Web, AI & API Protection

Discover your exposure. Block attacks. Remediate vulnerabilities with AI speed and expert certainty. One platform for protecting web apps, APIs, and AI workloads from zero-day, DDoS, and bot attacks.

★★★★★ **4.9** on Gartner Peer Insights · **300+** verified reviews

Threats blocked. Vulnerabilities closed. Without lifting a finger.

One DNS change and you're live. No complex deployments, no code changes. From that point, AppTrana finds, protects, and fixes while your team focuses on everything else.

- **Discover** — every domain, app, API, and AI workload. Found automatically, including shadow assets.
- **Scan** — DAST continuously scans apps, APIs, and AI workloads. Every finding feeds directly into autonomous vulnerability remediation.
- **Protect** — WAF blocks web attacks. API and AI Shield cover every endpoint and LLM workload. DDoS and bot defense keep you online. All in block mode from day one.
- **Monitor** — 24×7 experts monitor apps, tune protections in real time, and respond as attacks happen.

Benefits for your business

Remediated vulnerability reports

Expert-verified reports ready for compliance audits, board reviews, and customer security assessments within 72 hours.

Never block a legitimate user

Zero false positive guarantee — deploy in block mode from day one with 24/7 AI-powered protection and expert monitoring.

Stay online during attacks

100% uptime SLA — unmetered DDoS and bot mitigation keep your business running during the largest surges.

Protecting thousands of applications. Blocking billions of attacks.

<5 Min	100%	<72 hrs	6,500+
From a DNS change to complete protection	Of apps protected in block mode from day one	The only WAAP that patches open vulnerabilities in hours	Customers protected across 95+ countries

TRUSTED BY LEADING ENTERPRISES WORLDWIDE

HDFC ERGO · Bandhan Life · TATA CAPITAL · ITC HOTELS RESPONSIBLE LUXURY · TATA POWER
LTM · IndusInd Bank · Bank of India · DANUBE GROUP · TITAN COMPANY
marico · TATA Tele Business Services · LRN · VICTORINOX · YAMAHA Make Waves

APPTRANA PLATFORM CAPABILITIES

One platform. One protection loop.

ASSET DISCOVERY

Every protection loop starts with knowing what you have.

AppTrana continuously maps your attack surface: web apps, APIs, AI endpoints, and the shadow assets your team didn't know existed.

AUTONOMOUS REMEDIATION

Find vulnerabilities. Fix them. Walk into every audit with proof.

Every finding — from DAST scans or your own disclosures — gets an AI-generated virtual patch, expert-validated before enforcement. SwyftComply delivers an audit-ready report in under 72 hours.

DDOS & BOT DEFENSE

No surprise outages. No paying ransom for attack traffic.

Behavioral AI detects and absorbs automated attacks across every layer before spikes become outages. Included in every plan — unmetered.

THREE PILLARS · ONE PLATFORM

Web Application Protection

Adaptive Protections, block-mode-by-default, behavioral defense.

API Protection

Discovery, schema enforcement, OWASP API Top 10 coverage with DDoS and bot protection.

AI Agent / LLM Protection

Protect your LLMs and AI agents from prompt injection, abuse, and denial-of-wallet attacks.

24×7 MANAGED SERVICES

Security experts on your team. Always.

- ✓ Real-time attack monitoring and instant mitigation
- ✓ Expert-verified vulnerability remediation reports
- ✓ False positive removal and policy tuning on every update
- ✓ Named TAM for enterprise. Quarterly business reviews included.
- ✓ Zero-day and CVE response without waiting on your dev team

SOC 2 Type II · ISO 27001 · PCI DSS · HITRUST CSF

24×7
Expert coverage at every tier

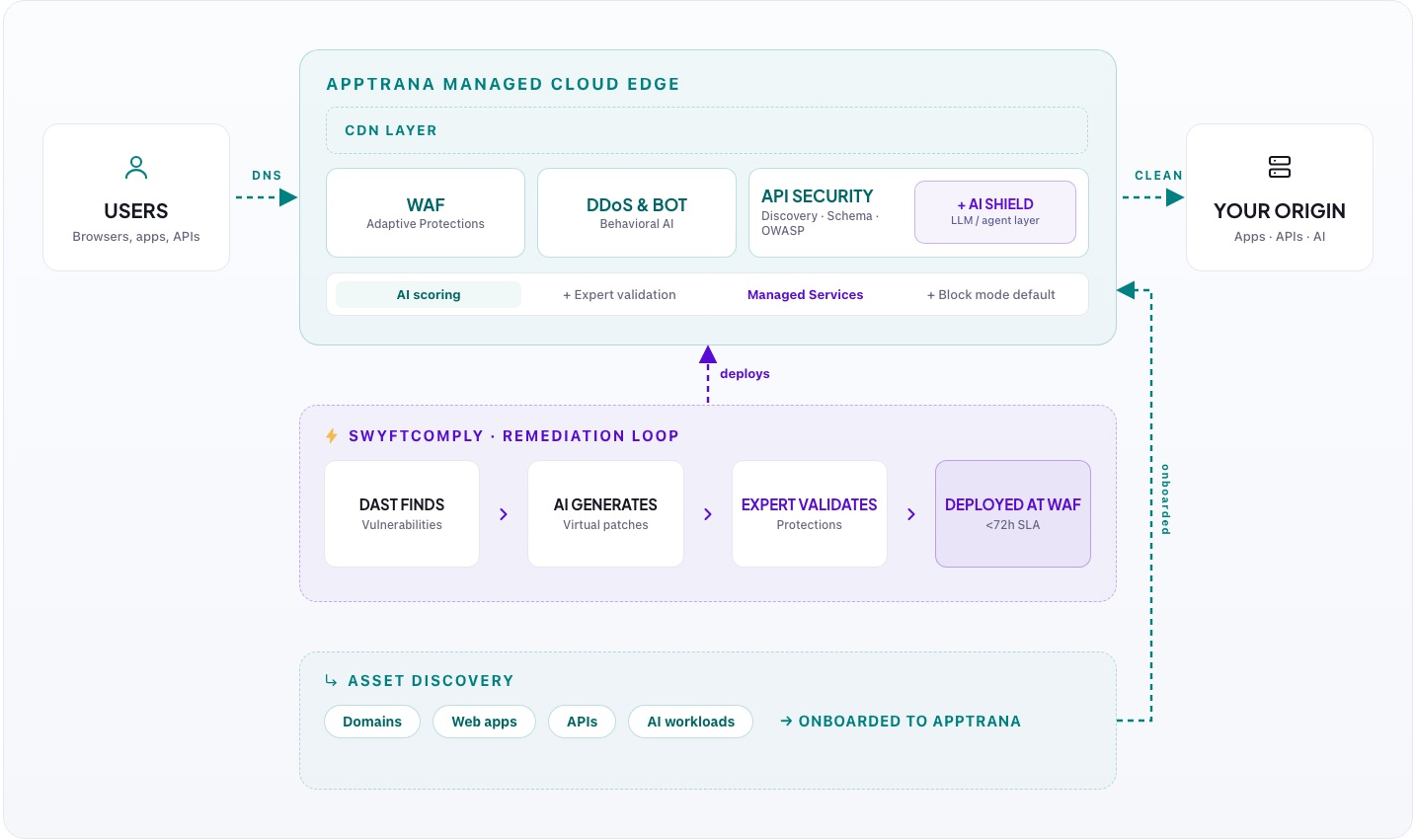
Unlimited
Expert support. No hours cap.

Named TAM
For enterprise accounts

100%
Uptime SLA, guaranteed

APPTRANA PLATFORM ARCHITECTURE

How traffic flows, gets inspected, and stays protected



TESTIMONIALS

4.9 ★★★★★

300+ verified reviews · Gartner Peer Insights

- 100% customer recommendation — 4 consecutive years
- Highest-rated Cloud WAAP and API Security solution

"AppTrana WAAP helps us detect vulnerabilities and protects against them in a single unified platform."

Kinshuk De

Head Cyber Incident Response · TCS

"AppTrana helped us elevate security posture while achieving significant operational savings."

Anubhav Rajput

CIO & CTO · PNB Housing Finance

"Indusface functions as an independent 'third eye' to continuously monitor and protect our application and API landscape 24×7."

Corporate Cyber Security Team

Tata Power

FEATURE COMPARISON

Key features	Benefits	Advanced	Premium	Enterprise
ASSET DISCOVERY				
External Asset Discovery	Discover external facing web applications and APIs so that no asset remains unprotected	✓	✓	✓
Unlimited On-demand Scans	Ability to demand external asset scan for the organization at any time	✓	✓	✓
72 HRS AUTOMATED REMEDIATION FOR VULNERABILITIES				
Managed Application Security Scanning	AppTrana automatically scans your site for OWASP Top 10 vulnerabilities & more	✓	✓	✓
AI-Powered Crawler	AI-powered crawler to identify optimal paths and reach areas other scanners cannot	**Normal Crawler**	✓	✓
Automated Remediation of web app and API vulnerabilities	SwyftComply: Industry-only, AI-driven remediation delivering zero-vulnerability reports	–	✓	✓
Automated FP removal	Removal of False Positives for Critical, High & Medium vulnerabilities	–	✓	✓
Full Support of HTML5, AJAX and JSON	Support to Scan JSON, AJAX and HTML5 based sites	✓	✓	✓
Remediation Guidance to Fix Vulnerabilities	Receive detailed information on how to fix vulnerabilities	✓	✓	✓
Vulnerability Revalidation Checks	Fix the vulnerabilities and have it quickly revalidated to know if the vulnerabilities are properly addressed	✓	✓	✓
Guided scans	Guided Scans can be enabled to ensure automated scans reach pages that other scans cannot	–	✓	✓
Authenticated scans	Provide authentication details and scan behind authenticated pages with admin and other user roles	–	✓	✓
Proof of Concepts	PoC for vulnerabilities to prioritise the right fixes.	**5**	**Unlimited**	**Unlimited**
Pen-testing by experts*	Have experts ethically hack your sites and find vulnerabilities including business logic vulnerabilities	–	**Add-On**	**Add-On**
AI-Assisted Pen Testing	Use AI-assisted pentesting to find 5x-10x more critical and high CVSS vulnerabilities when compared to traditional DAST and pentests.	–	**Add-On**	**Add-On**
Whitelisting of vulnerabilities	Ability to whitelist vulnerabilities based on business need. This is controlled with RBAC to avoid misuse	✓	✓	✓
RISK PROTECTION				
Layer 7 protection	Get AppTrana to operate in line with your website traffic, inspect it, and allow only legitimate traffic to your origin servers	✓	✓	✓

FEATURE COMPARISON

Key features	Benefits	Advanced	Premium	Enterprise
RISK PROTECTION (CONTD.)				
Virtual patching through advanced security rules	Have assured zero false positive rules to protect against OWASP Top 10 vulnerabilities out of the box	–	✓	✓
Virtual Patching via AI-Generated Rules	Rapidly protect new vulnerabilities using AI-generated security rules tuned to minimize false positives.	–	✓	✓
OWASP Top 10 for LLM Applications Protection	Protect AI applications against prompt injection, excessive request rates, and exposure of personally identifiable information (PII).	Add-On	Add-On	Add-On
Platform specific rule set	Deploy custom security policies written specifically for platforms like Joomla, WordPress and others.	✓	✓	✓
Restrict by IP & Geo	Quickly block IP & Geo based on traffic patterns	✓	✓	✓
Whitelist URI & IP	Whitelist URIs or IPs to ensure that critical usecases are not blocked accidentally	✓	✓	✓
Risk Prioritization	Portal provides a clear view of vulnerabilities that are protected by default, that can be protected through virtual patches, and which need fix in code	✓	✓	✓
Malware File Upload Protection	Restrict file uploads and types of files that can be permitted to prevent the upload of malicious files	Add-On	Add-On	Add-On
PCI DSS 4.0 Compliance	AppTrana is PCI Compliant and enables you to meet PCI DSS 6.6 compliance cost-effectively	✓	✓	✓
Origin Protection	Protect your origin by whitelisting AppTrana IPs and blocking all other traffic to prevent direct-to-origin/WAF bypass attacks	✓	✓	✓
Packet Size Detection	Inspection of payload of 100 MB and more	✓	✓	✓
Browser Protection	Protect applications from supply chain and man-in-the-browser attacks	–	✓	✓
Applications onboarded in block mode	False positive monitoring ensures the application is onboarded and remains in block mode from day zero	✓	✓	✓
Static Blocking with Rules in Log Mode	Statically block specified threats, IP and Geo traffic patterns while the broader security rule set remains in log-only mode	✓	✓	✓
DDOS MITIGATION				
Protection against Layer 3 & 4 attacks	Always on protection against Layer 3 & 4 attacks	✓	✓	✓
Protection against large volumetric layer 7 attacks	Always-on layer 7 protection that detects and mitigates large volumetric attacks seamlessly	✓	✓	✓
Geo-based DDoS Controls	Provide DDoS policy controls at the Geo level with the ability to set various limits for users from different regions	✓	✓	✓

FEATURE COMPARISON

Key features	Benefits	Advanced	Premium	Enterprise
DDOS MITIGATION (CONTD.)				
Behavior-Based Layer 7 Protection	AI-driven protection against Layer 7 attacks using unique behavioral analysis going beyond simple rate limits	✓	✓	✓
Captcha challenges	Enable CAPTCHA to challenge suspected traffic and block automated attacks	–	✓	✓
Granular DDoS Controls	Configure granular DDoS controls for critical applications by defining policies for URI, Geo, and other parameters	–	✓	✓
Advanced DDoS Configs	Apply custom, session-based policies to manage abusive sessions	–	✓	✓
Customize BDDoS behavior	Control how long certain policies should block traffic	–	✓	✓
Protection of origin IP address against DDoS attacks	Protect the origin IP against DDoS attacks by forcing all traffic to pass through the WAF	✓	✓	✓
Scalable Infrastructure	Highly scalable infrastructure to handle sudden surge of attacks	✓	✓	✓
BOT MITIGATION				
Allow good bots & block bot pretenders	Check for Bots that are pretending as good Bots and block those	✓	✓	✓
User Agent Based Detection	Detect known malicious bots based on the user agent of requests, and block them or increase their risk score	✓	✓	✓
Suspicious Countries	Check the countries from which requests originate and increase the risk score for suspicious regions	✓	✓	✓
Tor IP based detection	Check if request is coming from TOR clients and increase the risks score	✓	✓	✓
IP Reputation based protection	Check the IP reputation of connecting clients and increase the risk score based on reputation	✓	✓	✓
Validation of Bot signatures and blocking bad Bots	Validate requests for known bad Bot signatures and block them	✓	✓	✓
Datacenter Based Detection	Check if clients are connecting from a datacentre and increase risk score if they are	✓	✓	✓
Scanner / Exploitable tools Checks	Identify scanner activity and automated exploitation tools connecting to the application, and block those requests	✓	✓	✓
Web Scrapper Checks	Check if known web scrappers are connecting and block those	–	✓	✓
Anomaly Behaviour Detection	Identify anomalous behavior of Bots and increase their risk score	–	✓	✓
JS Challenge	JS Challenge to block autonomous Bots	–	✓	✓
ML Bot Module	Machine learning module to identify malicious Bots based on the behavior and characteristics of requests	–	✓	✓

FEATURE COMPARISON

Key features	Benefits	Advanced	Premium	Enterprise
BOT MITIGATION (CONTD.)				
LLM Crawler Detection	Detect GenAI crawlers accessing the application and take action based on application needs	–	✓	✓
Advanced Mitigation Options	Take actions such as crypto challenges, serving fake data, and other mitigations based on application needs	–	✓	✓
Workflow Based Policies	Create custom, workflow based policies to detect and protect against sophisticated Bots	–	✓	✓
Device Fingerprinting	Uniquely identify devices via fingerprinting	–	✓	✓
Bot Analytics	Data intelligence for accurate data collection and analysis	–	✓	✓
Managed Bot Mitigation	Managed services support to analyze attack traffic and develop targeted mitigation strategies	–	✓	✓
Unlimited Bot Mitigation	No cap on number of Bot requests	✓	✓	✓
RISK MONITORING				
Guaranteed search engine access	Ensure that genuine search engines are not blocked	✓	✓	✓
False positive monitoring	AI-driven False positive monitoring verified by human experts	✓	✓	✓
Premium rules	Premium rules designed to block complex Layer 7 attacks. These are enabled after false positive monitoring	–	✓	✓
DDoS Notification	Get immediate alerts for any abnormal spike in traffic to your site	✓	✓	✓
Premium DDoS mitigation	Get complex DDoS attacks mitigated through expert monitoring and customized rules based on attacks	–	✓	✓
Unlimited Self Service Rules	Ability for customers to create custom rules using the intuitive rule builder	✓	✓	✓
AI-Powered Threat Intelligence	Threat Intelligence and tracking of the evolving landscape using an AI platform, augmented by signature experts and pen-testers.	✓	✓	✓
Custom rules made by experts	Protect complex business logic vulnerabilities through expert-written rules	2	Unlimited	Unlimited
Zero-day rule set	Get instantaneous protection for zero-day vulnerabilities through continuous updates written by experts	✓	✓	✓
Instant customization and propagation of security rules	Rules can be pushed instantly and propagated throughout the infra	✓	✓	✓
24X7 management by Certified Application Security Experts	Real-time incident monitoring, response and reporting	Limited	✓	✓
Continous Updates of Rules	Constant monitoring of emerging threats and update of rules as needed	✓	✓	✓

FEATURE COMPARISON

Key features	Benefits	Advanced	Premium	Enterprise
RISK MONITORING (CONTD.)				
Site Availability Notification	Notification of site availability and notification in case of unavailability of sites	✓	✓	✓
License Utilization Notification	Notification in case of pending expiry of service	✓	✓	✓
Attack Anomaly Notification	Notification in case of a surge of attacks	–	✓	✓
Latency Monitoring	Monitor round-trip time and send notifications for any sudden increase in average latency	–	✓	✓
Training	Training of customer team on WAF and other features in AppTrana	–	–	✓
Named Account Manager	A single point account manager who handles the entire account and represents the customer internally to accelerate solutions	–	–	✓
Quarterly Service Review	Review conducted by the Account Manager on service utilization, along with a detailed explanation of recent updates and enhancements	–	–	✓
EXTERNAL API SECURITY				
Managed API Scanning	Automated Scanning of APIs for OWASP Top 10 API Threats and more	–	✓	✓
API Classification	Classification of APIs based on sensitivity, including identification of APIs exposing PII/PHI data and unauthenticated APIs	–	✓	✓
API definition Support	Support to understand APIs by parsing Postman files to enable API Scanning	–	✓	✓
Shadow API Discovery	Discovery of APIs that are not part of the swagger definition, but request served by API Server	–	✓	✓
API Discovery	Discovery of APIs based on traffic	–	✓	✓
Open API Documentation	Auto creation of swagger documentation for APIs discovered	–	✓	✓
Automatic creation of a positive security model for APIs	Positive security policies created from Swagger files	–	✓	✓
API specific WAF policies	Specific rules to protect against the Top 10 API threats	✓	✓	✓
Behaviour Based DDOS Protection for APIs	Granular BDoS policies for critical APIs	–	✓	✓
API Specific Bot detections	API specific Bot policies	–	✓	✓
Automated Remediation of Vulnerabilities	SwyftComply: Industry-first, AI-driven remediation delivering zero-vulnerability reports in just 72 hours	–	✓	✓

FEATURE COMPARISON

Key features	Benefits	Advanced	Premium	Enterprise
WHOLE SITE ACCELERATION				
Carrier grade CDN	With the world's 4th largest, wholly-owned Tier-1 IP backbone network: TATA Communications Whole site Acceleration reduce latency to ensure content reaches users in the shortest possible time	✓	✓	✓
Content optimization	Accelerate site content through optimization techniques like minification, auto-compression etc.	✓	✓	✓
Automatic static content caching	Cache static contents like images, JavaScript files and CSS	✓	✓	✓
Dynamic content caching	Cache dynamic contents by enabling advanced caching	✓	✓	✓
Manual cache purge	Cache items can be instantly purged through the portal	✓	✓	✓
Custom cache header	Advanced caching policies can be crafted using url parameters, file paths	✓	✓	✓
Advanced Profiling	Profiling of site and improving caching to reduce load on servers	✓	✓	✓
Image Optimization	Optimization of images to improve the performance of pages that are heavy on Images	Add-On	Add-On	Add-On
DNS MANAGEMENT & SECURITY				
Authoritative DNS	DNS for domains/zones. Customers can create DNS zones, manage records, and serve DNS answers globally.	–	Add-On	Add-On
DDoS Protection & Security	Built-in protections: e.g. protection against DNS-related DDoS attacks, DNSSEC support, TSIG, protocol validation, etc.	–	Add-On	Add-On
OTHER FEATURES				
Unified Application Security Platform	Unified platform with a single pane of glass for EASM, DAST, WAAP, DDoS/Bot Mitigation, CDN, and API Security	✓	✓	✓
Analytics Page	Analytics page to analyze traffic logs for the site	–	✓	✓
Standard Reports	Detailed executive and site-level scan reports	✓	✓	✓
Integration into 3rd party CDN	AppTrana is CDN agnostic and will work seamlessly with any CDN	✓	✓	✓
Highly available and scalable architecture	Infrastructure that scales seamlessly to handle millions of requests concurrently	✓	✓	✓
Custom Port	Support for Custom Ports in Application	–	✓	✓
WebSockets	Support for applications that transmit traffic through WebSockets	–	✓	✓
HTTP v2	Support for HTTP v2 protocol	–	✓	✓

FEATURE COMPARISON

Key features	Benefits	Advanced	Premium	Enterprise
OTHER FEATURES (CONTD.)				
CI/CD Integrations	Integrations for CI/CD tools like Jenkins and JIRA to support shift left initiatives	–	✓	✓
Zero downtime onboarding	Entire onboarding is done in a few minutes with zero downtime for the site. Protection starts on day zero	–	✓	✓
SSO	Single Sign-on support for the dashboard, enabling user management in a single place	–	✓	✓
RBAC	Granular, feature-level, role based access control to customers	–	✓	✓
2FA	2 factor authentication	–	✓	✓
SIEM	SIEM APIs to integrate with any SIEM customer has for Real-time access to data	–	✓	✓
Design For Availability	Retain complete control of the site and have the ability to bypass AppTrana with a single click to ensure 100% site availability	✓	✓	✓
Log mode	Have the ability to have all rules in log mode and monitor logs to ensure no false positives	✓	✓	✓
Real-time logging	Get real-time access to logs and ensure quick notification and action in case of attacks	✓	✓	✓
Support	24/7/365 support through phone, chat and emails, backed by guaranteed response time SLA	✓	✓	✓

ABOUT INDUSFACE

Autonomous Application Security for the AI Era

Indusface secures the web, API, and AI applications of thousands of organizations across 95 countries. Backed by leading institutional investors, Indusface is recognized by Gartner, Forrester, and IDC for its innovation in application security and meets globally accepted security and compliance standards, including ISO 27001, SOC 2, PCI DSS, and GDPR. Its globally distributed cloud infrastructure spans Asia, the Middle East, Europe, and North America, enabling low-latency protection and regional data residency for enterprises worldwide.

AppTrana is Indusface's autonomous enterprise application security platform that continuously discovers vulnerabilities, autonomously remediates exploitable risks through virtual patching, and protects applications against DDoS, bot, API, AI, and zero-day attacks. Combining AI-powered intelligence, expert governance, and SLA-backed protection, AppTrana helps organizations reduce the time from vulnerability discovery to protection while delivering compliance-ready reports with zero false positives.

Bangalore | Delhi | Mumbai | Vadodara | Dallas

www.indusface.com | sales@indusface.com | support@indusface.com