SOLUTION BRIEF

ThreatX Platform Defense: Unified Protection Without Blind Spots

A Web Application Protection Platform

The Problem with Siloed Defenses

Organizations today face a wide variety of threats–from web attacks and API exploits to bot campaigns and Layer 7 DDoS attacks. Each attack vector seems to require its own specialized defense, but the real challenge isn't just the need for a WAF, API defense, bot defense, and DDoS protection. The real challenge is that attackers don't operate in silos, yet many defenses still do. Some organizations just have point solutions, and don't cover the entire space. Other organizations try to assemble best-of-breed solutions, selecting the top tool in each category. But in both scenarios, defenses are deployed as standalone point solutions, lacking integration and shared intelligence. The result is fragmented defenses, blind spots, and slower responses–gaps attackers quickly exploit. These organizations may respond to this undesired result by relying on a SOC or SIEM to eventually correlate all this siloed information. This is not a true solution either. Overworked security teams are left with alert fatigue and limited visibility, trying to manually stitch together context that should have been unified from the start.

Best-of-breed tools, deployed in isolation, create overlap, inefficiency, and gaps. A SOC/SIEM can orchestrate, but the tools themselves–WAF, API protection, DDoS protection, bot protection–must also communicate and cooperate. Without that, the defense collapses. Even worse, every new security tool adds complexity, cost, and operational headache. Over time, organizations suffer from tool sprawl and technical debt, which wastes resources and expands risk. Meanwhile, attackers are executing coordinated, multi-vector campaigns against a siloed defense that only sees vectors individually. The bottom line is that fragmented security creates fragmented visibility. To stay ahead, organizations need defenses that act as a team — unified, adaptive, and integrated.

Challenge

Attackers don't operate in silos, but defenses still do, creating blind spots, higher costs, and alert fatigue.

Solution

ThreatX by A10 Networks delivers a web application protection platform that holistically, adaptively, and intelligently protects every application within the zone of the ThreatX deployment from every attacker.

Benefits

- Complete visibility across all attack vectors
- Lower cost and complexity via true consolidation
- More agile and precise protection with zero false positives[1]

Consolidated Protection Eliminates Blind Spots

ThreatX is a web application protection platform (WAPP) that safeguards an organization's applications from application attacks and their attackers. By consolidating WAF, bot defense, API protection, and Layer 7 DDoS protection within one solution, powered by its Hacker Mind decision engine. ThreatX enables organizations to:

- Gain a unified defense platform that correlates activity across all attack vectors
- Leverage continuous entity-based and transaction-based tracking for real-time context-enhanced risk score
- Reduce operational costs, tool sprawl, and technical debt by eliminating redundant products and costs

With ThreatX, blind spots are eliminated. Security teams gain full-picture visibility and confidence that multiple attack vectors are covered in a cohesive manner. Unlike siloed tools, ThreatX correlates activity across multiple attack vectors, including WAF, API, bot, and Layer 7 DDoS. The Hacker Mind decision engine adapts in real time. If an entity exhibits suspicious behavior in API traffic, that risk score is carried over when the same entity interacts with the WAF. Adaptive scoring and shared intelligence ensure consistent, precise mitigation across these vectors. The goal is to protect an organization's applications from attacks and attackers across all vectors.

After ThreatX generates refined alerts from its advanced detection method, the SOC that manages ThreatX further polishes the previously validated alerts before sending a near-zero false positive list to customer SOCs. This results in more actionable intelligence, less noise, and faster detection-to-response cycles for the customer. Attackers don't stick to one method. If blocked by DDoS defenses, they may pivot to API exploits. With ThreatX, vectors are evaluated holistically, allowing defense to be provided as one unified platform.

An Organization's Priorities

Agility	Savings	Efficiency	Resilience
Faster mean-time-to-detect/respond and zero false positives[1] allows customer security teams to free up time for higher priorities	**Consolidation lowers licensing, infrastructure, and operational costs**	**Managed SOC for ThreatX reduces workload and bridges the skill gap, allowing the customer SOC to focus on tasks without being overwhelmed**	**Unified defense eliminates blind spots between WAF, bot, API, and DDoS vectors**

[1] ThreatX the product generates a list of alerts, double checks its work, then passes it to ThreatX Managed SOC, where security experts triple check the work. When the finalized list of alerts reaches the customer SOC, this list can achieve zero false positives.

The Impact of ThreatX

Eliminate blind spots and establish comprehensive application defense by bringing WAF, API, bot, and DDoS defense together in a single web protection platform

- Reduce tool sprawl, technical debt, and operational overhead
- Accelerate threat detection and response with correlated insights across all attack vectors
- Enable security teams to spend less time chasing alerts and more time advancing business priorities

Always-on, Unified Defense

ThreatX delivers comprehensive application protection in a single platform. By eliminating siloed defenses, organizations gain stronger protection, faster time-to-value, and fewer false positives, while simplifying operations and lowering cost. ThreatX is the future. It is the first web application protection platform (WAPP) that changes how applications are secured, and how application attackers are stopped. Modern application security with ThreatX is proactive, unified, and resilient. ThreatX helps security teams focus on the most crucial tasks, delivering uninterrupted services, maintaining customer trust, and enabling business growth.

Next Steps

To learn more, visit A10Networks.com or A10Networks.com/solutions/network-security/api-protection.

About A10 Networks

A10 Networks provides security and infrastructure solutions for on-premises, hybrid cloud, and edge-cloud environments. Our 7000+ customers span global large enterprises and communications, cloud and web service providers who must provide business-critical applications and networks that are secure, available, and efficient. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit A10Networks.com and follow us @A10Networks.

About A10

A10Networks.com

Contact Us

A10Networks.com/contact

Part Number: A10-SB-19213-EN-01 October 2025