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

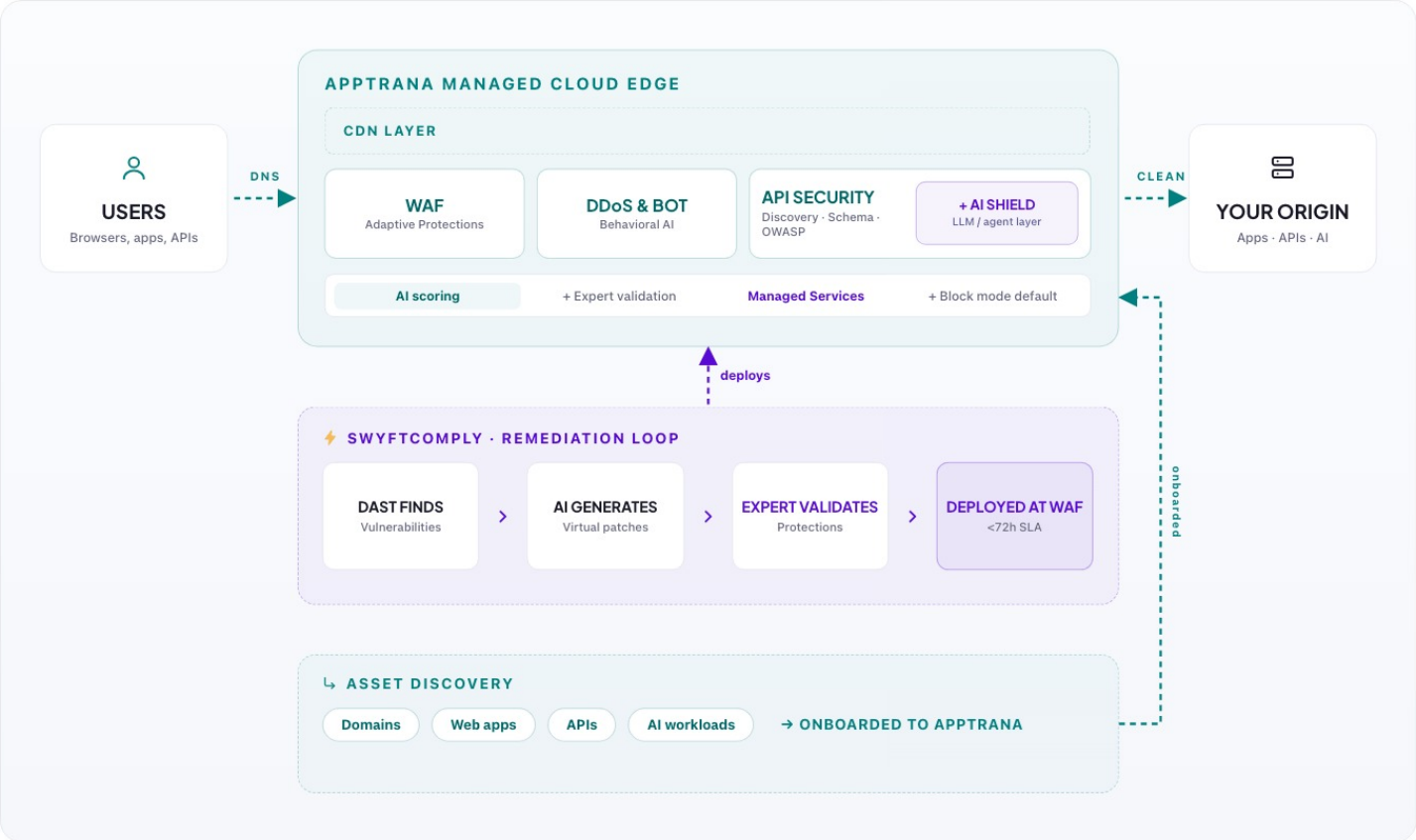
Unlimited
Expert support. No hours cap.

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

Risk detection & protection

Key features	Benefits	Advanced	Premium	Enterprise
RISK DETECTION				
Managed Application Security Scanning	Auto-scan for OWASP Top 10 and SANS 25 vulnerabilities.	✓	✓	✓
Full Support of HTML5, AJAX & JSON	Scan JSON, AJAX and HTML5-based sites.	✓	✓	✓
Remediation Guidance to Fix Vulnerabilities	Detailed guidance to fix each vulnerability.	✓	✓	✓
Vulnerability Revalidation Checks	Re-validate fixes to confirm vulnerabilities are closed.	✓	✓	✓
Guided Scans	Reach pages other scans cannot through guided automation.	✓	✓	✓
Authenticated Scans	Scan behind authenticated pages with provided credentials.	✓	✓	✓
Proof of Concepts	PoC for vulnerabilities to prioritise the right fixes.	5	Unltd	Unltd
Pen-testing by Experts	Experts ethically hack to find business-logic flaws.	–	Add-On	Add-On
Whitelisting of Vulnerabilities	Exclude accepted-risk vulnerabilities from reports.	✓	✓	✓
RISK PROTECTION				
Client-Side Protection	Protect against client-side / supply-chain script attacks.	✓	✓	✓
Layer 7 Protection	Inline inspection allows only legitimate traffic to the site.	✓	✓	✓
SwyftComply — Instant Vulnerability Remediation	Autonomous virtual patching; zero-vulnerability report in 72 hrs.	–	✓	✓
Virtual Patching via Advanced Rules	Zero-false-positive custom rules covering OWASP Top 10.	✓	✓	✓
Platform-specific Rule Set	Rules for platforms like WordPress, Joomla, etc.	✓	✓	✓
Restrict by IP & Geo	Block IPs and geographies based on traffic patterns.	✓	✓	✓
Whitelist URI & IP	Ensure critical URIs and IPs are never blocked accidentally.	✓	✓	✓
Risk Prioritization	See protected vs. unprotected vulnerabilities to prioritise fixes.	✓	✓	✓
Malware File Upload Protection	Restrict malicious file uploads and file types.	Add-On	Add-On	Add-On
PCI DSS 3.2 Compliance	Meet SOC 2, GDPR, PCI DSS, HIPAA, ISO 27001.	✓	✓	✓

FEATURE COMPARISON

DDoS & bot mitigation

Key features	Benefits	Advanced	Premium	Enterprise
DDOS MITIGATION				
Protection against Layer 3 & 4 Attacks	Always-on protection against network-layer attacks.	✓	✓	✓
Protection against Volumetric Layer 7 Attacks	Always-on protection against large volumetric L7 attacks.	✓	✓	✓
Geo-based DDoS Controls	Region-level DDoS policy limits.	✓	✓	✓
Behavior-based Layer 7 Protection	Behavioural analysis beyond simple rate limits.	✓	✓	✓
Captcha Challenges	Challenge suspected traffic to block automated attacks.	✓	✓	✓
Protection of Origin IP Address	Origin IP shielded; all traffic routed through the WAF.	✓	✓	✓
Protection against Hot-Linking	Protect bandwidth from unwanted hot-linking.	✓	✓	✓
Behavior-based URI-Level DDoS Protection	Granular DDoS controls for critical assets.	✓	✓	✓
Customize BDDoS Behavior	Control how long specific policies should block.	✓	✓	✓
BOT MITIGATION				
Allow Good Bots & Block Bot Pretenders	Detect bots pretending to be good bots and block them.	✓	✓	✓
Tor IP-based Detection	Raise risk score for requests from TOR clients.	✓	✓	✓
IP Reputation-based Protection	Score connecting clients by IP reputation.	✓	✓	✓
Scanner / Exploitable-tool Checks	Detect and block automated exploitation tools.	✓	✓	✓
Web Scraper Checks	Protect bandwidth and resources from scrapers.	✓	✓	✓
Validation of Bot Signatures	Validate requests against known bad-bot signatures.	✓	✓	✓
Anomaly Behavior Detection	Raise risk score on anomalous bot behaviour.	✓	✓	✓
Cookie Challenge-based Rules	Challenge suspicious clients with cookie tests.	✓	✓	✓
User-agent Based Detection	Score known malicious bots by user agent.	✓	✓	✓
Datacenter-based Detection	Raise risk score for datacentre-originated clients.	✓	✓	✓
Suspicious Countries	Raise risk score for non-business / suspicious countries.	✓	✓	✓

FEATURE COMPARISON

Risk monitoring & managed services

Key features	Benefits	Advanced	Premium	Enterprise
RISK MONITORING & MANAGED SERVICES				
Guaranteed Search Engine Access	Genuine search engines are never blocked.	✓	✓	✓
False Positive Monitoring	Experts monitor the core rule set for false positives.	✓	✓	✓
Premium Rules	Complex L7 rules enabled after false-positive monitoring.	–	✓	✓
DDoS Notification	Immediate alerts on abnormal traffic spikes.	✓	✓	✓
Premium DDoS Mitigation	Expert-monitored mitigation for complex attacks.	–	✓	✓
Unlimited Self-Managed Rules	Create and manage your own custom rules.	✓	✓	✓
Custom Rules Made by Experts	Expert-written rules for complex business-logic flaws.	2	Unltd	Unltd
Zero-day Rule Set	Instant protection for zero-day vulnerabilities.	✓	✓	✓
Instant Rule Customization & Propagation	Rules pushed and propagated instantly across the infra.	✓	✓	✓
24×7 Management by Certified Experts	Real-time incident monitoring, response and reporting.	✓	✓	✓
Continuous Updates of Rules	Rules updated as emerging threats are identified.	✓	✓	✓
Training	Full onboarding training of your team on AppTrana.	–	–	✓
Site Availability Notification	Real-time site availability alerts.	✓	✓	✓
License Utilization Notification	Alerts on pending service renewal.	✓	✓	✓
Attack Anomaly Notification	Alerts on a surge of attacks.	✓	✓	✓
Latency Monitoring	Alerts on increases in average round-trip time.	✓	✓	✓
Named Account Manager	Single point of contact managing your account.	–	–	✓
Quarterly Service Review	Review of service utilization and recent updates.	–	–	✓

FEATURE COMPARISON

Site acceleration, DNS & other features

Key features	Benefits	Advanced	Premium	Enterprise
WHOLE SITE ACCELERATION				
Carrier-grade CDN	Tier-1 TATA Communications backbone for full-site acceleration.	✓	✓	✓
Content Optimization	Minification and auto-compression.	✓	✓	✓
Automatic Static Content Caching	Cache images, JavaScript and CSS automatically.	✓	✓	✓
Dynamic Content Caching	Advanced caching for dynamic content.	✓	✓	✓
Manual Cache Purge	Instantly purge cached items from the portal.	✓	✓	✓
Custom Cache Header	Caching policies via URL parameters and file paths.	✓	✓	✓
Advanced Profiling	Site profiling to reduce server load.	✓	✓	✓
Image Optimization	Optimise images on image-heavy pages.	Add-On	Add-On	Add-On
DNS SECURITY				
Protection for DNS Hosts	Managed DNS hosting with built-in DDoS protection.	–	Add-On	Add-On
OTHER FEATURES				
Analytics Page	Independent analytics for traffic logs.	✓	✓	✓
Standard Reports	Executive and site-level scan reports.	✓	✓	✓
Integration into 3rd-party CDN	CDN-agnostic; works with any CDN.	✓	✓	✓
360° Application Security Posture Visibility	Comprehensive application risk-posture view.	✓	✓	✓
Highly Available & Scalable Architecture	Scales to millions of concurrent requests.	✓	✓	✓
Zero Downtime Onboarding	Live in minutes with day-zero protection.	✓	✓	✓
RBAC	Role-based access control.	–	✓	✓
2FA	Two-factor authentication.	–	✓	✓
SIEM	Feed any SIEM for real-time insights and alerts.	–	✓	✓
Bypass Mode	Bypass AppTrana with a single click.	✓	✓	✓
Log Mode	Deploy rules in log mode to confirm zero false positives.	✓	✓	✓
Real-time Logging	Real-time log access for quick action.	✓	✓	✓
Support	24×7 ISO 27001 support via email, chat and phone.	✓	✓	✓

ABOUT INDUSFACE

Autonomous Application Security for the AI Era

Indusface secures web, AI, and API applications of thousands of businesses across 95 countries. It is backed by institutional investors and is a category leader in cloud WAAP and API Security, with recognition from Gartner, Forrester, IDC, GigaOm, and G2.

Indusface AppTrana is the industry's only integrated autonomous application security platform that discovers and remediates vulnerabilities, and protects web, API, and AI applications against DDoS, bot, and zero-day attacks, backed by a 100% uptime guarantee. The human-in-the-loop system ensures zero false positives and SLA-backed compliance reports.

Bangalore | Delhi | Mumbai | Vadodara | Dallas

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