SRC CYBER SOLUTIONS LLP

THREATX | BATTLE CARD

LEGACY WAFs vs. THREATX

ThreatX protects web applications and APIs from cyber threats across cloud and on-prem environments. By combining behavior profiling and collective threat intelligence with deep analytics, ThreatX delivers precise protection and complete threat visibility. ThreatX Managed Service combines threat hunting with 24/7 access to security experts along with operational management, virtually eliminating costs associated with legacy WAFs.

ThreatX Web Application and API Protection Solution:

Unlike legacy WAFs that use inaccurate, signature-based blocking approaches and focus solely on the application, ThreatX focuses on the attacker, combining and corroborating multiple indicators of suspicious activity. As a result, ThreatX builds a progressive risk profile of intent, making accurate blocking decisions based on real behaviors. ThreatX is SaaS-based.

ThreatX protects against things like vulnerabilities, OWASP top 10, account takeovers, Bots (online fraud, fake account creation, content scraping, carding, marketing fraud, inventory abuse, credential stuffing), etc.

ThreatX AppSec-as-a-Service Offering

As an extension of your team, ThreatX's built-in AppSec-as-a-Service (ASaaS) offering combines threat intelligence, operational management and threat hunting with 24/7 access to a team of appsec experts, eliminating burdens on your team as well as reducing your ROI:

PROBLEMS WITH LEGACY WAFs

- ☒ High operational burden due to the high false positive rates inherent in legacy WAFs
- ☒ Heavy administrative burden as a result of continual tuning and configuration
- ☒ Painful deployment that can take weeks or months and ultimately only protect a subset of the application portfolio
- ☒ AppSec solutions that directly impact application availability via high false positive rates and inherent instability
- ☒ High rate of change from application development driving up WAF configuration and admin costs
- ☒ Need for seamless appsec integration with modern app deployment approaches (container and cloud)

THREATX

- ✓ **Single solution:** protection across entire application space, enterprise deployment types, and attack space
- ✓ **Precise protection:** high true positives and negatives
- ✓ **Ability to stay ahead of attackers:** protection for known vulnerabilities/virtual patching as well as automated behavior analysis for detection of new attacks
- ✓ **High availability:** actually exceeds availability of the applications it protects
- ✓ **Complete visibility:** into application security data for effective incident investigation
- ✓ **Near zero operational cost:** lower operational costs with access to expertise and operations management to support enterprise app sec needs

What's the difference between legacy WAFs & modern solutions, like ThreatX?

Legacy WAFs use inaccurate, signature-based blocking approaches and focus solely on the applications themselves. ThreatX focuses on the attacker, tracing their progress through the complete attack life cycle, combining and corroborating multiple indicators of suspicious activity. ThreatX builds a progressive risk profile of threat intent and makes highly accurate blocking decisions based on real behaviors, rather than inaccurate, static signature matching.

LEGACY vs THREATX

CUSTOMER NEEDS	LEGACY WAF	THREATX NEXT GEN WAF
HIGH ACCURACY THREAT DETECTION	Threat detection through predefined signature matches. **RESULT: High false positives, and limited zero-day identification**	Threat detection through attacker tracking, behavioral modeling, and risk measurement. **RESULT: High true positive, high true negative threat detection**
RIGHT-TIME RISK BASED PROTECTION	Traffic blocking based on binary signature matching and simple algorithmic analysis **RESULT: App protection requiring extensive administration by SecOps**	Dynamic traffic blocking based on real-time attacker behavior and multi-factor risk scoring. **RESULT: App protection that evolves with the attack landscape and application**
RAPID THREAT IDENTIFICATION	Threat analysis performed on a per application basis. **RESULT: New threat identification restricted to individual apps.**	Threat analysis performed across all apps & all customers worldwide. **RESULT: Fast identification and protection from emerging threats**
TUNELESS ADMINISTRATION	Threat protection updates through manual signature and rules. **RESULT: High burden for constrained security teams**	Automatic threat protection based on attacker tracking and real-time app profiling. **RESULT: Minimal maintenance and tuning burden**
UBIQUITOUS DEPLOYMENT ALIGNED WITH DEVOPS	Appliance and basic SaaS deployment options. **RESULT: WAF deployment and tuning can be out of sync with Devops**	Cloud-native, container based, auto-scaling with world-wide footprint. **RESULT: Auto-tuning/scale/update aligned with DevOps, and cloud**
ACCESS TO SECURITY AND OPERATIONAL EXPERTISE	Reactive managed service. Customer burden to maintain. **RESULT: Substantial customer staff investment required**	Proactive security experts that continually assesses target apps and vulnerabilities. **RESULT: Minimal customer investment & expertise required**

What to **LISTEN** for to recognize a new project:

- Need app protection solution quickly and do not have the staff for the project
- Recent malicious attacks (bot or not) on web applications & APIs
- Need to reduce the high application security operational costs
- Need to reduce deployment time to keep pace with app proliferation & DevOps requirements
- Cloud migration initiatives
- Need to address compliance (e.g., PCI) via WAF deployment

What to **ASK** when qualifying prospects:

- How are you securing your applications today?*(current solutions)*
- What is the level of false positives you are experiencing with your application protection solution today?
- Are you able to on-board application security protection in a day? *(current solutions)*
- Do you have staffing and access to appsec expertise?
- Are you able to track down the details of an attack when your security team needs to?
- Do you have a need to protect your cloud as well as on-prem applications?
- Do you have APIs and web services that need protection? *(breadth of protection needs)*
- Are you getting attacked by Bots, scrapers, account take-overs, credential stuffing? *(common and emergent use cases)*

COMPETITORS

COMPANY	LEGACY?	WEAKNESSES
Akamai	✓	High costs, unsatisfactory customer service, incomplete app protection with curated rules leaving protection gaps.
Imperva	✓	Legacy WAF approach based on rules and a negative security model, weak DevOps integration with no container deployment support and weak API.
F5	✓	Legacy WAF based on rules and negative security model, heavy operational costs due to frequent tuning.
Signal Sciences	✓	Limited behavioral attack and bot detection. Unbounded enterprise spend due to need for professional services.
Cloudflare	✓	Legacy WAF with curated rules leaving protection gaps, unsatisfactory customer service.