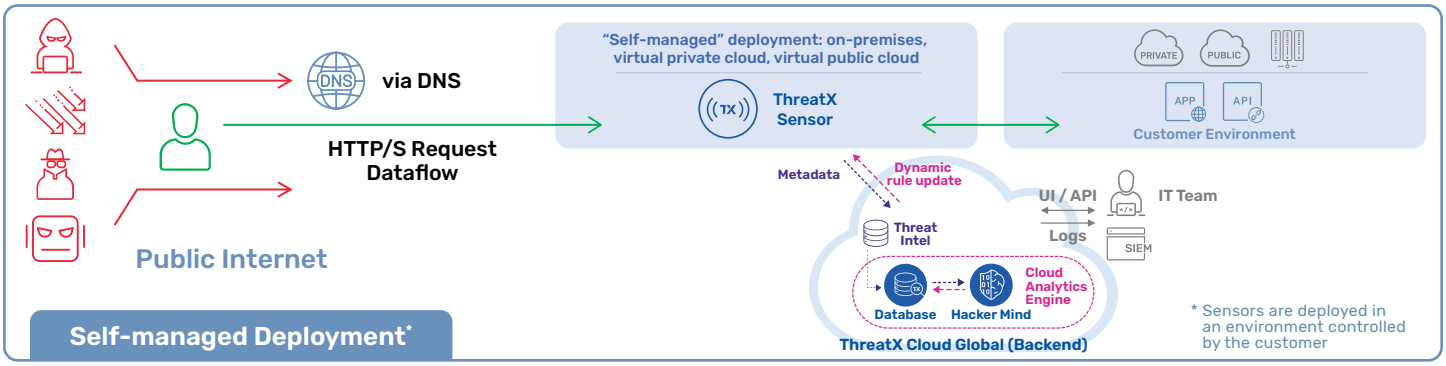
ThreatX

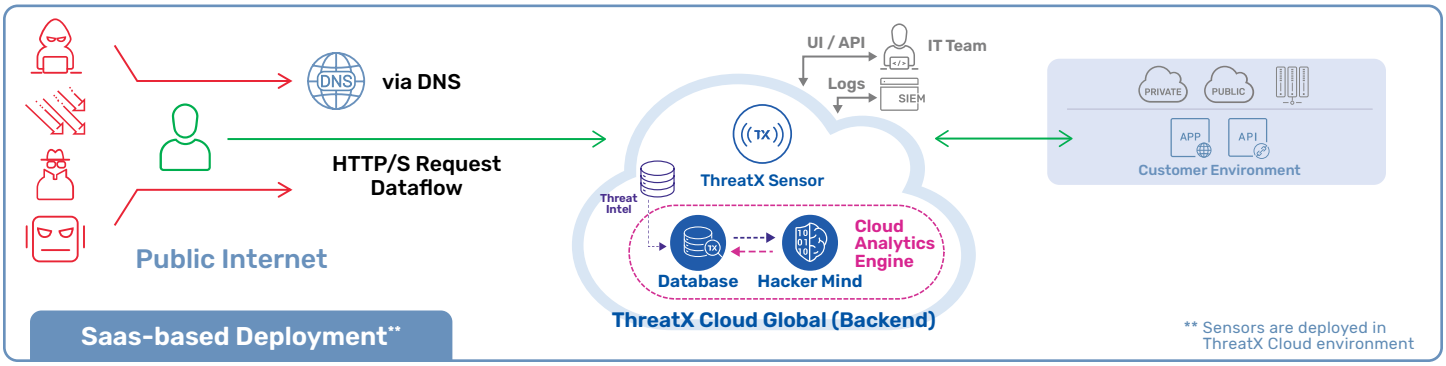
by A10 Networks for Healthcare

A Web Application Protection Platform (WAPP) That Protects Your Healthcare Application Ecosystem from Attacks and Attackers

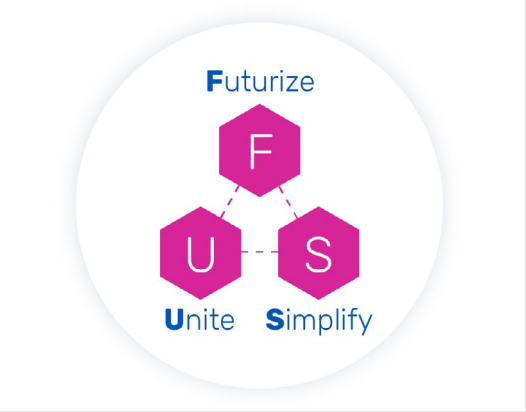
Defending the True Target: Applications

ThreatX by A10 Networks delivers application protection for modern healthcare ecosystems where patient data is accessed via applications, APIs, and even AI-driven workflows. While traditional WAFs focus on application-layer attacks and API security tools focus narrowly on API endpoints, these approaches miss the larger reality: attackers are not targeting vectors—they are targeting the applications and workflows where PHI (protected health information) is accessed, exchanged, and acted upon. From patient portals and PACS systems (picture archiving and communication system) to FHIR-based integrations (fast healthcare interoperability resources) and partner APIs, applications are the lifeblood of healthcare—and the true target of attackers. ThreatX takes a unified approach, protecting the entire healthcare 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. 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. This ensures customers receive only high-confidence, actionable alerts while streamlining application security operations.





©2026 A10 Networks, Inc. All rights reserved.



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.
- **United**: 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)**: Traditional application security approaches leave healthcare organizations exposed. Coverage is often incomplete and built from multiple best-of-breed tools, driving up costs through add-on pricing, increasing technical debt due to specialized expertise requirements, and overwhelming teams with false positives. Adding a SIEM does not resolve these challenges—alerts still require manual analysis, and protection remains focused on individual the true target: applications and workflows where patient data is accessed. The web application protection platform (WAPP) approach cohesively protects healthcare application ecosystems against both attacks and attackers. This approach helps healthcare organizations reduce HIPAA risk by protecting where PHI is accessed across patient portals, PACS systems, and FHIR-based. This unified approach reduces cost and complexity while improving accuracy by aligning multiple defense vectors around a single goal: protecting patient-critical applications.
- **Adaptive risk scores:** ThreatX uses an adaptive risk score, generated through cross-vector correlation, entity/transaction-based tracking, and battle-tested machine learning, to continuously improve detection accuracy. As an example of cross-vector correlation, early indicators of bot-like behavior can raise an entity's risk score, while subsequent actions like API abuse or L7 DDoS escalate risk more rapidly using accumulated behavioral context. ThreatX provides behavioral API protection across complex ecosystems, including FHIR-based and partner-driven integrations. While agentic AIs may leverage MCPs or chat-completion frameworks, their external interactions are still executed using APIs, meaning ThreatX can assess the behavior of AI systems as they interact with healthcare applications and services.
- **ThreatX SOC team allows for continuous monitoring, tuning, and response:** The ThreatX SOC combines automated protection with expert human oversight to reduce alert fatigue while supporting HIPAA's requirement for reasonable administrative safeguards. Customers benefit from continuous monitoring, policy tuning, and real-time response. For example, during the React2Shell (CVE-2025-55182) vulnerability, the ThreatX SOC identified underlying attack behaviors before public disclosure, enabling protections ahead of widespread exploitation. This proactive approach goes beyond virtual patching to help protect patient data before zero-day threats become 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

- The ThreatX solution 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 your team.

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

Adaptable

- Custom policies and needs can be addressed and implemented

About A10

A10Networks.com

Contact Us

A10Networks.com/contact

©2026 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Logo, A10 Control, A10 Defend, A10 Harmony, Harmony, A10 Thunder, Thunder, ACOS, A10 SSL Insight, SSL Insight, SSLi, vThunder, ThreatX, and ThreatX Protect are trademarks or registered trademarks of A10 Networks, Inc. or its affiliates in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: A10Networks.com/a10trademarks.

Part Number: A10-BR-20124-EN-01 Feb 2026