THREATX

SaaS-Based Web Application Firewall Protection

A Fundamentally DIFFERENT APPROACH to Web Application Threat Protection

The Challenges of Today's Web Application Environments

The complexity of modern, hybrid cloud and heterogeneous technology environments combined with an ever-evolving threat landscape creates a large and dynamic attack surface for almost any organization. Furthermore, "next-gen" rule, signature, and anomaly detection-based web application firewall (WAF) solutions are missing the most critical, high-impact attacks because they lack contextual information on the attacker itself. As a result, security teams are armed with limited intelligence from their current tools to address an increasing volume of sophisticated attacks.

73% organizations surveyed use a WAF, yet...

80% were compromised.

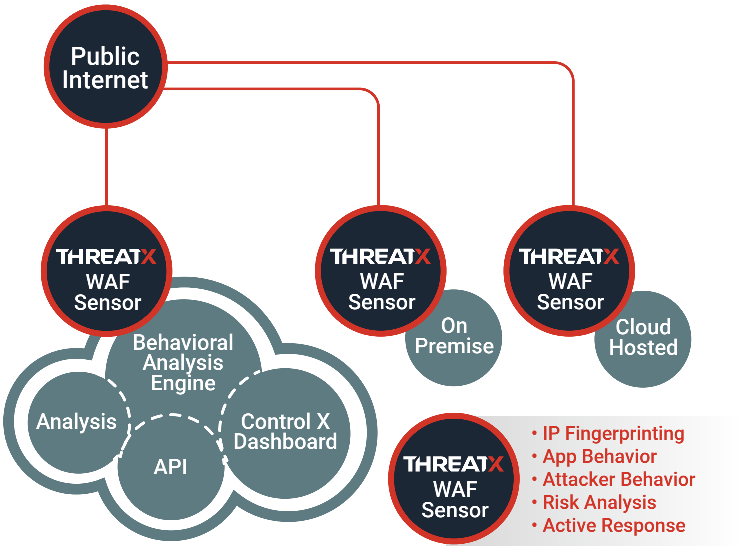
Source: Ponemon Institute, *Trends in the Cost of Web Applications and Denial of Service Attacks*, **September 2017**

An Attacker-Centric Web Application Security Solution

ThreatX's next-generation web application firewall addresses the gaps left by other 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. The result is deep visibility into the varying attack types and techniques, as well as the target vulnerabilities in your application environment.

ThreatX has transformed web application protection with a highly effective and accurate threat mitigation solution that reduces false positives without the constant tuning of rules and signatures:

- Precise detection and neutralization of even the most sophisticated, high-impact attacks (SQLi, XSS, OWASP)
- Comprehensive and accurate views into risk and vulnerability levels
- Significantly lower operational burden and cost



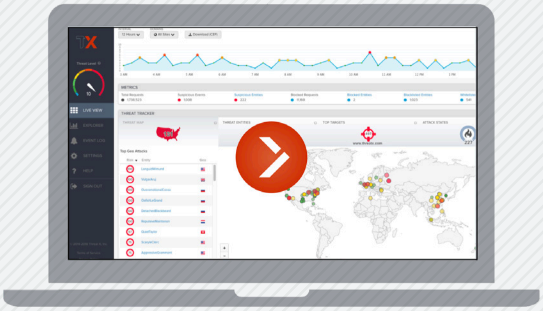
The ThreatX Platform

HOW IT WORKS

- A kill-chain based approach classifies suspicious behaviors and associated risk
- IP Interrogation uses javascript injection, cookies, and forms to validate suspicious users and build attacker profiles
- Deception overlays customer applications with bait URIs, headers, and forms to lure attackers into disclosing their intentions
- Shared threat analytics correlates attack patterns and techniques across multiple customers and applications
- Threats are blocked in real-time based on a configurable risk score, instead of rules

Combined Bot, DDoS, CDN, and WAF in a Rapidly Deployable Cloud-Native Solution

> *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



FREE TRIAL

Ready to see what a next-gen WAF should really do?

Take the next step. Start your free trial today and see how easy it is to enable comprehensive, unparalleled protection for your application environment from today's advanced threats.

TRUSTED BY GLOBAL ENTERPRISES

UNIVERSAL — UNIVERSAL MUSIC GROUP · Thrifty · KSE Kroenke Sports & Entertainment · bmcsoftware · GHX

THREATX

info@threatx.com
+1 888-303-5580

© 2018 ThreatX, Inc.