INDUSFACE™

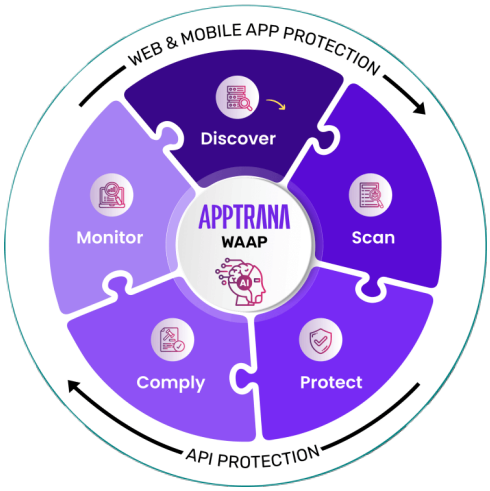
STATE OF APPLICATION SECURITY

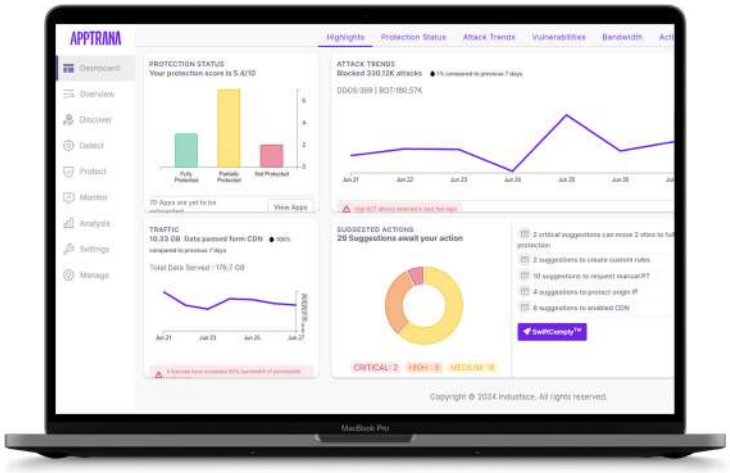
Q2 2024

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 2.37 billion attacks were blocked from 1st April 2024 to 30th June 2024
- On average, 960K attacks were blocked per website
- Cyberattacks grew by 105% in the Q2 of 2024 compared to the Q2 of 2023
- Bot attacks rose by 213% in Q2 2024 compared to Q2 2023:
    - 276+ million bot attacks in Q2 2024
    - 835+ million DDoS attacks in Q2 2024
- 6 out of 10 sites witnessed a DDoS attack, whereas 9 out of 10 sites witnessed a bot attack
- 25K critical and high vulnerabilities were found - 31% of these vulnerabilities were open for 180+ days
- Attacks on vulnerabilities grew by 1,200% in Q2 2024 compared to Q2 2023. A big part of this could be because of the widespread use of LLM tools such as ChatGPT enabling novice hackers to easily find and deploy scripts that could exploit open vulnerabilities
- The cyberattacks in India grew by 115% in the Q2 of 2024 compared to the Q2 of 2023
- 59% of attacks have been blocked with application-specific virtual patches and security policies, thereby reinforcing the importance of managed WAAP
- The Small and Medium Businesses (SMBs) globally faced over 559 million attacks across a sample of 500 websites in Q2 2024
    - DDoS is the #1 attack vector, where each website/app is seeing 124% more DDoS attacks when compared to the enterprise apps. This could be because DDoS attack monitoring requires either a managed WAAP or a specialised, 24x7 security operations centers (SOC) and SMBs can ill-afford them
- Power and energy companies faced up to 25 times higher number of attacks than the industry average. This could be because non-regulated industries with less stringent security requirements are soft targets for hackers

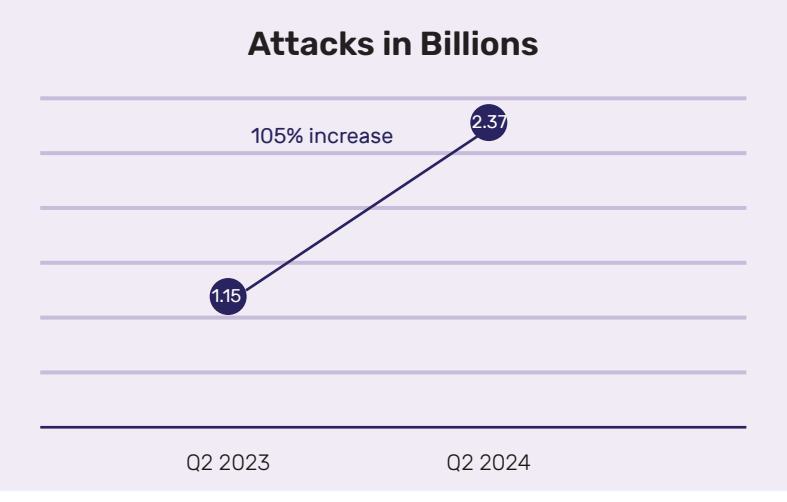
- SQL injection attack is the top vulnerability attack in the Banking, Financial Services, Insurance, Healthcare, and Retail sectors thereby reinforcing the importance of protecting critical customer data, including PII, credit card information and others that these applications host
- The banking, financial services and insurance sectors witnessed 45%-60% higher bot attacks
- The manufacturing industry faces 10X higher cross-site scripting (XSS) attacks compared to other industries

PROTECTION TRENDS:

Total Attacks Count

2.37+ Billion

We saw over 2.37 billion requests that got blocked across all sites protected by AppTrana.
The number of attacks increased by 105% in Q2 2024 compared to Q2 2023.

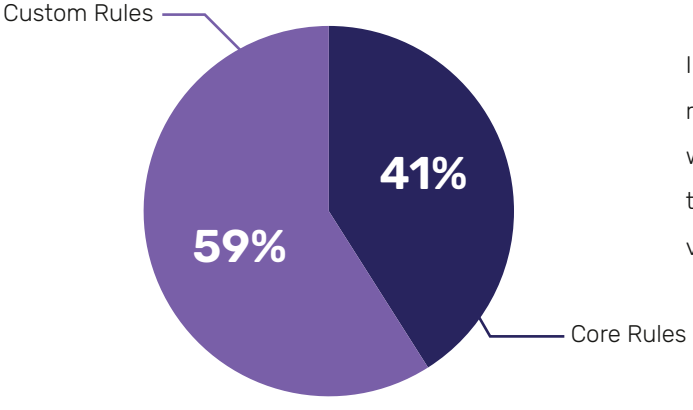


A view of the last 90-day attacks' trend across all sites:

Top 10 Attack Originating Countries

Country	Blocks
India	1722864193
United States	354654008
Germany	54002114
Taiwan	44963029
Singapore	33926472
France	28836929
Netherlands	17838426
United Kingdom	12682420
Japan	11489852
Russian Federation	10241492

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, Germany, and Taiwan.



In Q2 2024, just like last year, approximately 41% of requests were blocked by AppTrana's default rule set, while 59% were blocked by custom rules tailored to the specific needs of applications—highlighting the value of the managed services provided by AppTrana.

DDOS & BOT ATTACKS

- As new DDoS and bot attack trends emerge against web applications and APIs, business continuity becomes very important.
    - AppTrana WAAP guarantees zero false positives and ensures 100% uptime against layer 3-7 DDoS attacks with AI-driven behavioural DDoS mitigation and rate-limiting based on URI, IP, host, and geo. Click here to learn more.
    - Against bot attacks such as account takeover, credential stuffing, and scraping, AppTrana WAAP provides protection from day zero with AI-driven behavioural bot protection, real-time analysis of bot traffic, correlat-ed risk scoring, anomaly detection, and custom controls. Click here to know more.

We saw the following DDoS and bot trends in Q2 2024:

DDoS Attacks

Total Sites Affected by DDoS Attacks	Total DDoS Attacks
60%	**835+ Million**

Here is a view of the last 90-day DDoS attack trend across all sites:

Top 10 DDoS Attack Originating Countries

Country	Blocks
India	597209725
United States	83401174
Germany	40053700
Singapore	8362394
United Kingdom	5119885
Hong Kong	4173554
Japan	2287162
Netherlands	2216575
France	2031645
Sweden	1979986

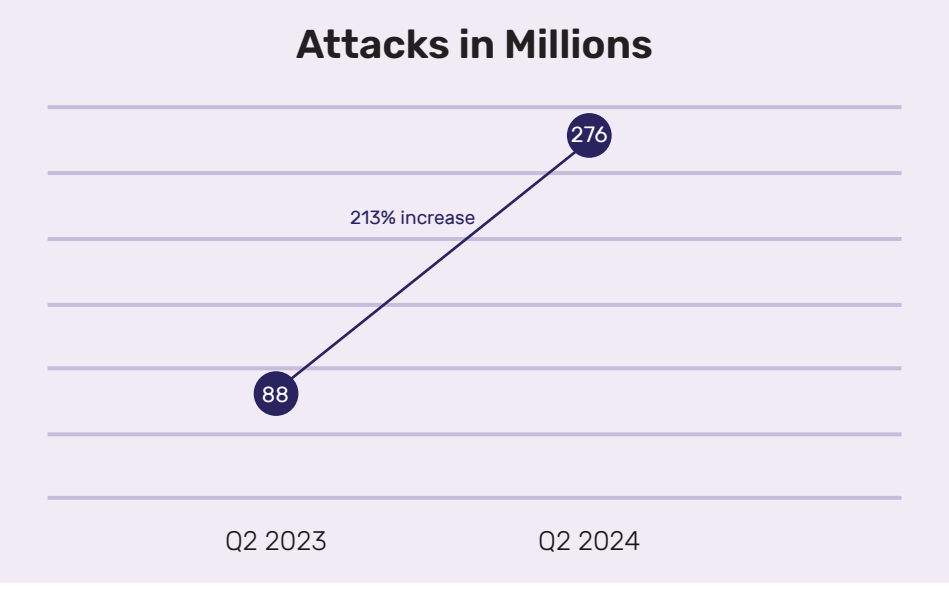
Major countries from where DDoS attacks were observed other than India are the United States, Germany, and Singapore.

In Q2 2024, 6 out of 10 sites witnessed a DDoS attack.

Bot Attacks

Total Sites Affected by Bot Attacks	Total Bot Attacks
90%	**276+ Million**

Here is the Q-o-Q visualisation of the bot attacks blocked in Q2 2024 vs. Q2 2023.



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

Top 10 BOT Attack Originating Countries

Country	Blocks
India	106103028
United States	78898659
Taiwan	27452730
Germany	10427328
Singapore	6208448
United Kingdom	5224390
Russian Federation	5071862
Japan	4912646
Netherlands	4835136
France	3064140

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

Bot attacks rose 213% compared to Q2 2023, whereas 9 out of 10 sites witnessed a bot attack.

VULNERABILITY EXPLOITS

Attacks on vulnerabilities surged by **1,200% in Q2 2024.** A big part of this could be because of the widespread use of LLM tools such as ChatGPT, which enable novice hackers to easily find and deploy scripts that could exploit open vulnerabilities. This accessibility has lowered the barrier to entry for cybercriminals, resulting in an unprecedented rise in vulnerability exploitation.

Total no. of critical and high vulnerabilities found in the applications in Q2 2024: **25K**

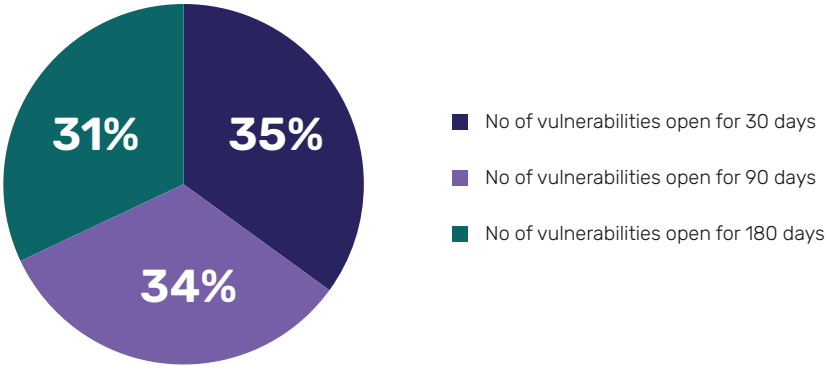
Top 10 critical and high vulnerability categories found:

VULNERABILITY TYPE	TOTAL ALERTS FOUND
Blind SQL Injection	9655
Trojan Shell Script	4084
Server Side Request Forgery	262
HTML Injection	224
Cross-Site Scripting (XSS)	143
SQL Injection	104
Apache Log4j RCE Vulnerability	48
Insecure Direct Object References	39
Privilege Escalation	37
SQL Injection OOB	19

Ageing trend of the website/application vulnerabilities

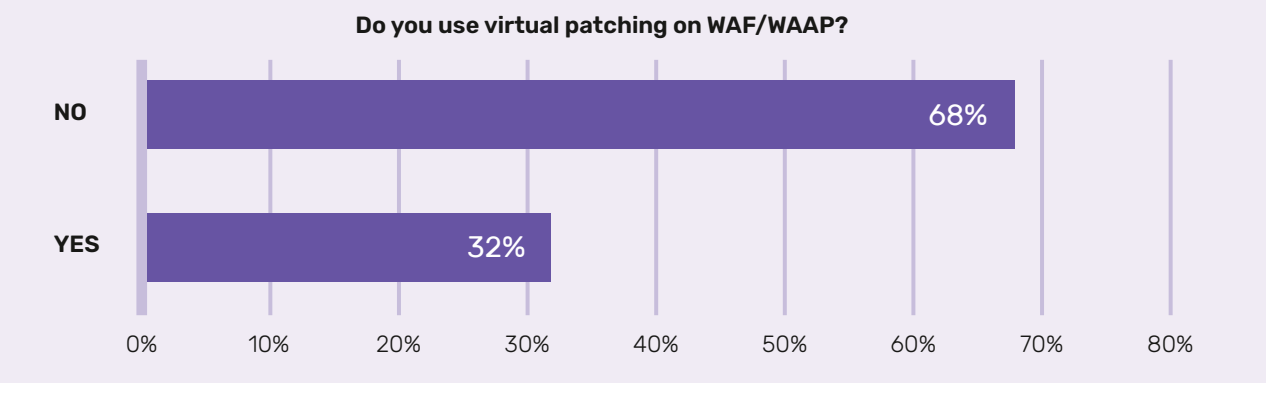
Over 1,400 sites were analysed, and we found 25,000 critical and high vulnerabilities. Around 31% of these vulnerabilities had been open for more than 180 days.

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 instead of a blocker.



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.

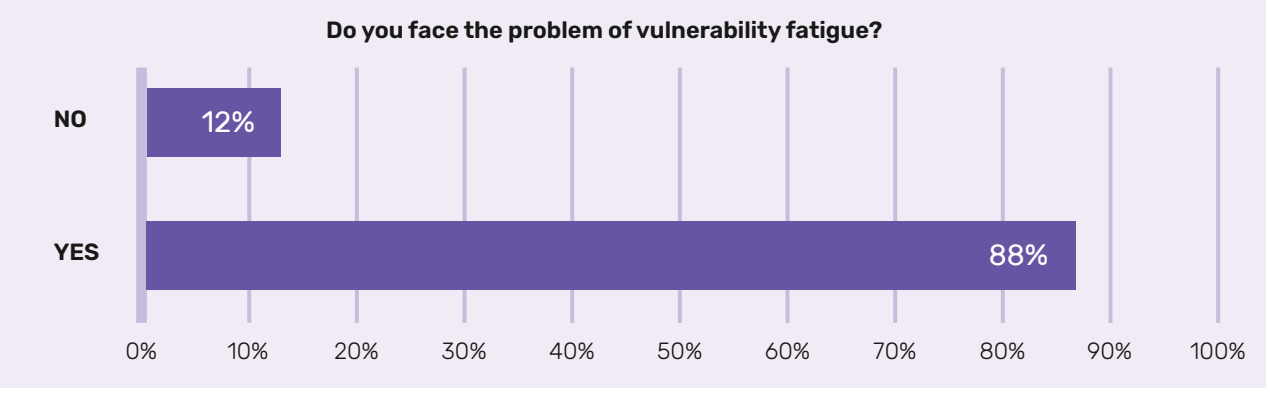


This may be because most WAFs/WAAPs don't include an integrated DAST scanner, which helps vendors understand how a vulnerability is detected before they can accurately patch it.

Another reason could be that most of these companies do not opt for managed services, where the WAAP vendor writes the rules and removes false positives.

In contrast, we observe nearly 100% adoption of virtual patching among our customers, primarily because false positive testing is handled by managed services included in AppTrana subscription plans.

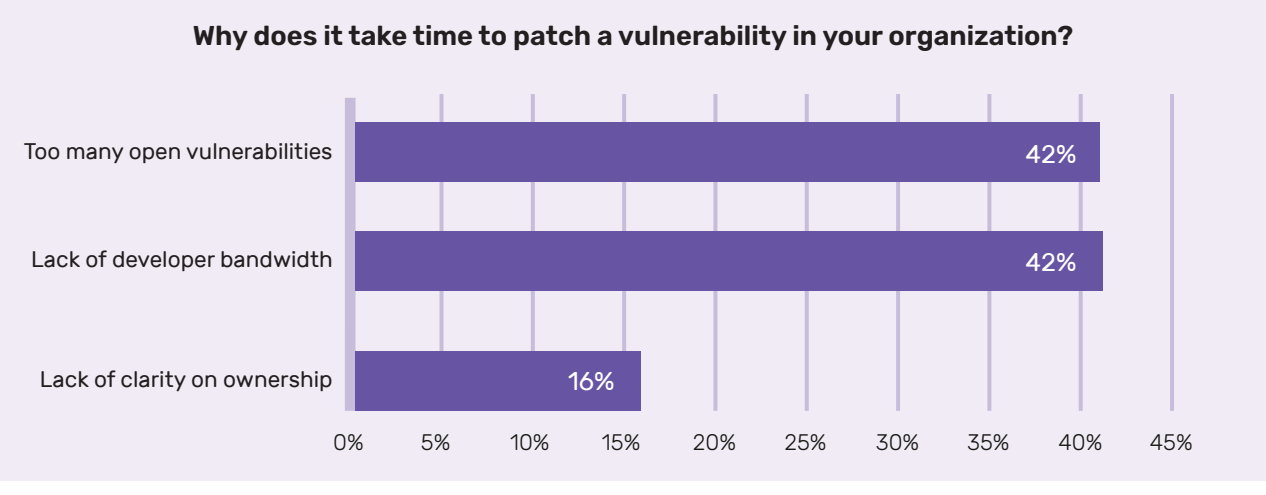
That said, prioritizing which vulnerabilities to patch and fixing vulnerabilities in the code remains a major challenge for organizations. The graph below illustrates this issue:



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 that security leaders mention why they take the time to patch a vulnerability in their organization:



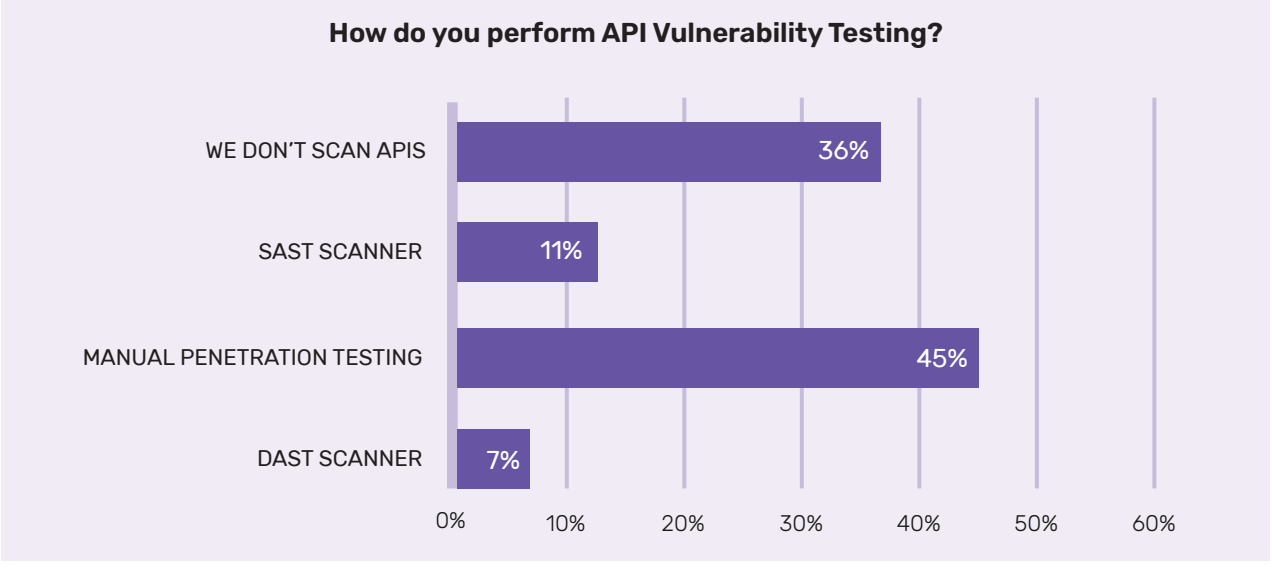
Top OWASP API vulnerability categories found:

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

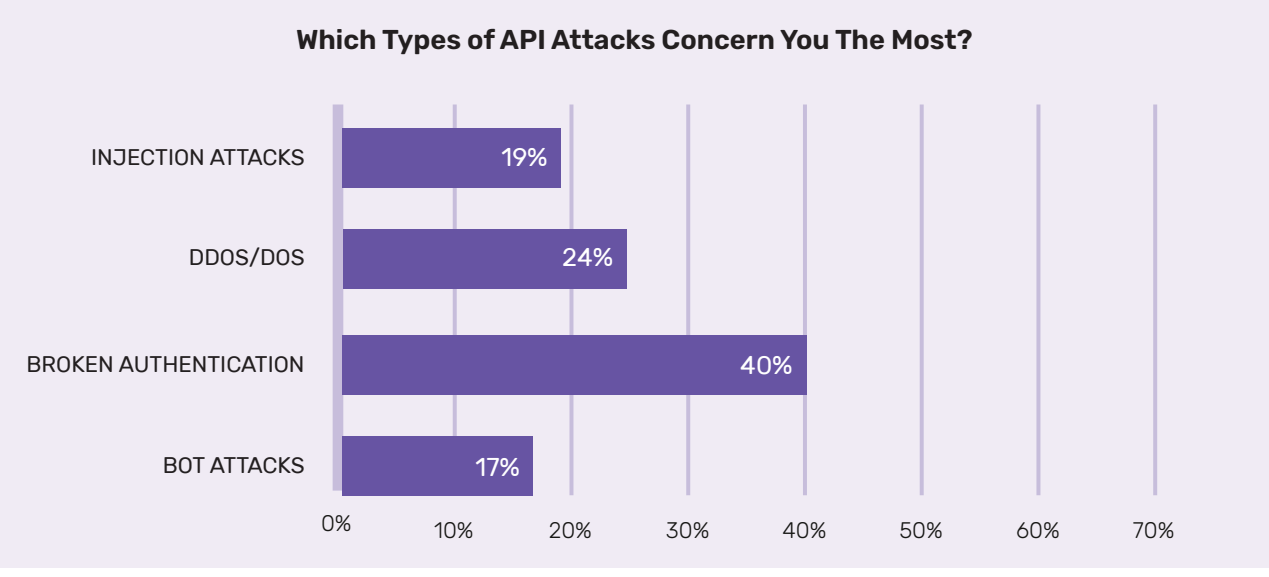
We asked security leaders about the testing methods they use to protect against API-specific vulnerabilities. It was surprising to find that around 36% of organizations don't scan their APIs at all, and only 7% use automated DAST scanners, which are among the easiest methods for scanning APIs for vulnerabilities.

While penetration testing is a best practice, it is often expensive, time-consuming, and usually conducted only once a year.

Indusface's DAST scanner for APIs typically identifies over 90% of the vulnerabilities found in manual penetration testing and completes the scan within a few hours. Additionally, it features CI/CD integration, allowing you to automatically trigger scans with code check-ins and assign open vulnerabilities to the development team for timely patching.



We also tried to understand which types of API attacks concern the security leaders the most, and broken authentication emerged as the top attack vector across organizations.

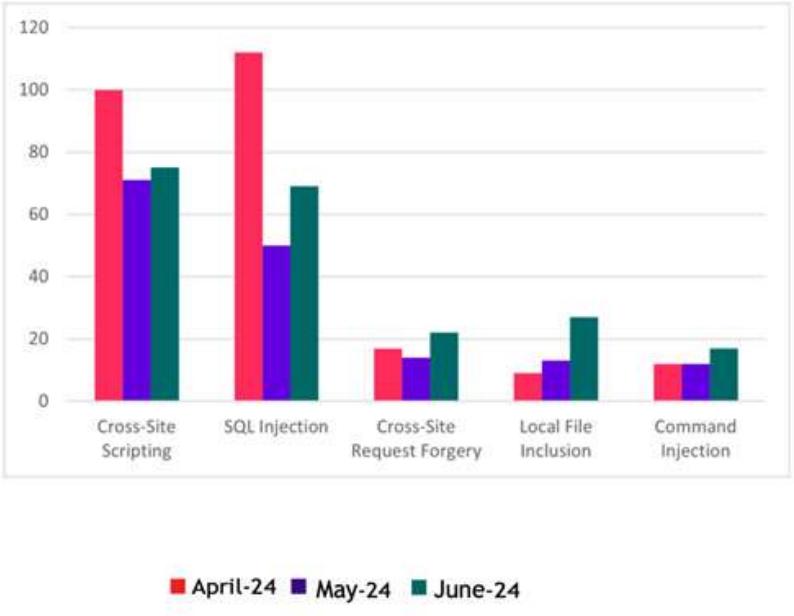


Zero Day Vulnerabilities

In Q2 2024, **644** zero-day vulnerabilities were identified for the websites protected by the AppTrana WAAP.

Most of our customers have utilized the risk-based protection of AppTrana, ensuring the detection and protection of zero-day vulnerabilities. By default, approximately 97% of zero-day vulnerabilities were protected by core rules, while the remaining 3% were safeguarded by custom rules, resulting in 100% protection from zero-day vulnerabilities throughout the quarter.

Top 5 zero-day vulnerability categories in Q2 2024:



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

Month	April		May		June	
Parameters	Value	Percentage	Value	Percentage	Value	Percentage
Total Vulnerabilities	260		169		215	
Protected by Core Rules	250	96%	160	95%	212	99%
Protected by Custom Rules	10	4%	9	5%	2	1%

In Q2 2024, the below zero-day vulnerabilities were the top attacked

- Apache OfBiz CVE-2023-51467 Auth bypass
- Auth bypass ScreenConnect CVE-2024-1708 and CVE-2024-1709
- Jenkins Remote Code Execution Policy CVE-2024-23897

Amidst known vulnerabilities, a critical zero-day, PHP CGI Argument Injection (CVE-2024-4577) Vulnerability in Windows Servers was identified as well.

GLOBAL SMALL AND MEDIUM BUSINESS (SMB) ATTACK INSIGHTS

Total SMB Sites Analysed	Total Attacks Count – Global SMBs
500	**559+ Million**

- Over 559 million attacks were blocked in Q2 2024
- On average, 112K attacks were blocked for SMBs per site
- The SMB sector witnessed 4X higher open vulnerabilities (C+H) compared to the enterprises. This could be because SMBs typically have smaller security teams, and an increase in vulnerabilities may lead them to face alert fatigue as well as spend more time patching them.
- 378+ million DDoS attacks and 56.9 million attacks are witnessed in the SMB sector in Q2 2024
    - 1.27+ million DDoS attacks witnessed per site
    - 120K+ bot attacks witnessed per site
- The SMB sector faced 124% more DDoS attacks per site than the global average.

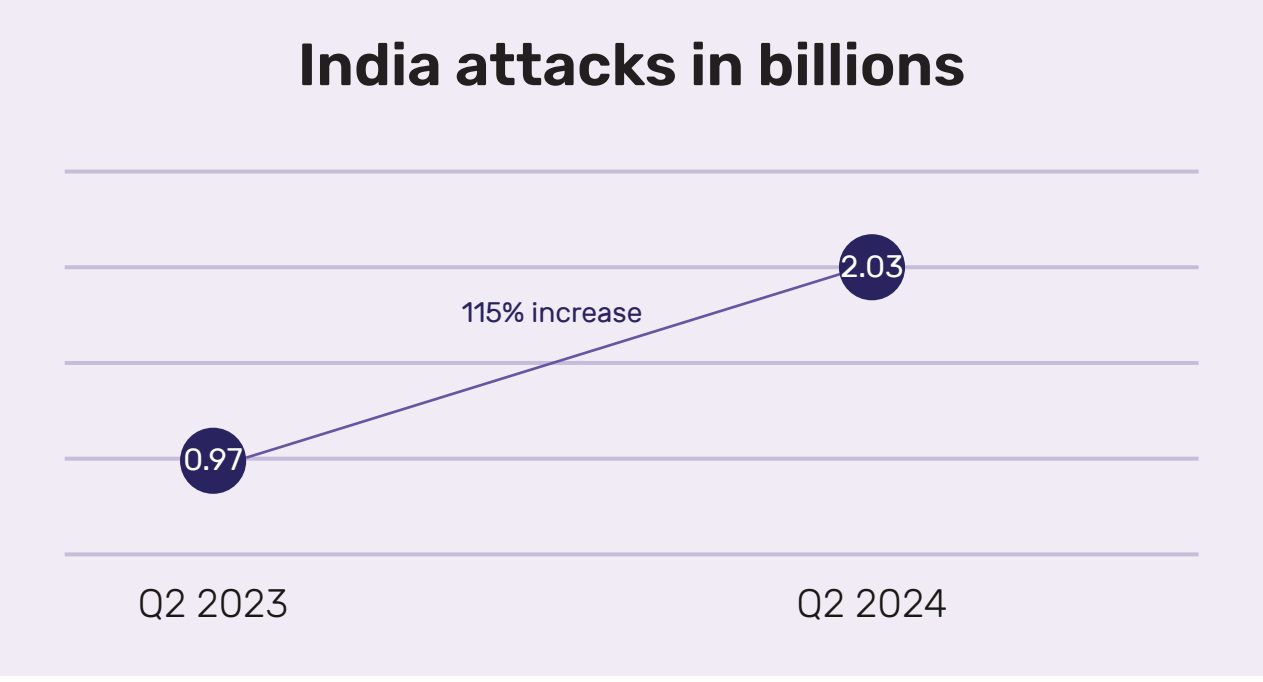
DDoS mitigation is complex and typically requires continuous 24/7 monitoring for application attacks. This can be especially challenging for SMBs, where security is often a part-time responsibility handled by tech or DevOps teams.

AppTrana offers a fully managed WAAP solution that is cost-effective, even for SMBs. This solution assists with DDoS monitoring, reduces issues related to alert fatigue, and supports virtual patching of open vulnerabilities

INDIA DATA INSIGHTS

Total Attacks Count - India
2.03+ Billion

- Over 2 billion attacks were blocked in Q2 2024
- The cyberattacks in India grew by 115% in the Q2 of 2024 compared to the Q2 of 2023



Industry-Wise Data Trends

Power & Energy:

- Power and energy companies faced up to 25 times the industry average number of attacks. In fact, they faced the highest number of attacks per site, with an average of 25 million attacks per site.
- This is due to hackers now seeking ransom options and targeting less regulated industries having a strong revenue stream.

Banking, Financial Services, and Insurance:

- SQL injection attack is the top vulnerability attack in the Banking, Financial Services, and Insurance sectors thereby reinforcing the importance of protecting critical customer data, including PII, credit card information, and others that these applications host
- The banking, financial services, and insurance sectors witnessed 45%-60% higher bot attacks per site compared to the global average.

- The highly regulated nature of these sectors means that the applications already have a robust infrastructure for cybersecurity. This could be one reason why they are targeted by bots more than other attack vectors such as DDoS. Bots are tougher to detect and could be used for a variety of exploits including vulnerability scanning, account takeover, credit card scams, and so on.

Manufacturing:

- The manufacturing industry faces 10X higher Cross-site scripting (XSS) attacks.
- Unlike BFSI and healthcare, which typically host sensitive PII and other data, the manufacturing industry has less sensitive data that could be exploited for ransom. This could be the reason why the manufacturing industry is mostly targeted by XSS attacks that are typically used to spread malware, deface websites, and so on. This makes it easier for hackers to demand ransom.

Healthcare:

- 100% of healthcare sites witnessed a bot attack

Retail & E-commerce:

- Retail industries face 2X as many bot attacks and 3X times more vulnerability exploits compared to DDoS attacks. The most common bot attacks on retail and e-commerce sites are credential stuffing and carding. Both these bots essentially try to place orders and commit purchase fraud.

CUSTOMER ATTACK STORY OF THE QUARTER

Application Attacks on Banking and Insurance Sites by Expiravit PMC Hacktivist Group

Solution Highlights:

- Banking and insurance websites faced a coordinated attack by Expiravit PMC hacktivist group
- Utilization of LLM tools by the script kiddies to perform targeted attacks
- 100% of attacks blocked by the AppTrana core rule set and the AI engine

Overview:

A large group of banking and insurance websites faced a coordinated attack by a hacking group known as Expiravit PMC. This group, primarily composed of script kiddies, employed a range of readily available exploitation tools and techniques to target multiple sites.

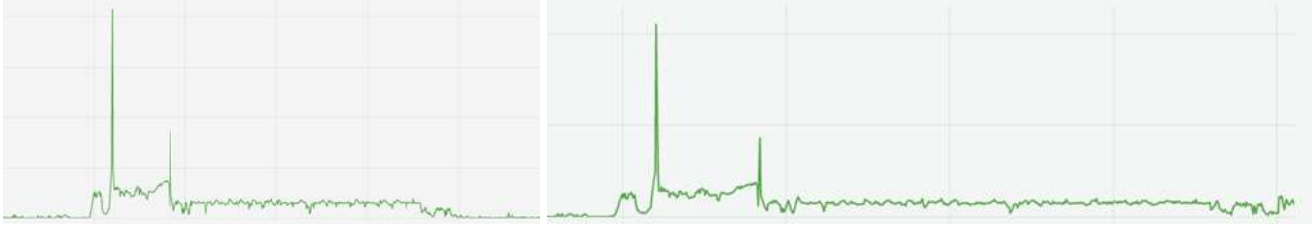
Attack Details:

- The hacking group executed a sequence of application-layer attacks on banking and insurance companies globally, utilizing a series of around 10,000+ IP addresses.
- They attempted various attacks such as cross-site scripting (XSS), SQL injections, command injections, path traversal, and other OWASP Top 10 vulnerabilities.
- The hacking group primarily relied on commonly used tools (bXSS, XSSer, Sqlmap, etc.) and utilized the most common hacking practices and exploitation scripts to perform the above-mentioned attacks.
- Additionally, the hackers may have also utilized LLM tools like ChatGPT, as a few automation scripts were customized to enhance the context-specific targeting of these applications to increase the chances of successful exploitation.
- They attempted attacks from various countries/locations to avoid detection, using diverse countries such as the US, India, Germany, Finland, Luxembourg, Russia, Poland, and more.
- The main aim of script kiddies would have been to create a distraction and attract attention to themselves. If successful, such attacks are also used as decoys to launch targeted attacks in other areas of the organization.

Solution:

- The layered 'always on' protection in AppTrana proved effective in safeguarding against a variety of attacks that were launched.
    - Its granular AI-backed behavioural DDoS policies were able to identify abnormal behaviours at the IP level and block malicious requests.
    - Additionally, in instances of low-rate attacks, the behavioural model notified the managed service team, providing insights into the attacks.
    - Leveraging AI-driven insights, Indusface's managed service team was able to quickly narrow down an abnormal pattern and apply sophisticated DDoS policies to ensure targetted attacks were blocked
- In a short time span, AppTrana completely blocked all IP address used by the attackers, protecting all sites that exhibited similar behaviour patterns.
- For attacks such as XSS, SQL injection, and others aimed at the OWASP top 10, AppTrana's core rule set automatically blocked all the attacks without the need for creating any sort of custom rules.
- This also lead to increase in risk score of IPs in AppTrana's bot module which tracks for abnormal behaviours, leading to blocks of certain attacks from BOT module.
- For all the targeted banking and insurance sites, the AI engine automatically increased the bot tolerance levels and ensured that even a minor anomaly in the request would be blocked at the highest priority.
- Even when hackers tried to use custom scripts for defacement, potentially utilizing LLM tools, AppTrana's robust core rule set effectively blocked 100% of these attacks.
- The combined measures effectively thwarted the attacks, causing the script kiddies targeting multiple sites to eventually give up within a few hours after seeing no success.

Attack neutralization images of a few sites:



Conclusion:

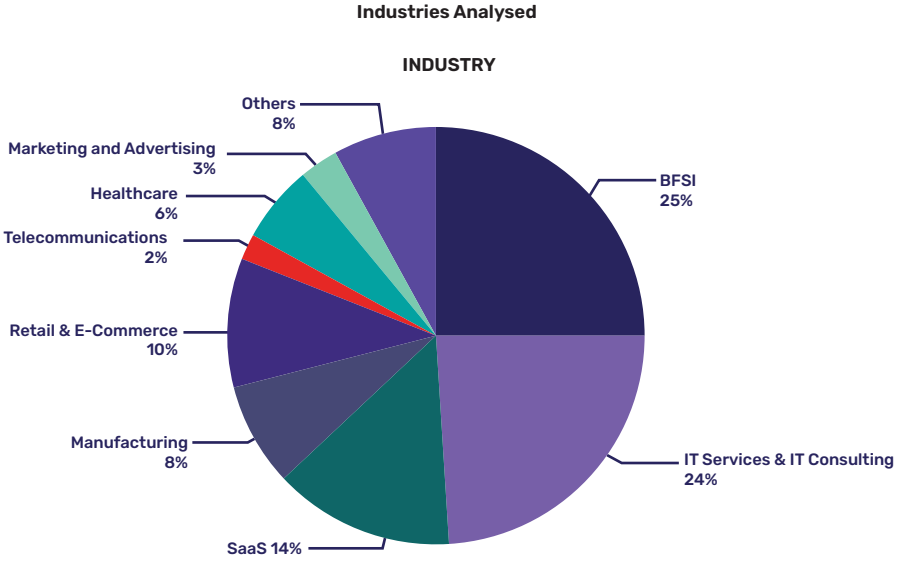
LLM tools like ChatGPT are reducing the barrier to entry for novice hackers and script kiddies, making it easier for them to launch sophisticated attacks. However, it is just a matter of time before script kiddies become more advanced as they continue to improve their hacking skills. Although in this case the core rule set worked well, future scenarios with an increase in custom attacks and sophisticated bot deployments will require more custom rules and a combined human and AI-based approach to attack mitigation.

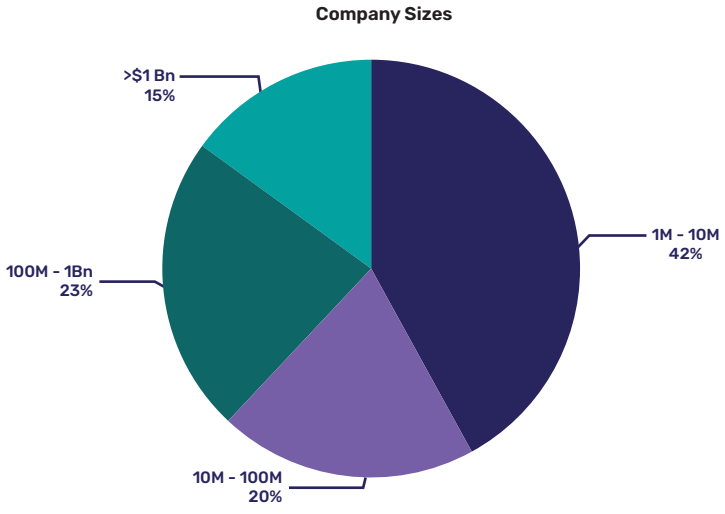
Therefore, having robust application security tools like AppTrana that provide multi-layered 24/7 AI Driven protection is essential to ensure that any and all kinds of attacks are thwarted before they can cause any threat.

Q2 2024 RESEARCH OVERVIEW

The State of Application Security Q2 2024 annual report is based on a sample size of 1400+ websites and applications that were analysed between April 1, 2024, and June 30, 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.
- **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, Bandhan 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

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

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