APPTRANA

Indusface AppTrana vs Imperva

Comparison

Indusface Analysis

- Imperva's base license is limited, and there are additional hidden charges that get added as add-ons
- Critical features like SIEM are treated as add-ons, and customers must pay extra
- Managed service is limited to basic monitoring and guidance activities. This also is an add-on

Unique Features of AppTrana

- Continuous monitoring and protection against OWASP Top 10, Zero-days, DDoS, Bot, and API attacks
- Proactive behaviour-based DDoS mitigation
- Real-time incident monitoring, response, and reporting
- 24-hour SLA for Virtually patching critical vulnerabilities
- Bundled VAPT: DAST Scanner + manual pen testing
- Asset and API Discovery to track external attack surface
- Zero false positives guarantee

AppTrana vs Imperva Business Comparison

APPTRANA

Key Features	Benefits	Indusface	Imperva
Asset Discovery			
External Asset Discovery	Discover external facing assets of an organization so no asset remains unprotected	✓	✗
Unlimited On-demand Scans	Ability to demand external asset scan for the organisation at any time	✓	✗
Risk Detection			
Managed Application Security Scanning	AppTrana automatically scans your site for OWASP Top 10 vulnerabilities	✓	✗
Full Support of HTML5, AJAX and JSON	Support to Scan JSON , AJAX and HTML5 based sites	✓	✗
Remediation Guidance to fix vulnerabilities	Get detailed information on how to fix the vulnerabilities	✓	✗
Vulnerability Revalidation Checks	Fix the vulnerabilities and have them quickly revalidated to know if 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 have scans be done behind authenticated pages	✓	✗
Proof of concepts	Get proof of concept for the vulnerabilities, enabling teams to prioritize risks	✓	✗
Pen-testing by experts*	Have experts ethically hack your sites and find business logic vulnerabilities	✓	✗
Risk protection			
Layer 7 protection	Get AppTrana to be in line with your website traffic to inspect traffic and allow only legitimate traffic to your website	✓	✓
Virtual patching through advance security rules	Have assured Zero false positive rules protecting OWASP Top 10 vulnerabilities out of the box	✓	✓
Platform specific rule set	Have rules written specifically for platforms like Joomla, WordPress etc.	✓	✓
Restrict by IP & Geo	Quickly block IP & Geo based on traffic patterns	✓	✓
Whitelist URI	Whitelist URI, to ensure that certain critical URI are not blocked accidentally	✓	✓
Self-learning behavioural rules	Have rules automatically become aggressive based on traffic patterns	✓	✓
Risk Prioritization	Portal provides a clear view of vulnerabilities that is protected, that can be protected, and which needs fixing in the code, allowing the application owner to prioritize critical bugs for development	✓	✗
Malware File Upload Protection	Restricting file uploads and type of file uploads that can be permitted to avoid uploading malicious files	✓	✗
PCI DSS 3.2 Compliance	AppTrana is PCI Compliant and enables you to meet PCI DSS 6.6 compliance effectively	✓	✓
Origin Protection	Protection of Origin by providing the ability to whitelist AppTrana IPs and block rest to ensure the origin is not directly attacked.	✓	✗
Packet Size Detected	Inspection of payload of 100 MB and more	✓	2MB
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 Protection against Layer 7 that is able to observe 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	✓	✗
Behaviour Based Layer 7 Protection	Protection against Layer 7 attacks using unique behaviourial analysis going beyond simple rate limits	✓	✗
Captcha challenges	Enable Captcha's so that suspected traffics are challenged to ensure automated attacks are blocked	✓	✓
Protection of origin IP address against DDoS attacks	Origin IP is protected against DDoS and forces all traffic to go through WAF	✓	✗
Protection against Hot-Linking	Protect against bandwidth and resources being used by other unwanted assets on the Internet	✓	✓
URI Based BDDoS Attack.	Configure granular DDoS controls for critical assets of the application	✓	✓
Customize BDDoS behaviour	Get control on how long certain policies should block	✓	✓
Scalable Infrastructure	Highly Scalable Infrastructure to handle sudden surge of attacks	✓	✓
BOT Mitigation			
Allow Good bots & Block Bot Pretender	Check for bots that are pretending to be good bots and block those	✓	Add-On
User Agent Based Detection	Checking for known malicious bots based on UA of requests and blocking or increasing risk score of identity	✓	Add-On
Suspicious Countries	Checking for countries where requests are coming from and increase risk score if it is from suspicious countries	✓	Add-On
Tor IP based detection	Check if the request is coming from Tor clients and increase the risk score	✓	Add-On
IP Reputation based protection	Check the IP reputation of connecting clients and increase risk score based on reputation	✓	Add-On
Validation of bot signatures and blocking bad bots	Validate requests for known bad bot signatures and block them	✓	Add-On
Datacenter Based Detection	Check if clients are connecting from a datacentre and increase risk score if they are	✓	Add-On
Scanner /Exploitable tools Checks	Check if scanners or other automated exploitation tools are connecting and block those	✓	Add-On
Web Scrapper Checks	Check if known web scrappers are connecting and block those	✓	Add-On
Anomaly Behaviour Detection	Identify anomalous behaviour of bots and increase the risk score	✓	Add-On

AppTrana vs Imperva Business Comparison

APPTRANA

Key Features	Benefits	Indusface	Imperva
Risk monitoring			
Guaranteed search engine access	We ensure that genuine search engines are not blocked	✓	✓
False positive monitoring	Get experts monitor the CRS for false positives & have rules tweaked to your site to ensure zero false positive	✓	✗
Premium rules	Premium rules which block complex layer 7 rules. Have them enabled after false positive monitoring		✓
DDoS Notification	Get immediate alerts on any abnormal spike in traffic to the site	✓	✓
Premium DDoS mitigation	Get complex DDoS attacks mitigated through expert monitoring and customized rules based on the attacks	✓	✗
Custom rules made by experts	Complex business logic vulnerabilities can be protected through expert written rules	✓	✗
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	✓	✓
Continous Updates of Rules	Constant monitoring of emerging threats and update of Rules as needed	✓	✓
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 surge of attacks	✓	✓
Latency Monitoring	Monitoring of round trip time and notification for sudden increase in average round trip time	✓	✗
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 customer internally to accelerate solutions	✓	✓
Quaterly Service Review	Review done by Account Manager on utilization of service and explanation of recent updates made	✓	✓
API Security			
Managed API Scanning	Automated Scanning of APIs for OWASP Top 10 API Threats and more	✓	✗
API definition Support	Support to understand APIs by parsing postman files to enable API Scanning	✓	✗
API Discovery	Discovery of APIs based on traffic	✓	Add-On
Open API Documentation	Auto creation of swagger documentation for API discovered	✓	Add-On
Auto creation of Positive security model for APIs	Positive security policies created from Swagger files	✓	Add-On
API specific WAF policies	Specific Rules to protect against Top 10 API Threats	✓	Add-On
Shadow API Discovery	Discovery of APIs that are not part of swagger definition, but requests served by the API Server	✓	Add-On
Behaviour Based DDoS Protection for APIs	Granular BDDoS Policies for critical APIs	✓	✗
API Specific BOT detections	API specific BOT detection policies	✓	✓
Whole Site Acceleration			
Carrier grade CDN	With the world's 4th largest, wholly-owned Tier-1 IP backbone network: TATA Communications Whole site Acceleration reduces 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, java script files and CSS	✓	✓
Dynamic content caching	Cache dynamic contents by enabling advance caching	✓	✓
Manual cache purge	Cache items can be instantly purged through the portal	✓	✓
Custom cache header	Advance caching policies can be crafted using url parameters, file paths	✓	✓
Adv Profiling	Profiling of the site and improving caching to reduce load on servers	✓	✓
Image Optimization	Optimization of Images to improve the performance of pages which are heavy on Images	✓	✓
Other Features			
Analytics Page	Analytics Page to analyse traffic logs for the site	✓	✓
Standard Reports	Detailed Executive , site level and scan reports	✓	✓
Integration into 3rd party CDN	AppTrana is CDN agnostic and will work seamlessly with any CDN	✓	✓
360* visibility into the application security posture	With an integrated Scanner and WAF, we provide a comprehensive view of the application risk posture	✓	✗
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 passing traffic through Websockets	✓	✓
HTTP v2	Support for HTTP v2 protocol	✓	✓
Zero downtime onboarding	Entinre onboarding is done in a few minutes with zero downtime for the site. Protection starts on day zero	✓	✓
RBAC	Role based access control to customers	✓	✓
2FA	2 factor authentitication	✓	✓
SIEM	SIEM APIs to integrate with any SIEM that customer has for real time access to data	✓	✓
Bypass mode	Retain complete control of the site and have the ability to bypass AppTrana with a single click	✓	✗
Log mode	Have 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	✓	✓