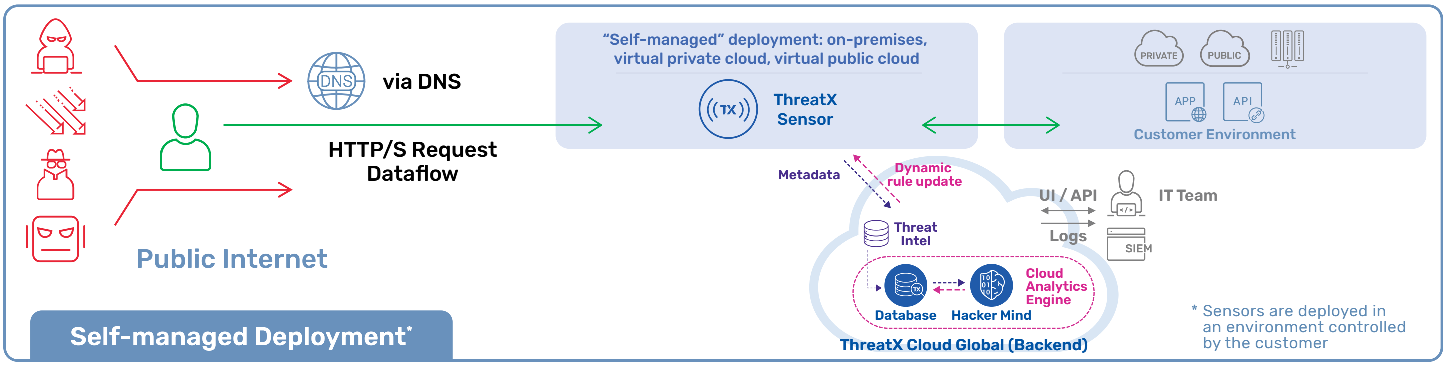
A10

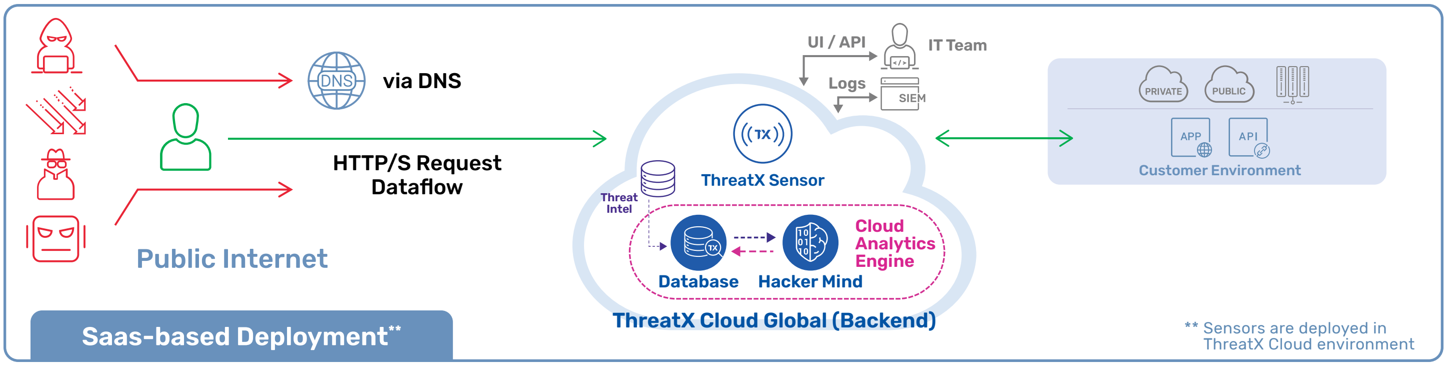
ThreatX by A10 Networks

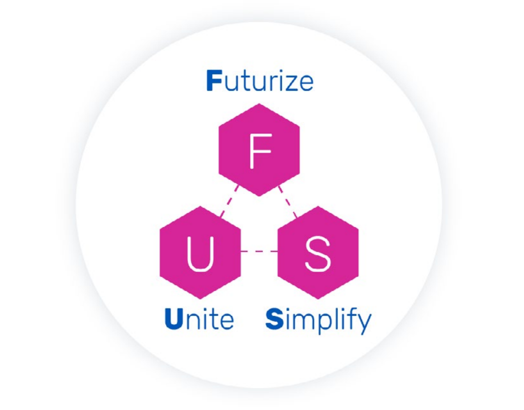
A Web Application Protection Platform (WAPP) That Cohesively Protects Your Application Ecosystem From Attacks and Attackers

Defending the True Target: Applications

ThreatX by A10 Networks is more than a traditional WAF. It provides application protection from the inside out. While WAFs predominantly protect against application-layer attacks, and API protection protects against API attacks, these approaches miss the bigger picture: attackers are not targeting vectors—they are targeting applications, the lifeblood of modern businesses. ThreatX takes a unified approach, protecting the application ecosystem against both attacks and attackers. It uses adaptive risk scoring that continuously evolves based on transaction/entity-based tracking, cross-vector correlation, historical behavior, and other factors to improve accuracy. This protection is further reinforced by the ThreatX SOC, which helps manage ThreatX, and therefore, manages the protection of your application ecosystem. With SOC teams facing an average of more than 3,000 alerts per day (Hacker News, 2025), separating real threats from noise is no longer humanly scalable. The ThreatX solution filters and validates malicious activity automatically, double-checks its own work, then has the ThreatX SOC team apply human expertise to triple-check the list of alerts before sending them off to customers, ensuring customers receive only high-confidence, actionable alerts while streamlining application security operations.







Futurize, Unite, and Simplify (FUS) the Protection of your Application Ecosystem

ThreatX unites protection across API, web, bot, and DDoS into a unified platform, a web application protection platform. Here's how:

- **Futurize**: ThreatX leverages advanced ML, behavioral learning, and risk-based profiling to stay ahead of attackers.
- **Unite**: Instead of siloed defenses, ThreatX correlates activity across attack vectors and uses the information cohesively to adjust detection and mitigation strategies.
- **Simplify**: Instead of buying a WAF, then tacking on API protection, and then layering on bot and DDoS defense, ThreatX delivers protection in a unified platform.

Read Blog

How It Works

- **Unified protection for your applications (WAPP)**: There are several problems with current application security approaches. Coverage is often incomplete and relies on multiple best-of-breed tools. This results in higher costs through add-on pricing, increased technical debt due to specialized expertise requirements, and reduced effectiveness as excessive false positives overwhelm security teams. Adding a SIEM does not solve these issues, as alerts still require manual analysis. Without a unified approach, protection is delivered by individual vectors, rather than protecting the intended target: applications. The web application protection platform (WAPP) approach cohesively protects the application ecosystem against both attacks and attackers. By delivering integrated, built-from-within protection, WAPP reduces cost and complexity while improving accuracy by aligning multiple defense vectors around a single goal: protecting applications.
- **Adaptive risk scores:** ThreatX uses an adaptive risk score, generated by cross-vector correlation, entity/transaction-based tracking, and battle-tested machine learning, to continuously adjust and elevate accuracy. As an example of cross-vector correlation, early indicators of bot-like behavior can raise an entity's risk score, while subsequent actions, such as L7 DDoS or API attacks, escalate it more rapidly using accumulated behavioral context. ThreatX, via Hacker Mind, continuously tracks both malicious transactions (snowballs) and the entities behind them (snowball throwers), updating risk in real time. Together, Hacker Mind's adaptive risk score is the key behind the cohesive application protection, which point solutions struggle to replicate.
- **ThreatX SOC team allows for continuous monitoring, tuning, and response:** Customers benefit from expert analysts who manage policies, investigate alerts, and take action in real time. This greatly streamlines application security operations. For example, during the React2Shell (CVE-2025-55182) vulnerability, the ThreatX SOC team had already identified the underlying attack behaviors well before public disclosure. As such, they were able to deploy protections ahead of the widespread exploitation. This proactive detection goes beyond virtual patching, providing customers with protection before zero-day vulnerabilities escalate into active attacks.

Hacker Mind

- Utilizes an adaptive risk score, generated by
  - Entity/transaction-based tracking
  - Cross-vector correlation
  - Battle-tested machine learning algorithms

WAPP

- A web application protection platform (WAPP) takes a unified, integrated, built-from-within approach to secure your application ecosystem against attacks and attackers.

SOC

- ThreatX the product is proactively, automatically, and continuously fine-tuned to best protect your application ecosystem. The produced alerts are double-checked by the ThreatX solution. This filtered list of alerts is checked by humans in the ThreatX SOC team before the finalized list of alerts is delivered to the customer.

Flexible

- ThreatX seamlessly fits into your application environment, not the other way around. It can be deployed in the following methods:
  - Self-managed: sensors are deployed in environment controlled by customer on-premises, private cloud, public cloud
  - SaaS-based: sensors are deployed in the ThreatX cloud
  - Fully self-hosted: sensors and Hacker Mind deployed locally
- Deployed in hours to days, instead of weeks to months

Adaptable

- Custom policies and needs can be addressed and implemented

About A10

A10Networks.com

Contact Us
A10Networks.com/contact

Part Number: A10-BR-20118-EN-04 Jan 2026