DATASHEET

INDUSFACE™

AppTrana - DDoS Mitigation

AI-powered, fully managed DDoS mitigation for websites and APIs

Any application accessible over the internet is prone to distributed denial-of-service attacks (DDoS/DoS). DDoS attacks vary and can be performed via multiple methods and, hence, are complex to protect against. As per Indusface's latest research, around 60% of sites faced a DDoS attack over the last year.

With AppTrana's AI-driven behavioral DDoS protection, you receive comprehensive protection against all types of DDoS attacks, backed by a zero false positive guarantee.

KEY FEATURES

Instant & Scalable Protection

Block DDoS attacks up to 2.3 Tbps and 700k requests per second right from day zero with highly scalable AWS infrastructure. Protect your applications and APIs against layer attacks (ICMP / UDP flood attacks), protocol attacks (like SYN flood attacks, UDP reflection attacks), and application layer attacks (like HTTP flood, Slow/low attacks, etc.)

Behavior-Based DDoS Protection

Ensure round-the-clock availability of your application by mitigating volumetric DDoS attacks with the AI-powered, unmetered, and always-on DDoS scrubber. Deploy machine learning based policies that adjust according to the typical behavior of traffic for the website demarcated at IP, session, host, and geographies. Receive alerts based on thresholds and automate DDoS attack blocks after a specified level.

URI-Based DDoS Protection

Ensure protection against account takeover and credential stuffing attacks through URI-based DDoS protection, an industry first. Leverage URI-based DDoS protection at various URIs including login page, check out pages, sign-up, and pricing pages.

Comprehensive & Unmetered Protection

Don't get penalized for being under attack. Get billed only for the legitimate traffic that is passed to your origin. AppTrana provides comprehensive DDoS attack protection, which is unmetered and always on.

24*7 SOC

Don't worry about building a security team to manage WAF. Leverage Indusface security experts 24X7 for protection against complex DDoS attacks. Get immediate alerts around complex alerts and recommendations to thwart complex attacks without affecting availability. Leverage the managed services team for custom rules to deploy tarpitting, captcha and other DDoS mitigation methods.

Content Delivery Network (CDN)

Get protection without compromising on speed. Accelerate your site through AppTrana's CDN ensuring cacheable content is served from edge networks nearest to your user. Work with our experts to plug-in your CDN or get our CDN configured for your application to ensure maximum efficiency

HIGHLIGHTS

24X7, fully managed DDoS mitigation

AI/ML based rate-limiting

Granular rate-limiting on URI, IP and GEO

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™

DDoS THREATS COVERED:

Attack Vectors	Details
Network Layer Attacks	
Reflection Attacks	Spoofing IP to make legitimate third party to send request to Victim
SMURF Attacks	Vulnerability in ICMP protocol exploited to make network inactive
ACK Attacks	Overloading server with TCP ACK
Flood Attacks（UDP/TCP/ICMP）	Flooding Server with requests to exhaust resource and make the server unavailable
Network Port scanning	Port scans done to exploit vulnerabilities found
Application Layer Attacks	
Slowloris	Send partial HTTP requests to a server, causing the server to wait for the rest of the request. As the server keeps waiting, it exhausts its resources, leading to a denial of service.
Slow Read attacks	Sends a request to server but does not read in a timely manner from the server
Slow POST attacks	Induces the server to expect a POST request of a specific length but either sends no data or sends it very slowly, causing the server to wait and exhaust its resources
HTTP Flood（GET & POST Attacks）	Requests are sent from a network of compromised devices（zombie army）, often one request at a time. Because they stay below traffic thresholds, these attacks are hard to detect but can overwhelm the server over time.
Resource exhaustion	Targeting a specific resource that can be exhausted, such as memory or connection pools, to overwhelm the system and cause a denial of service
Brute force attacks	A trial-and-error method used to break encryption by systematically testing all possible combinations until the correct one is identified.
Large payload POST Attack	Oversize payload attack where DOM Parser payload is increased to cause memory exhaustion
SSL exhaustion	Sending garbage data to an SSL server to exhaust its SSL connection pool, causing it to become overwhelmed and unable to handle legitimate requests.
Mimicked User Browsing	Sending requests that imitate normal user behavior, overwhelming the server and exhausting its resources.
Database connection pool exhaustion	Sending queries that keep database connections open, preventing new connections and exhausting the connection pool