot attack
- The top DDoS attack origin countries were India, the United States, Hong Kong and Netherlands
- Other than India, the major countries from where bot attacks were observed were the United States, Germany and Japan

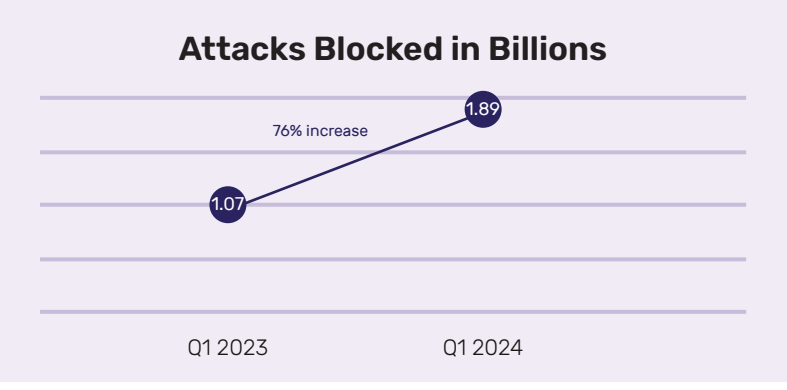
PROTECTION TRENDS:

Total Attacks Count

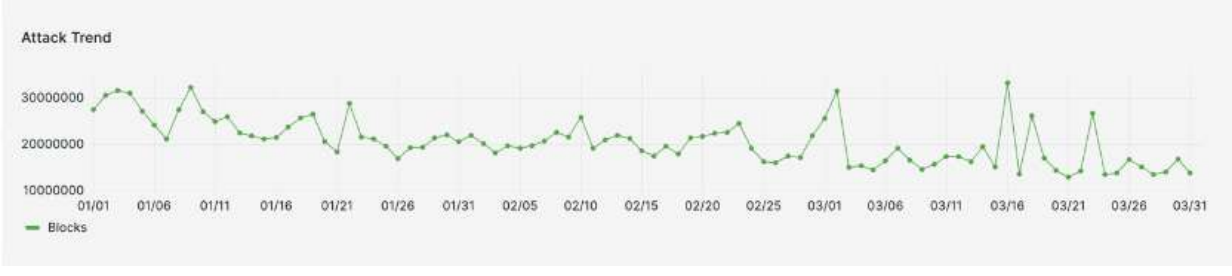
1.89+ Billion

We saw over 1.89 billion requests that got blocked across all sites protected by AppTrana.

The number of attacks increased by 76% in Q1 2024 compared to Q1 2023.



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



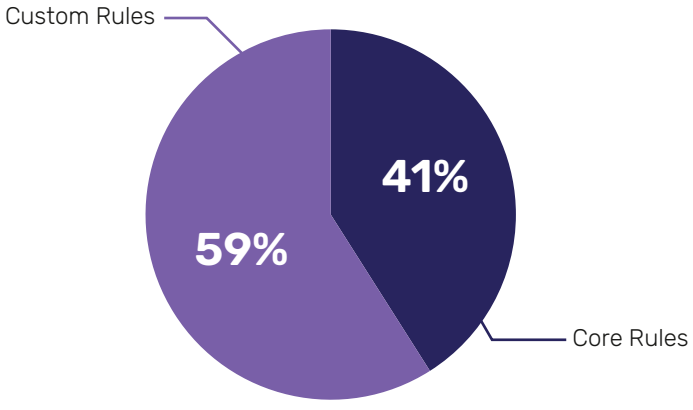
Top 10 Attack Originating Countries

Country	Blocks
India	1407363574
United States	285928876
United Arab Emirates	17372556
Germany	14896004
Hong Kong	14699690
Singapore	13118534
Netherlands	11755806
United Kingdom	10876789
France	9376223
Australia	8164437

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

In this quarter, **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 needs of applications - highlighting the value of managed services that AppTrana provides.

Also, compared to Q1 2023, custom rules blocked 11% more attacks in Q1 2024.



DDoS & BOT ATTACKS

As new attack trends of DDoS and bot attacks emerge against web applications and APIs, business continuity becomes very important.

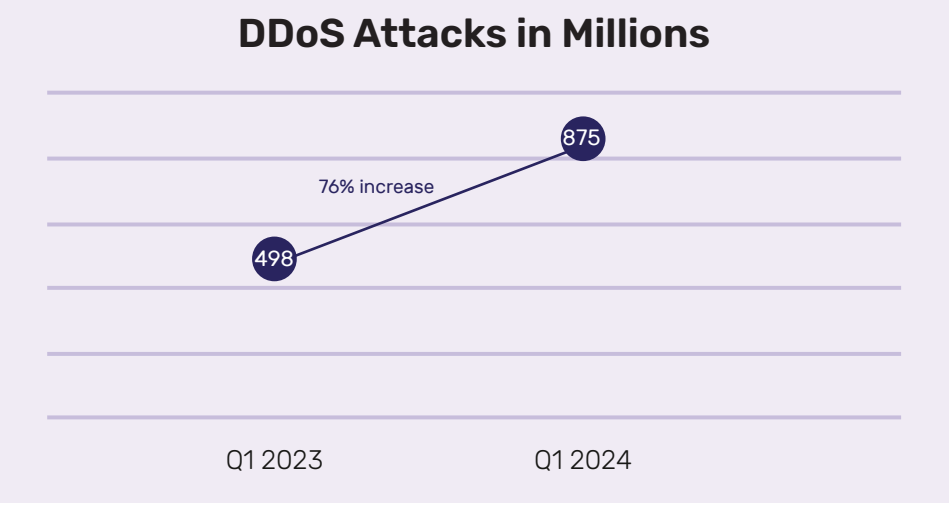
- AppTrana WAAP guarantees zero false positives and ensures 99.99% uptime against layer 3-7 DDoS attacks with behavioural DDoS mitigation, AI-based rate-limiting based on URI, IP, host, and geo. Click here to know more.
- Against bot attacks such as account takeover, credential stuffing, and scraping, 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 Q1 2024:

DDoS Attacks

Total Sites Affected by DDoS Attacks	Total DDoS Attacks
63%	**875+ Million**

Here is the Q-o-Q visualisation of the DDoS attacks blocked in Q1 2024 vs. Q1 2023.



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

Top 10 DDoS Attack Originating Countries

Country	Blocks
India	482971921
United States	56757226
Hong Kong	10725472
Netherlands	4812559
Germany	4297691
Singapore	4190362
United Kingdom	4080191
France	2430428
Bangladesh	1880571
Finland	1063025

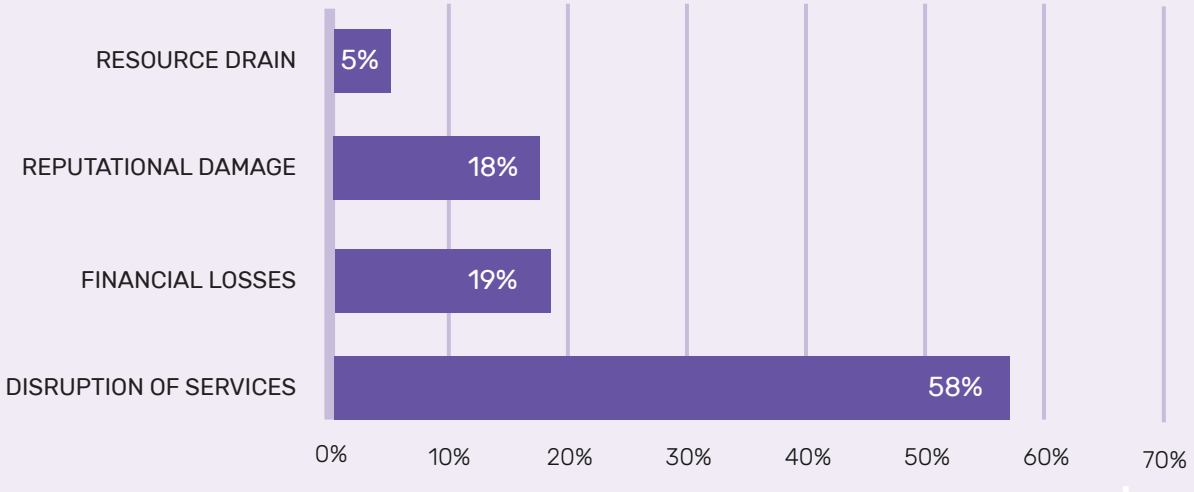
Major countries from where DDoS attacks were observed other than India are the United States, Hong Kong, and the Netherlands.

DDoS attacks rose by 76% compared to Q1 2023, whereas 6 out of 10 sites witnessed a DDoS attack.

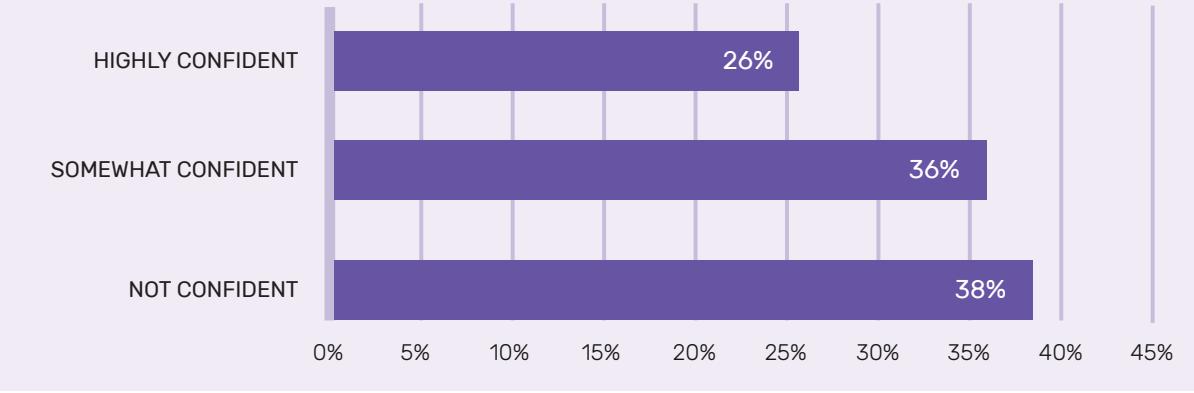
After asking 100+ CISOs, CTOs, and other security leaders outside of our customer base, here's what they had to say about their challenges in managing DDoS attacks.

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

What's the biggest problem your business faces due to DDoS attacks



How confident are you in your organization's ability to mitigate a large-scale DDoS attack?

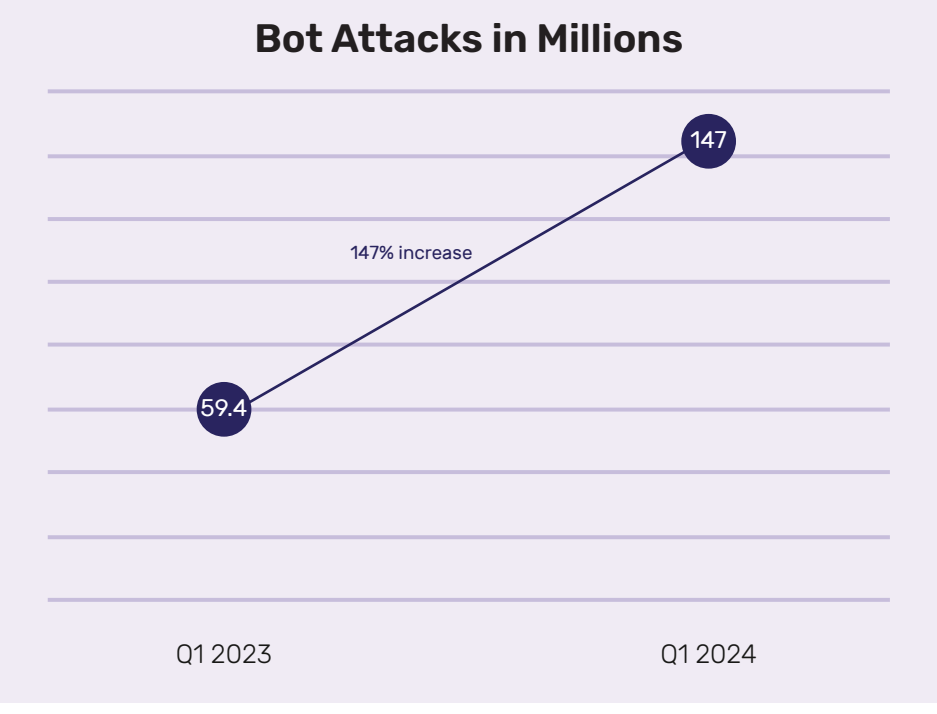


58% of leaders have identified service disruption as the biggest challenge resulting from DDoS attacks. Moreover, only 26% of the surveyed individuals expressed confidence in their WAF/WAAP solutions to safeguard their businesses from large-scale DDoS attacks.

Bot Attacks

Total Sites Affected by Bot Attacks	Total Bot Attacks
87%	**147+ Million**

Here is the Q-o-Q visualisation of the bot attacks blocked in Q1 2024 vs. Q1 2023.



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

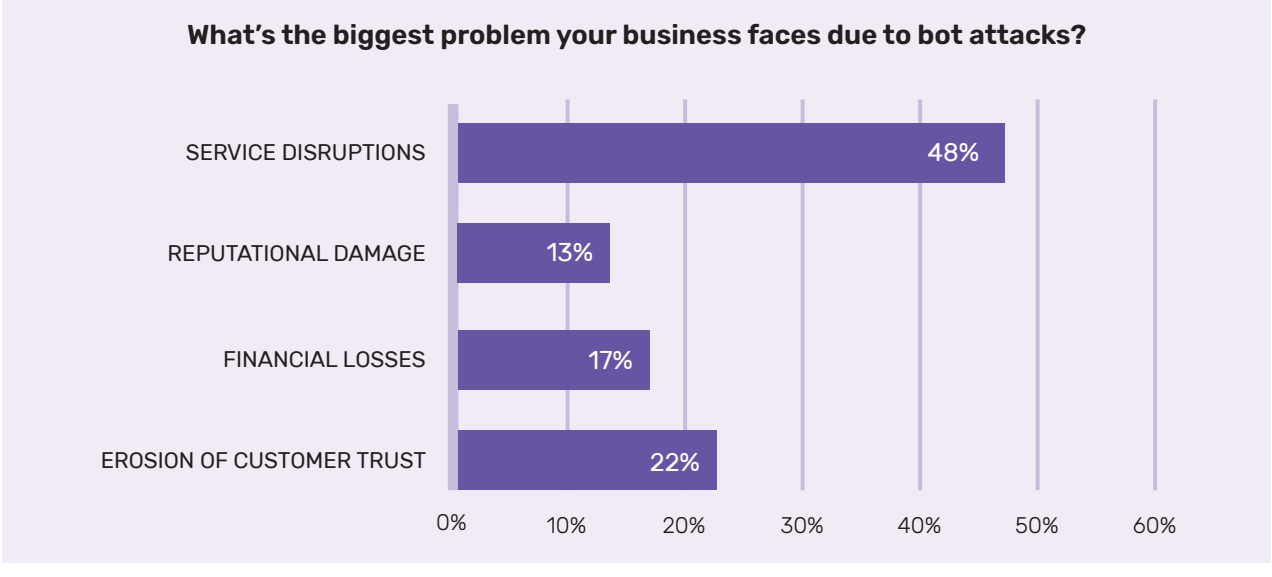
Top 10 BOT Attack Originating Countries

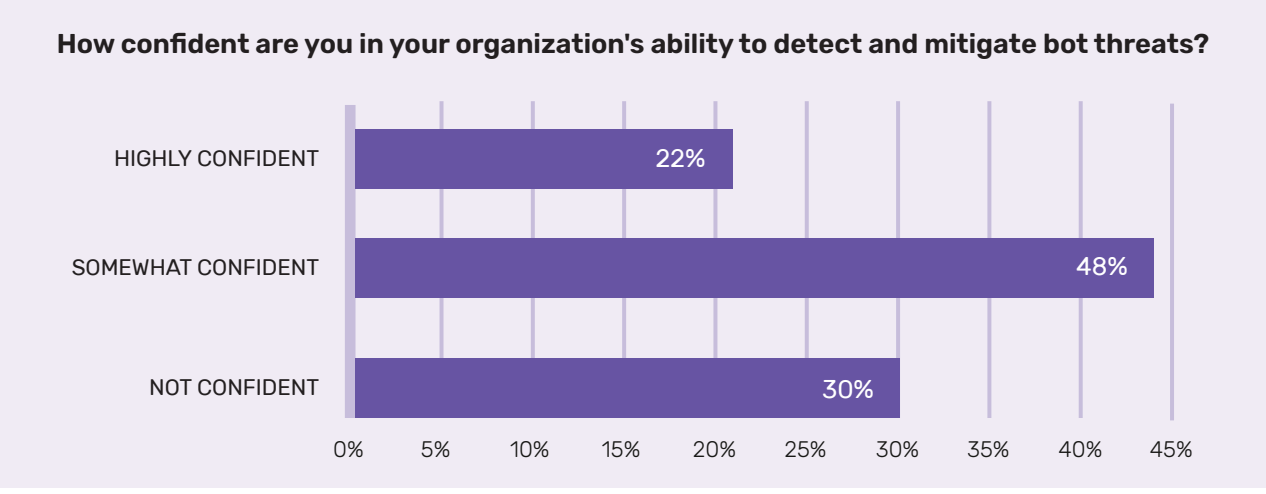
Country	Blocks
India	52551406
United States	50576189
Germany	6431466
Japan	3975660
Netherlands	3931271
Russian Federation	2854497
France	2550074
United Kingdom	2532523
Singapore	2262436
Bulgaria	1772595

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

Bot attacks rose 147% compared to Q1 2023, whereas 9 out of 10 sites witnessed a bot attack.

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.





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.

VULNERABILITY EXPLOITS

Total no. of critical and high vulnerabilities found in the applications: 17K

Top 10 critical and high vulnerability categories found:

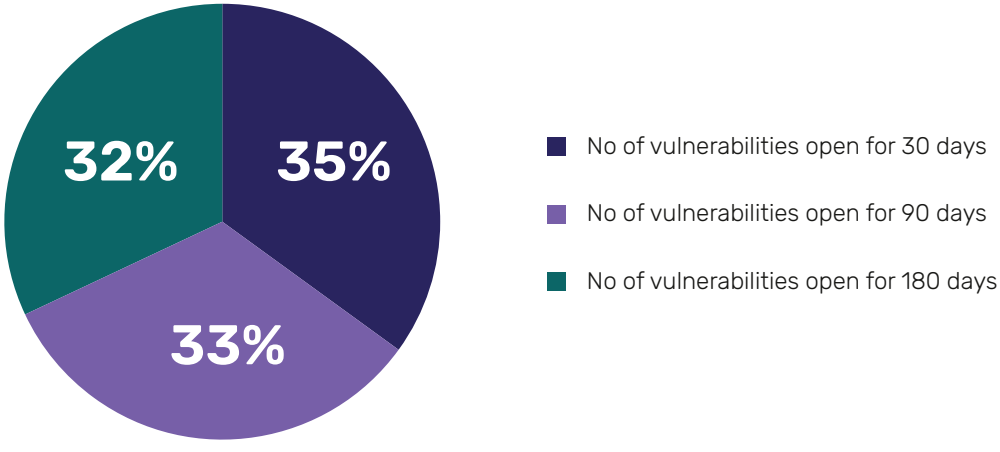
VULNERABILITY TYPE	TOTAL ALERTS FOUND
Apache OFBiz Authentication Bypass Vulnerability (CVE-2023-51467)	2081
SQL Injection	1433
Cross-Site Scripting (XSS)	405
HTML Injection	400
Server-Side Request Forgery Detected	337
Privilege Escalation	45
Insecure Direct Object References	36
TLS/SSL Server Certificate Expired	21
Apache Log4j RCE Vulnerability	19
Cross-Site Scripting (XSS) OOB	17

Aging trend of the website/application vulnerabilities

Over 1400 sites were analysed, and we found 17K 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 rather than a blocker.

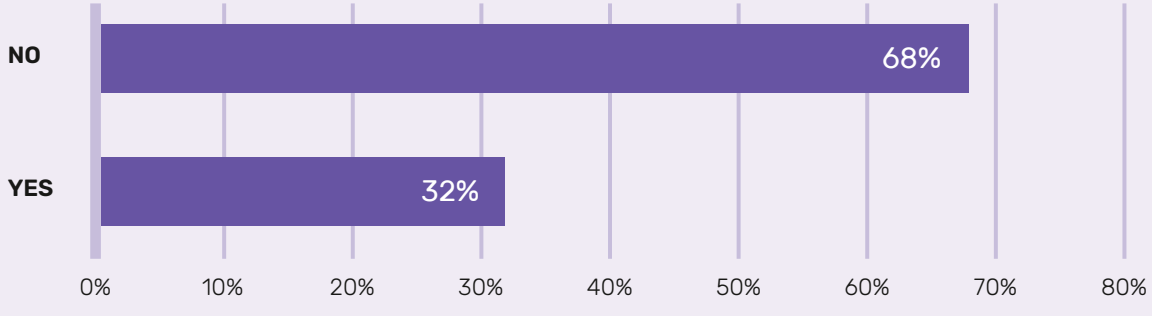
Open Vulnerability in Days



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.

Do you use virtual patching on WAF/WAAP?



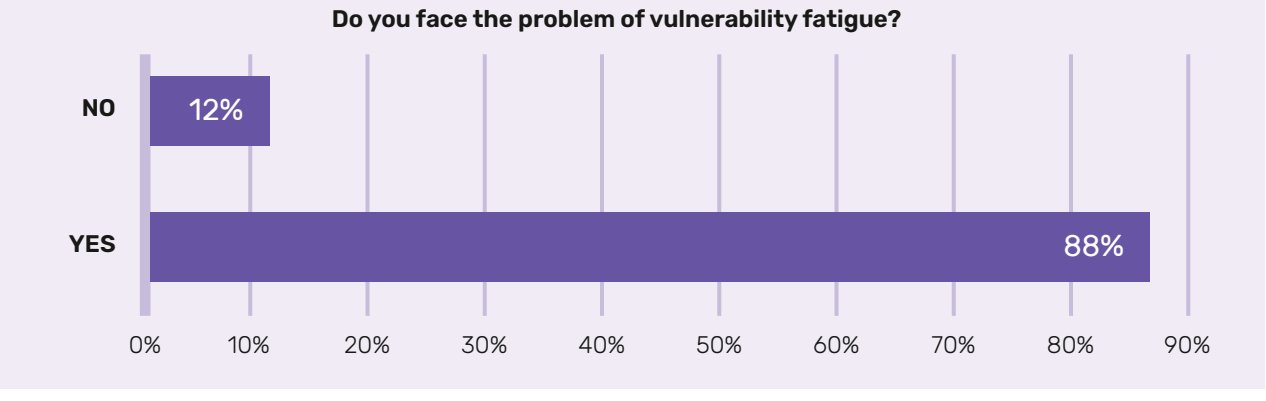
This could be because most of the WAFs/WAAPs don't come with an integrated DAST scanner, which helps the vendors understand how a vulnerability is found before patching it accurately.

Another reason could be that most of these companies do not opt for managed services, where the WAAP vendor writes the security policies, tests them for false positives and also does 24x7 false positive monitoring after pushing the policy live.

In contrast, we see a near 100% adoption of virtual patching among our customers, mainly because false positive testing is done by managed services that are bundled in AppTrana subscription plans.

In fact, with the release of SwyftComply, it is now easier for customers to virtually patch all the open vulnerabilities within 72 hours. It is as simple as clicking a button on the platform.

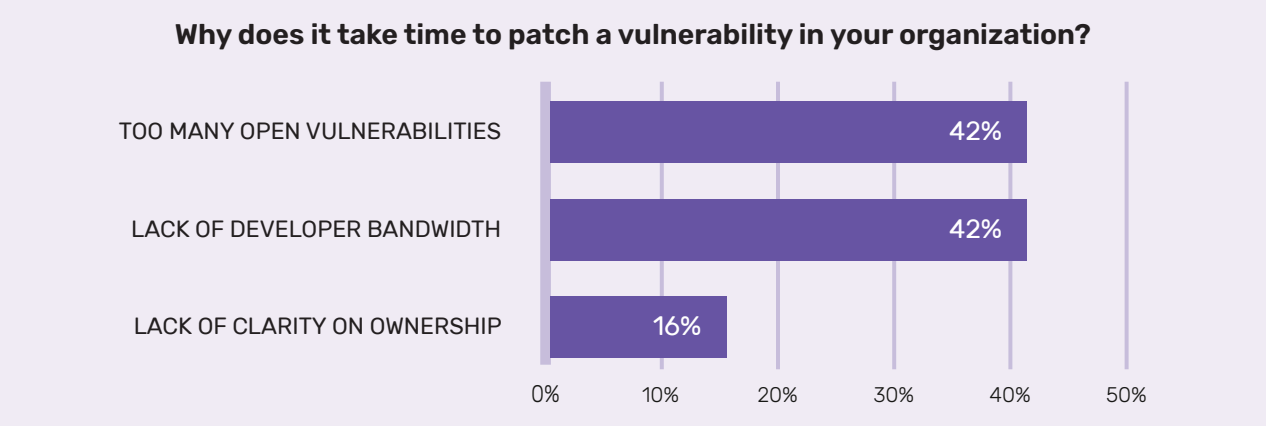
That said, prioritising which vulnerabilities to patch and fixing the vulnerabilities in code is a major challenge for the organisations and the below graph explains the same:



88% of customers face the problem of vulnerability fatigue. This is because an average organisation sees tens to hundreds of open vulnerabilities throughout the year, and finding the vulnerabilities that pose the highest business risk is difficult and time-consuming.

However, our customers who utilised the AcuRisQ feature in the Indusface DAST scanner were able to reduce fatigue by up to 80% and easily find and patch the vulnerabilities that cause the biggest business risks.

Here are some of the reasons why vulnerability patching is delayed:



Top 10 API vulnerability categories found:

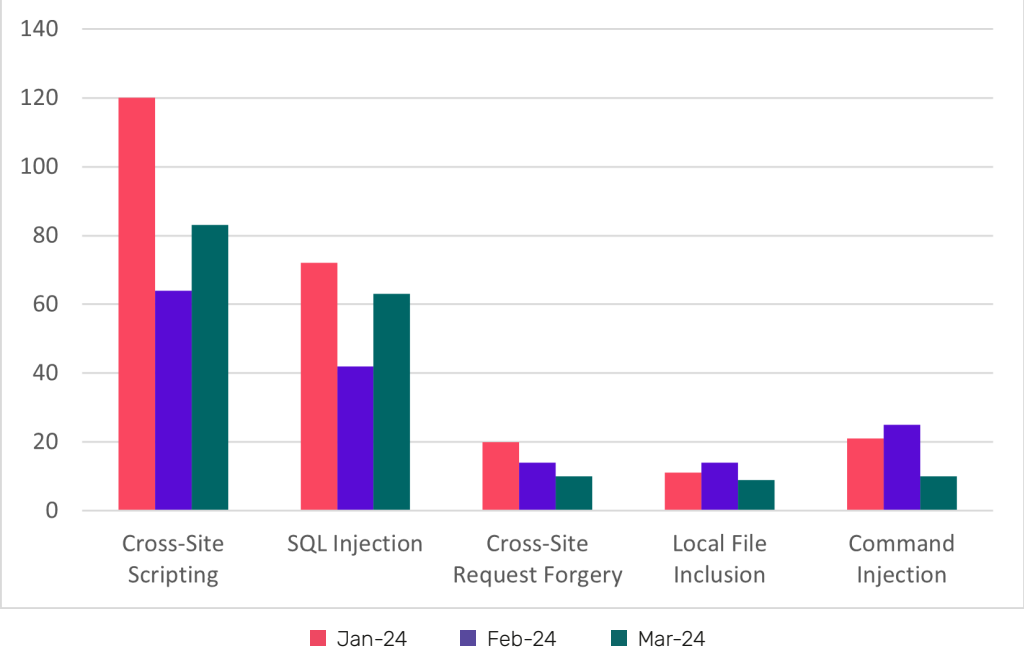
#	API Vulnerability Type
1	A3: Injection
2	A5: Security Misconfiguration
3	A7: Identification and Authentication Failures
4	A2: Cryptographic Failures
5	A1: Broken Access Control

Zero Day Vulnerabilities

In Q1 2024, **614** zero-day vulnerabilities were identified for the websites and APIs 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, around than 95% of zero-day vulnerabilities were protected by core rules, while the remaining 5% were safeguarded by custom rules, **resulting in 100% protection from zero-day** vulnerabilities throughout the year.

Top 5 zero-day vulnerability categories in Q1 2024:



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

Month	Jan		Feb		Mar	
Parameters	Value	Percentage	Value	Percentage	Value	Percentage
Total Vulnerabilities	257		174		183	
Protected by Core Rules	246	96%	160	92%	175	96%
Protected by Custom Rules	9	4%	14	8%	8	4%

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

- Critical Apache OFBiz Zero-day AuthBiz (CVE-2023-49070 and CVE-2023-51467)
- ScreenConnect Authentication Bypass (CVE-2024-1709 & CVE-2024-1708)
- CVE-2024-1071 – Critical Vulnerability in Ultimate Member WordPress Plugin

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

The below zero-day vulnerabilities were the top targeted in Q1 2024:

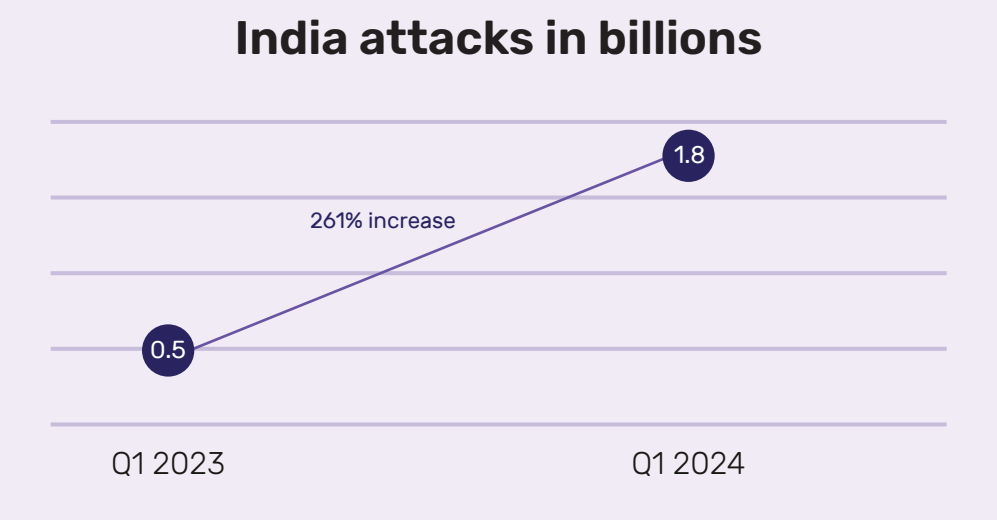
Zero day vulnerabilities	Attacks in Q1	No of sites targeted
CVE-2023-22515 - Broken Access Control Vulnerability in Confluence Data Center and Server Policy	10229	374
Auth bypass ScreenConnect CVE-2024-1708 and CVE-2024-1709 Policy	4193	409
CVE-2024-23897 Jenkins Code Execution Policy	7884	141
Apache OFBiz Auth bypass and Pre-Auth RCE Vulnerability (CVE-2023-49070 and CVE-2023-51467) policy	6522	332

INDIA DATA INSIGHTS

Total Attacks Count - India

1.80+ Billion

- Over 1.80 billion attacks were blocked in Q1 2024
- The cyberattacks in India grew by 261% in the Q1 of 2024 compared to the Q1 of 2023

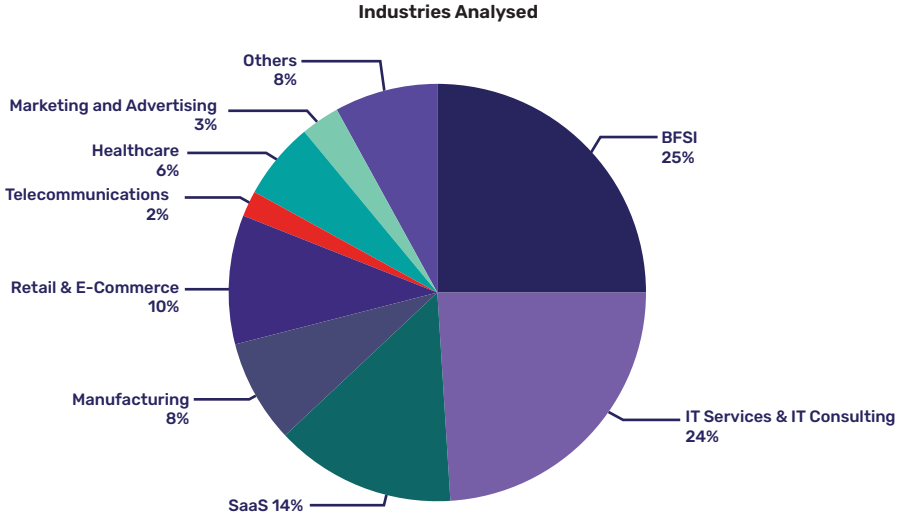


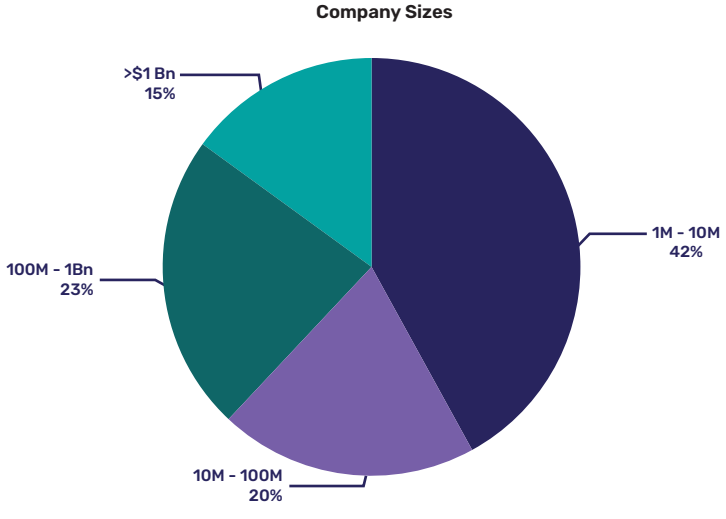
- In this quarter, power and energy companies faced up to 500x higher number of attacks than the industry average. This is because hackers are now finding options for ransom and targeting less regulated industries.
- Banking, Finance, & Insurance are the most targeted sectors overall.
- Banking and Finance sectors face 4x higher encoding attacks where hackers are using evasion techniques to bypass security measures and probe into sensitive data.
- The banking and Finance sectors also face 3x higher HTTP protocol enforcement attacks than the other industries. These attacks involve manipulating or abusing the HTTP protocol to escalate privileges and perform unauthorized actions like Injections, arbitrary code execution, etc.
- SQL injection attacks were the top vector in the banking, insurance, SaaS and retail industries. Whereas cross-site scripting attacks were the top attack vector in financial services and healthcare.
- 9 of 10 BFSI sites witnessed a bot attack throughout the quarter.
- Manufacturing industry is increasingly targeted with Local File Injection(LFI) attacks, where hackers try to access protected folders by manipulating inputs. Successful exploitation of such vulnerabilities may result in manipulation of application logic or functionality by including and executing malicious files.
- 100% of healthcare sites witnessed a bot attack.
- Retail, manufacturing and healthcare industries saw a higher number of bot attacks than DDoS attacks

Q1 2024 RESEARCH OVERVIEW

The State of Application Security Q1 2024 annual report is based on a sample size of 1400+ websites and applications that were analysed between January 1, 2024, and March 31, 2024.

During this period, various enterprise, government, and SME websites were analysed. The below figure illustrates the diversity of industries represented in this report.





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.

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.
- **LFI Attack**
    - LFI stands for Local File Inclusion. It's a type of vulnerability found in web applications that allows an attacker to include files on a server through the web browser.
- **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.

INDUSFACE™

CUSTOMER TESTIMONIALS

Kiran Belsekar

Executive Vice President - CISO & IT Governance, Aegon Life

The Risk Based Fully Managed Application Security technology offering from Indusface provided us the best value for money.

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.

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.

INDUSFACE IS THE ONLY CLOUD WAAP (WAF) VENDOR WITH 100% CUSTOMER RECOMMENDATION FOR 4 CONSECUTIVE YEARS

A CUSTOMERS' CHOICE FOR 2024, 2023 AND 2022 GARTNER® PEER INSIGHTS™

Gartner Peer Insights Customers' Choice 2024

INDUSFACE™

BENGALURU | VADODARA | MUMBAI | NEW DELHI | DALLAS TX

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

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