THREATX

DATA SHEET

ThreatX Platform vs. AWS & Microsoft Azure WAF

The built-in security capabilities of AWS and Azure offer basic and limited protection, and require extensive tuning and maintenance to provide effective API and web app protection.

The ThreatX platform offers robust API and web app protection immediately, with virtually no tuning or maintenance.

The ThreatX platform scans all inbound API and web app traffic in real time, identifying and blocking attacks. This real-time monitoring enables ThreatX to execute advanced threat engagement techniques, such as IP fingerprinting, interrogation, and tar-pitting. When a series of user interactions cross an established risk threshold, ThreatX blocks the attack. These capabilities allow ThreatX to identify and stop the most complex attacks, including large-scale bots and DDoS-level threats.

	AWS/Azure WAF	ThreatX
Custom Rules & Rules Management	Static rules engines – with only five custom rules out of the box Additional rules would have to be customized/paid for	Comes with out-of-the-box, behavior-based detection that requires little to no tuning, as well as risk-based blocking Enables robust protection within hours & minutes vs. days & weeks with no maintenance required
Configuration & Tuning	Enabled easily but require extensive: • Customization and management to detect more than OWASP Top 10 attacks • Tuning to avoid false positives and blocking of legitimate traffic	ThreatX's 24x7 experts act as an extension of your team and help with onboarding, support, and security operations Little to no tuning and configuration required Once the initial sensor configuration is deployed, adding new hostnames is less than 5 minutes
Cloud Environment Support	Only protection for AWS/Azure apps	Cloud-agnostic coverage – even if acquire non-AWS or Azure apps, or switch to GSP or other hosting solution
Bot Protection	Basic bot detection	DDoS, API, WAF, plus advanced bot detection in ThreatX platform
DDoS Protection	No Layer 7 DDoS protection	DDoS, API, WAF, plus advanced bot detection in ThreatX platform
False Positives	High false positives	Risk-based blocking creates very few false positives, and allows "set it and forget it" blocking mode Better protection, less work
Attack Visibility	No visibility into attack data	Visibility into attacker behavior across threat actors, attack types, and targets