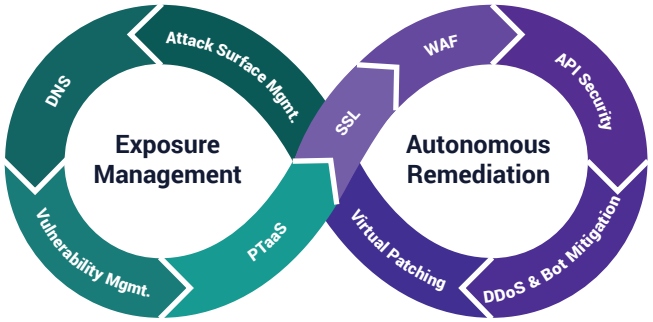
INDUSFACE™

DATASHEET

AI-Powered App Security. Human-Verified Accuracy.

No false positives. No open vulnerabilities. AI-powered WAAP with human verification ensures every application and API is protected against all known threats—remediated within 72 hours, an industry only capability.

AI-Powered, Continuous Compliance for Web Apps and APIs



AppTrana Cloud WAAP

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

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

Gartner Peer Insights Customers' Choice 2024™

Key Benefits

SwyftComply - Autonomous Vulnerability Remediation

- Continuously discover exposed assets with attack surface management (ASM)
- Get AI-powered penetration testing as a service (PTaaS) for web apps & APIs
- Get autonomous vulnerability remediation in 72 hours, free of false positives
- Seamless reporting with automated POCs & CI/CD integration

Protect Against DDoS & Bot Attacks at Internet Scale

- Unmetered behavioral protection against sophisticated AI & LLM based Attacks
- 24/7 Indusface SOC
- Scalable double-layered architecture to absorb 100x traffic and mitigate attacks in minutes
- All applications deployed in block mode

Ensure Application Availability

- 100% uptime guarantee
- Automated failover built-in
- Highly scalable infrastructure
- Accelerate performance with CDN

Remove Silos in Your AppSec Journey

- Real-time correlation between attack surface and threats for swift mitigation
- Unified security management with a single pane of glass for WAF, API security, DDoS & bot protection, DAST, and manual penetration testing—all in one platform

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.

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.

Unmetered Behavior-Based DDoS and Bot Mitigation

Ensure round-the-clock availability of your application by mitigating DDoS and Bot attacks with our inbuilt DDoS scrubber. Go beyond static rate limits and leverage AI-based auto-mitigation methods that drive decisions based on inbound traffic received by host, IP, URI and Geography.

SwyftComply – Autonomous Vulnerability Remediation within 72 Hours

Comply with global and regional security audits through a zero-vulnerability report. Get autonomous vulnerability remediation within 72 hours on AppTrana for critical, high, and medium-level vulnerabilities.

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.

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.

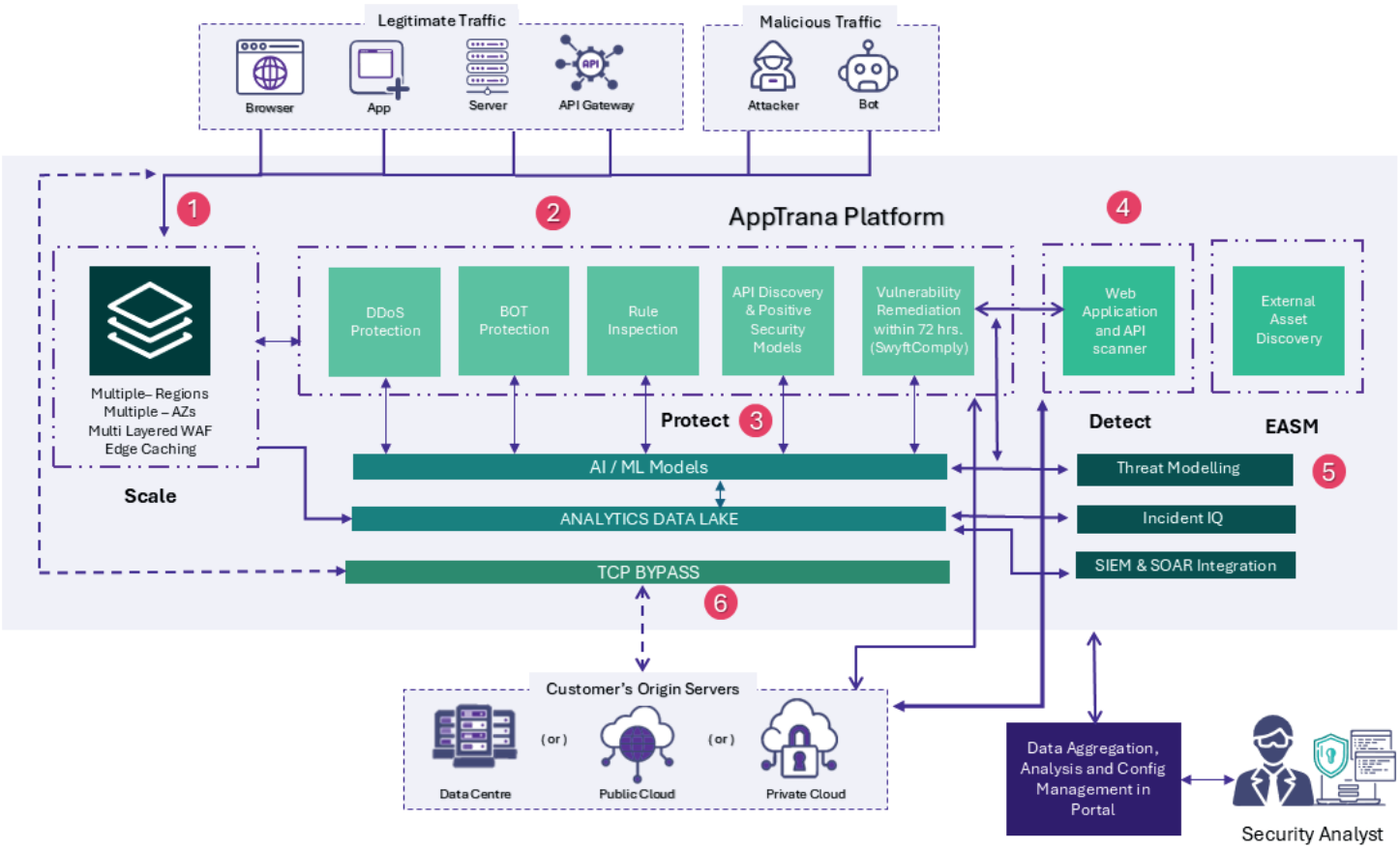
Instant Origin Server Protection: Protect your origin server against vulnerability, zero-day and complex layer 3-7 DDoS attacks.

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: Integrate AppTrana to the CI/CD pipeline to trigger scans on new builds and create tickets to patch open vulnerabilities. You can also send scan logs to all major SIEM providers.

AppTrana WAAP Architecture Diagram



1. Application traffic hits the nearest AppTrana region—each built for high resilience, scalability, and failure-tolerance at every layer.
2. Each region features a scalable protection layer to defend against DDoS, Bot, API attacks, and more.
3. Traffic insights are stored in an Analytics Data Lake, powering ML/Gen AI models in real time to enhance the protection layer.
4. Apps are scanned and virtually patched within 72 hours with zero false positives.
5. Threats are continuously monitored and modeled for real-time defense.
6. A multi-layered failover design — including at the application layer — ensures traffic is safely bypassed during rare platform incidents, maintaining uninterrupted application availability.

Feature List - AppTrana for Websites

Key Features	Benefits	Advance	Premium Includes SwyftComply	Enterprise Includes SwyftComply
		Comprehensive Web App & API Security	Fully Managed Web App & API Security	Fully Managed Web App & API Security for Enterprises.
		$99 /App/Month Billed Monthly"	Custom	Custom
Asset Discovery				
External Asset Discovery	Discover internet facing assets of organization	Yes	Yes	Yes
Unlimited On-demand Scans	Ability to demand external asset scan for organization at any time	Yes	Yes	Yes
Instant Automated Remediation for Vulnerabilities				
Managed Application Security Scanning	AppTrana automatically scans your site for OWASP Top 10 vulnerabilities	Yes	Yes	Yes
Automated Remediation of vulnerabilities	SwyftComply: Industry-first AI-driven remediation delivering zero-vulnerability reports in just 72 hours	x	Yes	Yes
Full Support of HTML5 , AJAX and JSON	Support to Scan JSON , AJAX and HTML5 based sites	Add-On	Add-On	Add-On
Remediation Guidance to fix vulnerabilities	Get detailed information on how to fix the vulnerabilities	Yes	Yes	Yes
Vulnerability Revalidation Checks	Fix the vulnerabilities and have it quickly revalidated to know if vulnerabilities are properly addressed	Yes	Yes	Yes
Guided scans	Guided Scans can be enabled to ensure automated scans reaches pages that other scans cannot	Yes	Yes	Yes
Authenticated scans	Provide authentication details and have scans be done behind authenticated pages	Yes	Yes	Yes
Automated FP removal	Removal of False positive for Critical, High & Medium vulnerabilities	x	Yes	Yes
Manual verification of vulnerabilities by experts	Get proof of concept for the vulnerabilities, enabling teams to prioritize work on right vulnerabilities	5	Unlimited	Unlimited
Pen-testing by experts*	Have experts ethically hack your sites and find business logic vulnerabilities	x	Add-On	Add-On
CI/CD - Jenkins Integration	Identify vulnerabilities in every deployment cycle by integrating AppTrana in the CI/CD pipeline	Yes	Yes	Yes
JIRA Integration	Manage vulnerabilities discovered on AppTrana seamlessly on JIRA platform	Yes	Yes	Yes
Whitelisting of Vulnerabilities	Ability be whitelist vulnerabilities based on business need. This is controlled with RBAC to avoid misuse	Yes	Yes	Yes
Risk protection				
Layer 7 protection	Get AppTrana be in line to your website traffic and have it inspect traffic and allow only legit traffic to your site	Yes	Yes	Yes
Virtual patching through advance security rules	Have assured Zero false positive rules protecting OWASP Top 10 vulnerabilities out of the box	Yes	Yes	Yes

Key Features	Benefits	Advance	Premium Includes SwyftComply	Enterprise Includes SwyftComply
Platform specific rule set	Have rules enabled written specifically for platforms like Joomla, WordPress etc.	Yes	Yes	Yes
Restrict by IP & Geo	Quickly block IP & Geo based on traffic patterns	Yes	Yes	Yes
Whitelist URI & IP	Whitelist URI or IP, to ensure that certain critical URI/IP are not blocked accidentally	Yes	Yes	Yes
Risk Prioritization	Portal provides clear view of vulnerabilities that is protected, that can be protected and which needs fix in code, allowing application owner prioritize critical bugs for development	Add-On	Add-On	Add-On
Malware File Upload Protection	Restricting file uploads and type of file uploads that can be permitted to avoid upload of malicious files	Yes	Yes	Yes
Malware Scanning for Uploaded files	Scanning of files uploaded for malwares	Yes	Yes	Yes
PCI DSS 4.0.1 Compliance	AppTrana is PCI Compliant and enables you to meet PCI DSS compliance cost effectively	Yes	Yes	Yes
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
Browser Protection	Protecting applications from Supply chain, man in the browser attacks	x	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 is able to 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	x	Yes	Yes
Behavior Based Layer 7 Protection	Protection against Layer 7 attacks using unique behavioral analysis going beyond simple rate limits	Yes	Yes	Yes
Captcha challenges	Enable Captcha's so that suspected traffics are challenged to ensure automated attacks are blocked	Yes	Yes	Yes
Protection of origin IP address against DDoS attacks	Origin IP is protected against DDOS and forcing all traffic goes through WAF	Yes	Yes	Yes
Granular DDoS Attacks	Configure granular DDoS controls for critical assets of the application by configuring policies for URI, Geo etc..	x	Yes	Yes
Scalable Infrastructure	Highly Scalable Infrastructure to handle sudden surge of attacks	Yes	Yes	Yes

Key Features	Benefits	Advance	Premium Includes SwyftComply	Enterprise Includes SwyftComply
Customize BDDoS behavior	Get control on how long certain policies should block	x	Yes	Yes
BOT Mitigation				
Allow Good bots & Block Bot Pretender	Check for bots that are pretending as good bots and block those	Yes	Yes	Yes
User Agent Based Detection	Checking for known malicious bots based on UA of requests and blocking or increasing risk score of identity	Yes	Yes	Yes
Suspicious Countries	Checking for countries where requests are coming from and increase risk score if it is from suspicious countries	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	Check the IP reputation of connecting clients and increase risk score based on reputation	Yes	Yes	Yes
Validation of bot signatures and blocking bad bots	Validate requests for known bad bot signatures and block them	x	Yes	Yes
Datacenter Based Detection	Check if clients are connecting from a data center and increase risk score if they are	x	Yes	Yes
Scanner /Exploitable tools Checks	Check if scanners or other automated exploitation tools are connecting and block those	x	Yes	Yes
Web Scrapper Checks	Check if known web scrappers are connecting and block those	x	Yes	Yes
Anomaly Behavior Detection	Identify anomalous behavior of bots and increase risk score	x	Yes	Yes
JS Challenge	JS Challenge to block autonomous BOTs	x	Yes	Yes
BotSense ML	ML module to identify malicious bots based on behavior and characteristic of requests	x	Yes	Yes
AI Crawler Detection	Detect GenAI crawlers accessing the application and take the decisions based on application need	x	Yes	Yes
Advance Mitigation Option	Take actions like Crypto challenge, Fake data etc.. Based on application need	x	Yes	Yes
Workflow Based Policies	Create custom workflow-based policies to detect and protect against sophisticated BOTS	x	Yes	Yes
Risk Monitoring				
Guaranteed search engine access	We ensure that genuine search engines are not blocked	Yes	Yes	Yes
False positive monitoring	Get experts monitor the CRS for false positives & have rules tweaked to your site to ensure zero false positive	x	Yes	Yes

Key Features	Benefits	Advance	Premium Includes SwyftComply	Enterprise Includes SwyftComply
SwyftComply	Get a clean zero-vulnerability report for audit and compliance needs in 72 Hrs.	x	Yes	Yes
Premium rules	Premium rules which blocks complex layer 7 rules. Have them enabled after false positive monitoring	x	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 attacks	x	Yes	Yes
Unlimited Self Managed Rules	Ability for customer to create custom rules using intuitive rule builder	Yes	Yes	Yes
Custom rules made by experts	Complex business logic vulnerabilities can be protected through experts written rules	2	Yes	Yes
Zero-day rule set	Get instantaneous protection for zero-day vulnerabilities through continuous updates written by experts	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	Constant monitoring of emerging threats and update of Rules as needed	Yes	Yes	Yes
Site Availability Notification	Notification of site availability and notification in case of unavailability of sites	Yes	Yes	Yes
License Utilization Notification	Notification in case of pending expiry of service	Yes	Yes	Yes
Attack Anomaly Notification	Notification in case of surge of attacks	x	Yes	Yes
Latency Monitoring	Monitoring of round trip time and notification in sudden increase in average round trip time	x	Yes	Yes
Training	Training of customer team on WAF and other features in AppTrana	x	Yes	Yes
Named Account Manager	A single point account manager who handles the entire account and represents customer internally to accelerate solutions	x	x	Yes
Quarterly Service Review	Review done by Account Manager on utilization of service and explanation of recent updates made	x	x	Yes
DNS Security				
Protection for DNS Hosts	Protect DNS Hosts from attacks including DDoS Attacks targeting DNS	x	Add-On	Add-On
Whole Site Acceleration				
Carrier grade CDN	Backed by world's 4th largest, wholly-owned Tier-1 IP back- bone network: Whole site Acceleration reduce latency to ensure content reaches users in the shortest possible time	Yes	Yes	Yes
Content optimization	Accelerate site content through optimization techniques like minification, auto-compression etc.	Yes	Yes	Yes

Key Features	Benefits	Advance	Premium Includes SwyftComply	Enterprise Includes SwyftComply
Automatic static content caching	Cache static contents 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 can be instantly purged through the portal	Yes	Yes	Yes
Custom cache header	Advance caching policies can be crafted	Yes	Yes	Yes
Adv Profiling	Profiling of site and improving caching to reduce load on servers	Yes	Yes	Yes
Image Optimization	Optimization of Images to improve performance of pages which are heavy on Images	Add-On	Add-On	Add-On
Other Features				
Executive Report	Canned reports for executives that gives trends across various assets and actionables	Yes	Yes	Yes
Groups	Ability to create groups and assign assets to various groups based on business needs	Yes	Yes	Yes
Detailed Reports	Detailed asset level reports for various scans	Yes	Yes	Yes
Multi-User	Ability to create any number of users based on business need	Yes	Yes	Yes
Target Management for users	Ability to assign different assets/groups to various users based on business needs	Yes	Yes	Yes
Flexible Reporting	Ability to create customized reports based on business need and create reporting schedules	Yes	Yes	Yes
Customer Error Pages	Create Custom Error pages based on application need	x	Yes	Yes
False positive reporting	Report highlighting changes done as part of false positive monitoring by Indusface security team	x	Yes	Yes
Custom Port	Support for Custom Ports in Application	x	Yes	Yes
WebSockets	Support for Application passing traffic through Websockets	x	Yes	Yes
HTTP v2	Support for HTTP v2 protocol	Yes	Yes	Yes
Zero downtime onboarding	Entire onboarding is done in few minutes with zero downtime for the site. Protection starts on day zero	Yes	Yes	Yes
SSO	Single Sign on support for dashboard enabling user management in a single place	x	Yes	Yes
RBAC	Role Based access control to customers	x	Yes	Yes
2FA	2 factor authentication	Yes	Yes	Yes
SIEM Integration	SIEM APIs to integrate with any SIEM customer has for real time access to data. Alternatively, logs can be shared in S3 bucket and picked from there	x	Add-On	Add-On

Key Features	Benefits	Advance	Premium Includes SwyftComply	Enterprise Includes SwyftComply
Bypass mode	Ability to quickly bypass WAF Infra to debug production issue with a single click. Helps in having availability of assets behind AppTrana in the unlikely event of failure with infrastructure	Yes	Yes	Yes
Log mode	Have ability to have all rules in log mode and monitor logs to ensure no 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
Email Notification Customizations	Ability to customize which notification a user should receive based on business need	Yes	Yes	Yes
Free Let's Encrypt DV SSL Certificate	Onboard site in AppTrana using free Let's Encrypt certificate	Yes	Yes	Yes
Option to buy Entrust OV or EV certificate	Buy Enterprise grade Entrust certificates from Indusface	Yes	Yes	Yes
Custom SSL Certificate	Bring your own certificate and use it in AppTrana in secured manner	Yes	Yes	Yes

Feature List - AppTrana for APIs

Features	Advance	Premium Includes SwyftComply	Enterprise Includes SwyftComply
Asset Discovery			
External Asset Discovery	Yes	Yes	Yes
Unlimited On-demand Scans	Yes	Yes	Yes
Risk Detection			
Managed API Scanning	On-Demand - Unlimited	On-Demand-Unlimited	On-Demand-Unlimited
Daily Scans	Add-On	Add-On	Add-On
No of Application credentials	1	2	2
Coverage for OWASP Top 10 API	Yes	Yes	Yes
Manual Pen-testing by Experts	Add-On	1	Add-On
Automated FP removal	Yes	Yes	Yes
Manual verification of vulnerabilities by experts	Unlimited	Unlimited	Unlimited
Remediation Guidance to fix vulnerabilities	Yes	Yes	Yes
Vulnerability Revalidation Checks	Add-On	Unlimited	Unlimited
Discover Shadow APIs	Yes	Yes	Yes
Whitelisting of Vulnerabilities	Yes	Yes	Yes
Risk Protection			
Layer 7 Web Application Firewall	Yes	Yes	Yes
Virtual patching through advance security rules	Yes	Yes	Yes
SwyftComply for APIs – Get a clean zero-vulnerability report for audit and compliance needs in 72 Hrs.	No	Yes	Yes
API Specific Rules	Yes	Yes	Yes
Zero day vulnerability Protection	Yes	Yes	Yes
Restrict by IP & Geo	Yes	Yes	Yes
Malware Scanning for Uploaded files	Add-On	Add-On	Add-On
Whitelist of URI & IP	Yes	Yes	Yes
Risk Prioritization	Yes	Yes	Yes
Origin Protection	Yes	Yes	Yes
Reduce attack surface through auto-generated positive security policies	Yes	Yes	Yes
DDOS Mitigation			
Protection of Layer 3, 4 Volumetric Attacks	Yes	Yes	Yes
Protection against large volumetric Layer 7 attacks	Yes	Yes	Yes
Scalable Infrastructure	Yes	Yes	Yes
Behavior Based DDOS Protection for APIs	Yes	Yes	Yes
Captcha Challenges	Yes	Yes	Yes
Protection of Origin IP against DDoS Attacks	Yes	Yes	Yes
Behavior Based DDOS Protection for APIs	Yes	Yes	Yes
Geo based DDoS Controls	Yes	Yes	Yes
Customized DDoS Behavior	Yes	Yes	Yes

Features	Advance	Premium Includes SwyftComply	Enterprise Includes SwyftComply
BOT Mitigation			
Allow Good bots/ Bot Pretender Checks	Yes	Yes	Yes
Tor IP based detection	Yes	Yes	Yes
Validation of bot signatures and blocking bad bots	Yes	Yes	Yes
Datacenter Based Detection	Yes	Yes	Yes
Scanner /Exploitable tools Checks	Yes	Yes	Yes
Suspicious Countries	Yes	Yes	Yes
Behavior based detection	Yes	Yes	Yes
Risk Monitoring			
DDoS Notification	Yes	Yes	Yes
Expert written custom rules	Yes	Yes	Yes
Instant customization and propagation of security rules	Yes	Yes	Yes
24X7 management by certified application security experts	Yes	Yes	Yes
Continuous Updates of Rules	Yes	Yes	Yes
Site Availability Notification	Yes	Yes	Yes
License Utilization Notification	Yes	Yes	Yes
False positive monitoring	Yes	Yes	Yes
Premium rules	Yes	Yes	Yes
Premium DDoS mitigation	Yes	Yes	Yes
Zero-day rule set	Yes	Yes	Yes
Latency Monitoring	Yes	Yes	Yes
Training	Yes	Yes	Yes
Named Account Manager	x	x	Yes
Quarterly Service Review	x	x	Yes
DNS Security			
Protection for DNS Hosts	Add-On	Add-On	Add-On
Other Features			
Executive Report	Yes	Yes	Yes
Groups	Yes	Yes	Yes
Detailed Reports	Yes	Yes	Yes
Multi-User	Yes	Yes	Yes
Target Management for users	Yes	Yes	Yes
Flexible Reporting	Yes	Yes	Yes
False positive reporting	Yes	Yes	Yes
Custom Port	Yes	Yes	Yes
Customer Error Pages	Yes	Yes	Yes
WebSockets	Yes	Yes	Yes
HTTP v2	Yes	Yes	Yes
Zero downtime onboarding	Yes	Yes	Yes

Features	Advance	Premium Includes SwyftComply	Enterprise Includes SwyftComply
RBAC	Yes	Yes	Yes
2FA	Yes	Yes	Yes
SSO Integration	Yes	Yes	Yes
SIEM Integration	Yes	Yes	Yes
Bypass mode	Yes	Yes	Yes
Log mode	Yes	Yes	Yes
Real-time logging	Yes	Yes	Yes
Support	Yes	Yes	Yes
Email notification customization	Yes	Yes	Yes
Other Features			
Free Let's Encrypt DV SSL Certificate	Yes	Yes	Yes
Option to buy Entrust OV or EV certificate	Yes	Yes	Yes
Custom SSL Certificate	Yes	Yes	Yes

Indusface is a leading application security SaaS company, securing over 5,000 customers across 95 countries with its award-winning platform. Funded by institutional investors, it has been a category leader in Gartner Peer Insights™ for the past three years.

The industry's only AI-powered, all-in-one AppSec platform helps businesses discover, detect, remediate, and protect web applications and APIs at internet scale, backed by a 100% uptime guarantee.