Next-Gen, SaaS-Based Web Application Firewall

DDoS, Bot, and CDN Capabilities in One Solution.

The ThreatX vs. other Next-gen and Legacy WAF's

Instead of focusing solely on the applications themselves,ThreatX focuses on the attacker. By tracking their progress through the kill-chain, and combining and corroborating multiple indicators of suspicious activity,ThreatX is able to build a progressive risk profile of threat intent.

	Legacy WAF	ThreatX
Approach	- Static rules and signatures (but evolving)	- Purpose-built, attack-centric, kill-chain based contextual analysis
Event Correlation and Analysis	- 10,000 -100,000+ suspicious events per application, per day • Manual analysis overload security team • Purchase and integrate a separate log correlation	- Continuous real-time corroboration, correlation and analysis of all suspicious events (across applications and customers) in real time. - Complete forensic record of all activity for malicious entities instantly available
Operational Overhead	- Manually tune and customize hundreds of static rules and signatures to effectively block malicious entities without blocking legitimate traffic	- Automated response based on risk analysis and a clearly articulated pattern of behavior - Dynamic rule sets that evolve with threats and changes to the environment
Installation and Configuration	- 2-4 weeks of analysis and tuning by customer per application	- 1-2 days to safe blocking via machine learning and auto-tuning
Upgrades and Maintenance	- Customer's responsibility to schedule and perform patches and upgrades to the platform	- Highly scalable, Cloud-based, SaaS platform continuously maintained by ThreatX for all customers

ThreatX WAF Sensor Capabilities

The ThreatX platform delivers rapidly deployable, kill-chain based threat detection and neutralization in a highly adaptable, cloud-based architecture designed for modern application environments and constantly evolving threats. The ThreatX WAF Sensor is packaged asa Docker container and can be deployed on-premises, in private and public clouds, in hybrid clouds, and even hosted within the ThreatX worldwide cloud. Capabilities include:

	Description	Benefits
Application Profiling	- Machine learning that determines appropriate application inputs and responses while continuously adapting to application and environmental factors	- Rapid application baselining - Faster threat identification - Fewer false positives
Entity Behavior Profiling	- Real-time/continuous threat identification, classification, and correlation for all suspicious IPs/entities across all applications and customers.	- Automated behavior recognition and dynamic rule generation - Instant visibility to highest risk attackers and targeted applications - Complete visibility to attack profile and targeted application weaknesses
Attacker Fingerprinting	- Cookie injection, JavaScript injection, and IP profiling to fingerprint suspicious IPs for future identification and event correlation	- Botnet Detection - Correlation of events for attacks executed from multiple IP's - Ability to track multiple users behind the same address
Active Deception	- Injection of fake fields, URLs, error codes, headers, JavaScript, etc. for bot identification	- Differentiate between legitimate users and bots - Reduce server load from botnet traffic - Protect from Account Take Over and other bot attacks
Cross Customer Correlation	- Risk analysis and active blocking based on suspicious entity behavior correlated across applications and customers over time - The ability to define appropriate action as risk escalates	- Highly accurate decision/response engine - Fewer false positives without creating backdoors/false negatives - Dramatic reduction in threat analysis and response workload for overburdened security teams

ThreatX Bot Detection Capabilities

ThreatX's revolutionary approach to the WAF changes how organizations can see and mitigate bots and other forms of malicious automation. This stems from ThreatX's unique capabilities that blend multiple approaches of behavior analysis with active engagement.

Capability	Benefits	Bot Types Mitigated			
		DOS	Scraping	Credential Stuffing	Fake Account Creation
Application Profiling Machine learning and heuristics baseline your normal application traffic	- Quickly profile sites and API's and block bots (w/in 24 hours) - Automatically tune entity behavior rules to identify normal vs. bot traffic - Continuously adapt to application changes	X	X	X	X
Entity Profiling Killchain modeling of site visitor behaviors for signs of bot activity and other application threats	- Highly accurate bot behavior detection - Highly accurate web and API threat detection - Classify all bots by behaviors	X	X	X	X
Cross Site and CrossCustomer Correlation Detect bots and threat actors before they attack your sites	- Understand the true risk level of a bot or attacker in seconds - Rapid analysis from common entity names across sites and customers - Quickly mitigate known bad actors - Access real time threat data not available from standard intel feeds	X	X	X	X
Curated Intel High quality threat and behavior intel for commodity bots	- Low false positive rates - Reduce the burden of maintaining intel - Community identification of commodity bots - Catalogs known good and bad bots	X	X		
Attacker Interrogation Fingerprint the attacker via cookies and JavaScript injection	- Easily track bots with similar attributes across many IP addresses - Track attackers as they hop from IP to IP			X	X
Active Deception Inject fake links, form fields, error codes, etc. in HTTP responses	- Improve bot detection and classification fidelity - Infer entity intent well ahead of attack		X	X	X
Tarpitting Slow down HTTP responses to detected bots and attackers	- Increase the overhead "cost" of bot activity for the attacker - Identify and slow persistent attackers - Reduce L7 DOS exposure	X	X	X	X
Custom Behavior-based Rules Create custom rules to block or allow specific bot activity	- Block bad bots while allowing desired automated activity - Augment automated detection with human intelligence	X	X	X	X
Volumetric DDOS Scrubbing Mitigate L3 and L4 DDOS attacks from bots	- On-demand or Always-on options - Terabit scale protection	X			
Cloud Native Deployment Easily deploy as a container in any environment without redesigning the architecture	- AWS, Azure, Google Cloud, etc. - VMware, OpenStack - Kubernetes (service layer or sidecar pattern) - Scales without increasing cost				
Consolidated Application Security Platform Reduces the number of application security platforms to manage	- Single dashboard for bot detection and application security - Simplifies management and upgrades - Reduced latency to the application				
Fully Managed Option SOC augmentation of Level 1 to Level 3 issues	- 24x7 monitoring and custom rule implementation for the most comprehensive bot detection and mitigation - Bot and web application attack expertise - 10-minute response SLA on urgent requests - No need to manage sensors on-premises				
API Management RESTful JSON API to manage all aspects of the platform	- Fully automate incident response - Easily integrate with your existing security stack - Full compatibility with orchestration platforms				
SIEM Integration Log emitter for on-premises log storage and analysis	- JSON Lines format for future-proof compatibility - Secure, encrypted connectivity - Allows long-term storage of bot detection and mitigation events				