THREATX

Web Application and API Protection (WAAP) that Just Works

PROTECT YOUR APPS

Anywhere. Effortlessly.

It Just Keeps Getting Tougher Every Day

More apps. Changing architectures. More sophisticated threats. Who has the time—or the staff—to keep up with it all?

Modern organizations need to support both on-prem and hybrid cloud environments. APIs and microservices architectures must be securely protected to prevent abuse and thwart debilitating attacks. At the same time, revenue-generating access to those same services must be allowed to flow freely. And, to make matters worse, a wide array of highly sophisticated and high-impact threats like injection attacks, denial of service, account takeover, brute force, credential stuffing, vulnerability scanning, and web scanning are persistently targeting the perimeter.

The result? An untenable burden on security staff who are required to constantly tune rules, analyze false positives and false negatives, and investigate inconclusive anomalies.

Add to all of that the need to work in lockstep with DevOps teams, and you've got a perfect storm of security challenges brewing.

It's complicated. And legacy WAFs are falling short in delivering solutions that help. ThreatX's cloud-native Web Application and API Protection (WAAP) takes a fresh approach that eliminates many of the headaches currently associated with legacy WAFs.

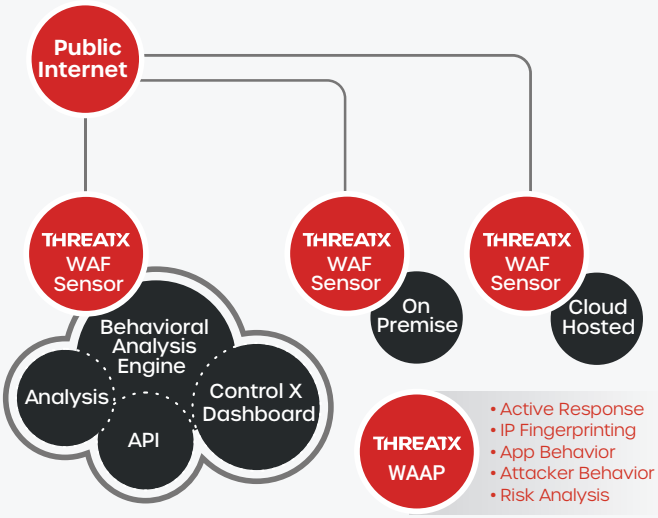
Gartner observed a 15% growth in WAAP inquiries in 2020 compared with the previous year...attributed to the expansion of organizations' digital transformation initiatives adding more applications and APIs to their portfolios.*

An Attacker-Centric Web Application Security Solution

ThreatX protects web applications and APIs from cyber threats across cloud, on-prem and hybrid environments, by delivering precise protection and complete threat visibility. A unique combination of behavior profiling, collective threat intelligence, and deep analytics delivers confident coverage. Our Fully-Managed WAAP Security Service provides on-demand access to AppSec experts 24/7 that reduces added costs associated with legacy WAFs.

ThreatX alleviates many of the headaches currently associated with legacy WAFS:

- A complete solution for all types of threats: OWASP Top 10, bots, targeted attacks, and DDoS
- Native cloud deployment implementations will have you blocking in hours, not days
- Unprecedented visibility into the attacks targeting your business
- On-demand, 24/7 access to AppSec experts reduces the need for internal expertise



"The real business benefit for us, first and foremost, is the level of protection that ThreatX provides to our web applications. Next would be the ability to provide this protection across all our services with very little overhead. Using ThreatX moves us forward without impacting my team's constrained resources."

Senior Director of Information Security,
BMC Software

The ThreatX Platform

HOW IT WORKS

- A kill-chain based approach classifies suspicious behaviors and associated risks
- Simple, SaaS-based deployment provides coverage for hybrid app environments & all APIs
- IP interrogation uses javascript injection, cookies, & forms to validate suspicious users
- Deep visibility into attack activity, attack classifications and risks enabling teams to perform incident triage and response
- Shared threat analytics correlates attack patterns and techniques across multiple customers and apps
- Threats are blocked in real-time based on a configurable risk score
- Access to managed services for additional threat hunting or analysis and monitoring 24x7
- Combines Bot, DDoS, and WAF protection in a rapidly-deployable, cloud-native solution

LIVE DEMO

Ready to look under the hood of a cloud-native WAAP solution?

Take the next step. Request a demo today and see how you can effortlessly protect your web apps and APIs against today's complex threats while reducing the burden on your security team.

* Source: Gartner, Magic Quadrant for Web Application and API Protection, 20 September 2021, Jeremy D'Hoinne et al.