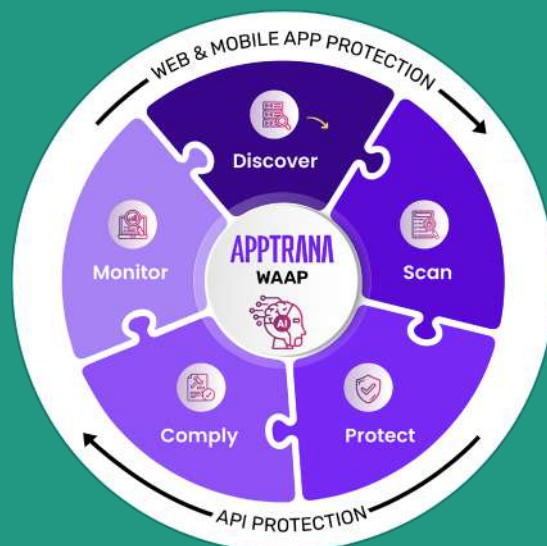# AI-Powered, Fully Managed Application and API Protection

Integrated platform for managed WAF, API security, DDoS & bot protection, DAST and manual penetration testing

AppTrana Cloud WAAP (WAF)

The only Cloud WAAP (WAF) with 100% customer recommendation for 4 consecutive years

A Customers' Choice 2024, 2023 and 2022 Gartner® Peer Insights™

Key Differentiators of AppTrana WAAP

SwyftComply – Security Compliance within 72 Hours

Comply with SOC2, ISO:27001, PCI, GDPR, RBI, and other regional security guidelines within 72 hours through a zero-vulnerability report. Post onboarding, Indusface security experts constantly identify zero-day, OWASP Top 10 & business-logic threats via DAST scanner and pen test services, along with support for SLA-based virtual patching.

Unmetered Behavioural DDoS Mitigation

Ensure high application availability through system-generated rate-limits that adapt to changes in user behaviour.

Asset and API Discovery

Continuously identify the external attack surface and ensure immediate risk mitigation.

Real Protection with Zero False Positives

Deploy 100% of your applications in block mode with our zero false positives guarantee.

*Industry benchmark - only 53% of WAFs are deployed in block mode

Salient Features of AppTrana WAAP

Fully Managed WAF

Get the support of Indusface security experts 24X7 as an extended SOC team. Leverage the benefit of unlimited, application specific custom rules/virtual patches on open vulnerabilities, false positive monitoring on core rules and custom rules and DDoS and Bot-monitoring. Zero false positive guarantees on all rules.

API Security

Discover and document your APIs automatically. Secure your public facing API endpoints with positive & negative security policy automation on AppTrana WAAP. Identify vulnerabilities in your APIs through the automated API scanner and pen testing to protect them instantly.

Unmetered Behavioural DDoS Mitigation

Block DDoS attacks up to 2.3 Tbps and 700k requests per second right from day zero with highly scalable AWS infrastructure. Ensure round-the-clock availability of your application (with SLA of 99.99%) by mitigating DDoS attacks with our inbuilt DDoS scrubber and get billed only for clean traffic. Go beyond static rate limits and automate rate-limits based on the behaviour of inbound traffic received by IP, URI and Geography.

Bot Protection

Protect your business from bot attacks such as Account Takeover, Credential Stuffing, Card Cracking and Web Scraping attacks. Get anomaly detection for the bad bots based on the behavioural pattern of the bot traffic. Get expert support for designing complex workflows to protect your business from sophisticated bot attacks (URI blacklisting, rate-limiting, geo-fencing rules, anonymous proxy and such other policies.)

Web Application and API Protection Service
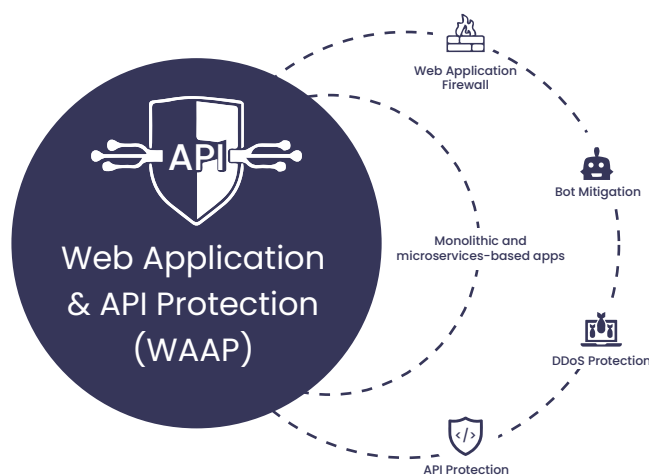
Asset & API Discovery

Discover and maintain an up-to-date inventory of your public-facing web assets (domains, subdomains, IPs, mobile apps, data centers, site types) and APIs. Generate OpenAPI specification file (Swagger 3.0) automatically for the APIs discovered.

Content Delivery Network (CDN)

Maximize website performance by leveraging TATA communication's tier-1 IP backbone and global footprint with strategically located dense nodes physically connected to massive IP gateways.

Trusted by over 5000+ customers globally across 95+ countries

Why AppTrana WAAP can be your dependable security tool?

Unified Platform: The only WAAP with asset discovery, VAPT, DDoS & Bot mitigation, API security and managed WAF in one platform.

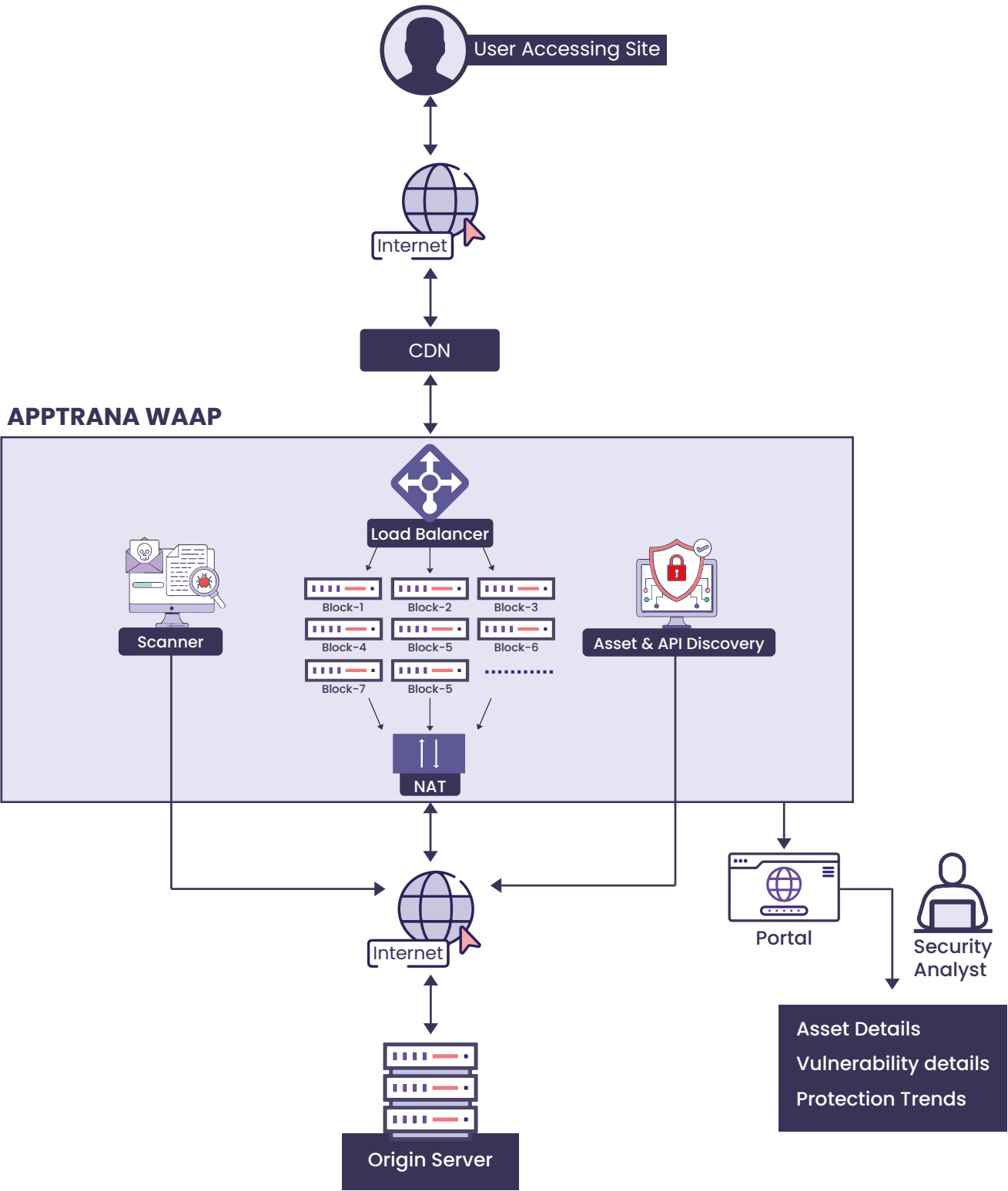**Zero Downtime Onboarding with Day-Zero Protection:** Go-live on the WAAP within five minutes through just a DNS change.

Instant Origin Server Protection: Protect your origin server against vulnerability, zero-day and complex layer 3-7 DDoS attacks.

Security Compliance: We comply with ISO 27001, PCI DSS, GDPR, SOC 2 and CERT-In.

Simplistic UI: AppTrana provides a simplistic yet meaningful UI to help you find details effortlessly and enable you to download a clean report for your internal team.

Integrations: Easily integrate AppTrana into any of your systems. Feed data into your SIEM solutions to ensure real-time insights and alerts. Also, sign in with your existing corporate credentials from any device with the help of SSO/SAML integration.

AppTrana WAAP Architecture Diagram

Feature List

Key Features	Benefits	Advance	Premium	Enterprise
PRICING		$99/App/ Month	$399/App/ Month	Custom/Billed Annually
DISCOVERY				
External Asset Discovery	Discover your external facing assets so that no asset remains unprotected.	Yes	Yes	Yes
Unlimited On-demand Scans	Ability to demand external asset scan for organisation at any point in time	Yes	Yes	Yes
RISK SCANNING				
Managed Application Security Scanning	Auto scan your site for OWASP Top 10 vulnerabilities and SANS 25	Unlimited	Unlimited	Unlimited
Full Support of HTML5 , AJAX and JSON	Support for scanning JSON , AJAX and HTML5 based sites	Yes	Yes	Yes
Remediation Guidance to fix vulnerabilities	Get detailed remediation to fix the vulnerabilities	Yes	Yes	Yes
Vulnerability Revalidation Checks	Fix the vulnerabilities and revalidate quickly to know if ulnerabilities are addressed properly	Yes	Yes	Yes
Guided scans	Guided Scans to ensure automated scans reach the pages that other scans cannot	Yes	Yes	Yes
Authenticated scans	Provide authentication details and have scans be done behind the authenticated pages	Yes	Yes	Yes
Schedule scans	Scan onboarded applications periodically. Set the frequency at which the applications must be scanned.	Yes	Yes	Yes
Proof of concepts	Get proof of concept for the vulnerabilities, enabling teams to prioritise work on the right vulnerabilities	5	Unlimited	Unlimited
Pen-testing by experts*	Have experts ethically hack your sites and find business logic vulnerabilities	No	Yes	Yes
RISK PROTECTION				
Layer 7 protection	Get AppTrana be in line to your website traffic and have it inspect traffic - allow only legit traffic to your site	Yes	Yes	Yes
Zero-vulnerability report	Get a zero vulnerability report for the critical, high & medium vulnerabilities within 72 hours of the onboarding time	No	Yes	Yes
Virtual patching through advance security rules	Leverage custom rules with assured Zero false positive rules protecting OWASP Top 10 vulnerabilities out of the box	Yes	Yes	Yes
Platform specific rule set	Rules written for specific platforms like Joomla, WordPress etc.	Yes	Yes	Yes
Restrict by IP & Geo	Block IP & Geo based on the traffic patterns	Yes	Yes	Yes
Whitelist URI	Whitelist URI, to ensure that certain critical URIs are not blocked accidentally	Yes	Yes	Yes
Self-learning behavioural rules	Have rules to automatically learn and push the right triggers based on the traffic patterns	Yes	Yes	Yes
Risk Prioritization	Get a clear view of vulnerabilities that are protected & unprotected vulnerabilities that need a fix in the code- allowing application owner's to prioritize fixing critical bugs during the development	Yes	Yes	Yes
Malware File Upload Protection	Restricting file uploads and the type of file uploads to avoid any impacts due to the malicious malware files	Yes	Yes	Yes
PCI DSS 3.2 Compliance.	AppTrana is PCI compliant and lets you to save time in meeting the compliances like SOC 2, GDPR, PCI DSS, HIPAA, ISO 27001, etc.	Yes	Yes	Yes

Key Features	Benefits	Advance	Premium	Enterprise
PRICING		$99/App/ Month	$399/App/ Month	Custom/Billed Annually
Origin Protection	Protection of Origin by providing ability to whitelist AppTrana IPs and block rest to ensure origin is not directly attacked	Yes	Yes	Yes
Packet Size Detected	Inspection of payload of 100 MB and more	Yes	Yes	Yes
DDOS MITIGATION				
Protection against Layer 3 & 4 attacks	Always on protection against layer 3 & 4 attacks	Yes	Yes	Yes
Protection against large volumetric Layer 7 attacks	Always on protection against layer 7 that may observe large volumetric attacks seamlessly	Yes	Yes	Yes
Geo-based DDoS Controls	Provide DDoS policy controls at Geo level with ability to set various limits for users from different regions	No	Yes	Yes
Behaviour Based Layer 7 Protection	Protection against Layer 7 attacks using unique behavioural analysis & protecting beyond simple rate limits	Yes	Yes	Yes
Captcha challenges	Enable Captcha's so that suspected traffics are challenged to ensure that the automated attacks are blocked	Yes	Yes	Yes
Protection of origin IP address against DDoS attacks	Origin IP is protected against DDOS and the entire traffic goes through the WAF	Yes	Yes	Yes
Protection against Hot-Linking	Protect against bandwidth and resource due to unwanted assets on the Internet	Yes	Yes	Yes
URI Based BDDoS Attack	Configure granular DDoS controls for critical assets of the application	No	10	10
Customize BDDoS behaviour	Get control on how long certain policies should block	Yes	Yes	Yes
Scalable Infrastructure	Highly Scalable Infrastructure to handle sudden surge of attacks	No	Yes	Yes
BOT MITIGATION				
User-defined bot configurations	Create rules to identify bad bots and add mitigation rules such as crypto challenge, show Captcha and drop requests	Yes	Yes	Yes
Allow good bots & block bot pretender	Check for bots that are pretending as good bots and block those	Yes	Yes	Yes
Tor IP based detection	Check if request is coming from TOR clients and increase the risks score	Yes	Yes	Yes
IP Reputation based protection	Know the IP reputation of connecting clients and increase the risk score based on the reputation	Yes	Yes	Yes
Scanner /Exploitable tools Checks	Understand if scanners or other automated exploitation tools are connecting and block those	Yes	Yes	Yes
Web Scrapper Checks	Twelve checks	Yes	Yes	Yes
Validation of bot signatures and blocking bad bots	Validate requests for known bad bot signatures and block them	Yes	Yes	Yes
Anomaly Behaviour Detection	Identify anomalous behaviour of bots and increase the risk score	No	Yes	Yes
User Agent Based Detection	Check for known malicious bots based on UA of the requests and blocking or increasing risk score of identity	No	Yes	Yes
Datacenter Based Detection	Identify if clients are connecting from a datacentre and increase risk score	No	Yes	Yes
Suspicious Countries	Checking for countries where requests are coming from and increase risk score if it's marked as suspicious countries / non-business countries	No	Yes	Yes

Key Features	Benefits	Advance	Premium	Enterprise
PRICING		$99/App/Month	$399/App/Month	Custom/Billed Annually
RISK MONITORING				
Guaranteed search engine access	Genuine search engines are not blocked	Yes	Yes	Yes
False positive monitoring	Get experts monitor the core rule set for false positives & have rules tweaked to ensure zero false positive	No	Yes	Yes
Premium rules	Premium rules which blocks complex layer 7 rules. Have them enabled after false positive monitoring	No	Yes	Yes
DDoS Notification	Get immediate alerts on any abnormal spike in traffic to the site	Yes	Yes	Yes
Premium DDoS mitigation	Get complex DDoS attacks mitigated through expert monitoring and customized rules based on the attacks	No	Yes	Yes
Custom rules made by experts	Complex business logic vulnerabilities can be protected via expert-written rules	2	Unlimited	Unlimited
Self-service rules (Custom rules)	Create and manage the custom rules all by yourself	2	Unlimited	Unlimited
Zero-day rule set	Get instantaneous protection for zero-day vulnerabilities	Yes	Yes	Yes
Instant customization and propagation of security rules	Rules can be pushed instantly and propagated throughout the infra	Yes	Yes	Yes
24X7 management by certified application security experts	Real time incident monitoring, response and reporting	Yes	Yes	Yes
Continuous Updates of Rules	Continuous monitoring of emerging threats and updating the rules as per the security needs	Yes	Yes	Yes
Training	Full-fledged training of customer team on the entire set of features & capabilities in the AppTrana WAAP	Yes	Yes	Yes
Site Availability Notification	Real-time notification of site availability and notifying in case of any unavailability of the sites	Yes	Yes	Yes
License Utilization Notification	Notifying in case of pending renewal of the service	Yes	Yes	Yes
Attack Anomaly Notification	Notifying in case of surge of the attacks	No	No	Yes
Latency Monitoring	Monitoring the incomings calls for to-and-fro time and notifying in case of sudden increase in average round trip time	No	No	Yes
Named Account Manager	Indusface provides single point account manager who handles the entire account and represents customer internally to accelerate the security	No	No	Yes
Quarterly Service Review	Review provided by the account manager on utilization of the services & explains any sort of recent updates made	No	No	Yes
API SECURITY				
Managed API Scanning	Automated Scanning of APIs for OWASP Top 10 API Threats and more	No	Yes	Yes
API definition Support	Support to understand APIs by parsing postman files to enable API scanning	No	Yes	Yes
Shadow API Discovery	Discovery of APIs that are not part of swagger definition but request served by API Server	No	Yes	Yes
API Discovery	Discovery of APIs based on traffic	No	Yes	Yes
Open API Documentation	Auto creation of swagger documentation for API discovered	No	Yes	Yes

Key Features	Benefits	Advance	Premium	Enterprise
PRICING		$99/App/ Month	$399/App/ Month	Custom/Billed Annually
Auto creation of Positive security model for APIs	Positive security policies created from Swagger files	No	Yes	Yes
API specific WAF policies	Specific Rules to protect against Top 10 API Threats	No	Yes	Yes
Behaviour Based DDOS Protection for APIs	Granular BDDOS Policies for critical APIs	No	Yes	Yes
API Specific BOT detections	API specific BOT policies	No	Yes	Yes
WHOLE SITE ACCELERATION				
Carrier grade CDN	With the world's 4th largest, Tier-1 IP back- bone network: TATA Communications – Customers get complete full-site acceleration to reduce latency & ensure content reaches users in the shortest time	Yes	Yes	Yes
Content optimization	Accelerate site content through optimization techniques like minification, auto-compression etc.	Yes	Yes	Yes
Automatic static content caching	Perform automatic static content caching for content like images, java script files and CSS	Yes	Yes	Yes
Dynamic content caching	Cache dynamic contents by enabling advance caching	Yes	Yes	Yes
Manual cache purge	Cache items that can be instantly purged through the portal	Yes	Yes	Yes
Custom cache header	Advance caching policies can be crafted using URL parameters & file paths	Yes	Yes	Yes
Adv Profiling	Site profiling and improving caching to reduce the load on the servers	Yes	Yes	Yes
Image Optimization	Optimizing of Images to improve performance of pages which are heavy on Images	Add-On	Add-On	Add-On
OTHER FEATURES				
Analytics Page	Independent analytics page to analyse traffic logs for the site	Yes	Yes	Yes
Standard Reports	Detailed Executive and site level scan reports	Yes	Yes	Yes
Integration into 3rd party CDN	AppTrana is CDN agnostic and will work seamlessly with any CDN	Yes	Yes	Yes
360* visibility into application security posture	With integrated DAST Scanner and WAF, AppTrana provides a comprehensive view to the application's risk posture	Yes	Yes	Yes
Highly available and scalable architecture	Infrastructure that scales seamlessly to handle millions of requests concurrently.	Yes	Yes	Yes
Custom Port	Support for Custom Ports in Application	Yes	Yes	Yes
WebSockets	Support for Application passing traffic through Websockets	Yes	Yes	Yes
HTTP v2	Support for HTTP v2 protocol	Yes	Yes	Yes
Zero downtime onboarding	Entire onboarding is done within a few minutes ensuring zero downtime for the site (protection right from the day zero)	Yes	Yes	Yes

Key Features	Benefits	Advance	Premium	Enterprise
PRICING		$99/App/ Month	$399/App/ Month	Custom/Billed Annually
RBAC	Role based access control to the customers	No	Yes	Yes
2FA	Two-factor authentication	No	Yes	Yes
SIEM	SIEM integration with any SIEM providers for gathering real-time insights and alerts for swift threat response	No	Yes	Yes
SAML Integration/SSO	Sign in to AppTrana with your existing corporate credentials from any device without compromising security	Yes	Yes	Yes
Bypass mode	Retain complete control of the site and have ability to bypass AppTrana with a single click	Yes	Yes	Yes
Log mode	Have ability to deploy all rules in the log mode and monitor logs to ensure zero false positives	Yes	Yes	Yes
Real-time logging	Get real time access to logs and ensure quick notification and action in case of attacks	Yes	Yes	Yes
Support	24/7/365 support through phone, chat and emails, backed by guaranteed response time SLA	Yes	Yes	Yes

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.