USE CASE

Prevent Multi-vector, Complex Cyberattacks with a Managed SOC

The Scenario that Modern Organizations are Facing

A global organization faces a persistent onslaught of evolving complex, multi-vector threats: Layer 7 DDoS attacks, zero-day threats, exploitation of APIs, sophisticated credential stuffing attacks, and others. These attacks are often performed in conjunction with one another, using multi-vector, simultaneous approaches that can combine techniques like volumetric application traffic spikes, leveraging the OWASP Top 10 API and app threats, using business logic exploits, account takeovers, and even stealthy attacks that infiltrate, then bide their time for months before executing a wide-scale all-out attack. Standard security teams lack the bandwidth, visibility, and contextual information to differentiate real threats from noise—especially across such diverse environments, such as APIs, multi-cloud environments, hybrid workloads, and geographically distributed infrastructure. Even for advanced security teams, it's like having one person simultaneously play whack-a-mole on 10 different machines.

Ultimately, the goal of this organization's security team is to keep the company secure and proactively find ways to better protect the organization in the future. This helps them elevate the organization's bottom line of maintaining a reputable brand name, maintaining uptime, and continuing to grow the business. The dream scenario is to have productivity and security go hand-in-hand. However, because of the challenges listed above, in-house SOCs are instead on wild goose chases — ill-equipped with deeply insufficient security tools and struggling to distinguish real threats from false positives.

SECURITY SOLUTION

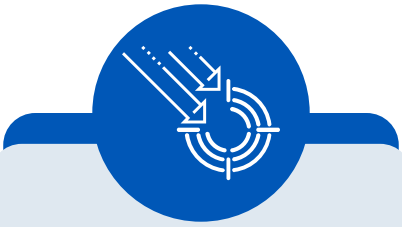
ThreatX, A Web Application Protection Platform

CRITICAL ISSUES

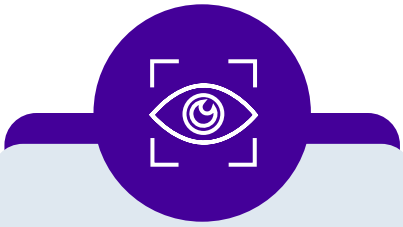
- Multi-vector threats: DDoS, zero-day, API exploits, Top 10 OWASP flaws, and stealthy attacks
- In-house SOCs lack visibility and struggle to prioritize threats amid overwhelming false positives
- Security teams remain reactive, unable to proactively defend against emerging vulnerabilities

THREATX™ by A10 Networks

Key Challenges



Complex multi-vector threats may include simultaneous DDoS, API exploitation, credential stuffing, zero day, and stealthy attacks, using OWASP Top 10 vulnerabilities, business logic abuse, application traffic surges, and long-dwell-time attacks.



In-house SOCs usually lack integrated/ comprehensive visibility and are too hamstrung to quickly prioritize crucial threats in the event of a flood of false positives.

Security teams are stuck in a reactive mode, unable to proactively protect and prepare the organization from future vulnerabilities.

Potential Risks

The risks of such a scenario include:

- **Slow incident response time** due to an understaffed, overwhelmed SOC, leading to a negative impact on revenue and reputation.
- **Increased likelihood of successful attacks**, resulting in loss of customer trust.
- **Alert fatigue and burnout amongst security teams**, leading to higher attrition, and a crippled ability to respond to future incidents, which can lead to decreased team morale and reduced capacity to respond to future incidents

How ThreatX by A10 Networks Secures Your Organization

ThreatX by A10 Networks, a web application protection platform (WAPP), delivers a SOC that manages everything within the ThreatX solution suite—intelligently adapting to your modern application protection needs. For this use case, the focus is the SOC that manages the ThreatX portfolio. The team of security experts acts as a one-stop shop for all of your security needs. With a team of security experts at your disposal, this approach shifts the organization's security posture from one that is reactively fighting fires to proactively erecting an adaptive defense that evolves with the threat landscape without requiring additional overhead or infrastructure from the customer.

Below are some of the processes and technology leveraged by the team of SOC experts to streamline your security.

- **High-severity Alerts Only**: ThreatX uses behavioral learning, correlation analytics, entity/transaction-based tracking, and business logic comprehension to create an adaptive risk score. The SOC can further refine parameters contributing to the risk score. This ensures false positives are accurately filtered out, allowing your internal security team to be notified and brought on to address only the most crucial of threats.
- **Consolidated Application Protection Platform**: Stop application attackers, and protect customers' applications from all types of threats, be it ATOs, OWASP Top 10 API and web app threats, automated attacks, Layer 7 DDoS attacks, and others, by leveraging the adaptive risk score generated by Hacker Mind, ThreatX's decision-making engine.
- **SOC-driven Continuous Monitoring and Threat Response**: A ThreatX analyst team continually monitors traffic and intervenes when necessary—blocking threats, fine-tuning policies, and investigating anomalies in real-time.

Immediate Time-to-Value

By leveraging the ThreatX managed SOC, organizations experience a greatly enhanced understanding of their security posture, without adding any extra workload on the internal security team. They can instead focus on only the most important alerts, and work on improving other aspects of the business. Multi-vector threats that once bypassed rule-based defenses and overwhelmed security teams using outdated security tools can now be identified proactively.

The SOC team from ThreatX will provide:

- Faster threat detection and lower false positives
- Continuous protection
- Outstanding time-to-value
- Provide tuning and policy enhancements, as needed
- Improved customer experience and service uptime
- Detailed logs and reporting for compliance requirements

With the SOC that manages the ThreatX portfolio, your team will be able to rest easy. Let business downtime, security headaches, and brand damage be a thing of the past.

About A10

A10Networks.com

Contact Us

A10Networks.com/contact

Part Number: A10-CS-80254-EN-03 Aug 2025