SOLUTION BRIEF

ThreatX API Defense: On-demand Security for All N-S Requests Toward Your APIs

Real-time API And Web App Protection

The Problem

APIs are crucial for modern business operations, enabling seamless communication between applications, services, and users. Because APIs often have elevated access privileges to back-end systems and sensitive data, they are high-value targets for attackers. As a comparison, if a cross-site scripting attack were run on a social media post, where attackers commented with malicious code, the web page itself would only have so much access to sensitive information and even a successful attack would only be able to negatively impact the business so much. APIs, on the other end, are in the heart of back-end operations. If compromised, data breaches, downtime, loss of customer trust, significant reputational harm, and costly compliance violations would be soon to follow.

Many organizations are actively protecting their own APIs, but do they protect against all inbound requests, and are they able to secure requests going toward known and unknown APIs within their domain? All APIs must be protected. They are listed below:

Known APIs

- These are your documented and managed APIs
- The goal is to secure, monitor, and control these APIs
- We protect a customer's known APIs against requests coming from any entities

Unknown APIs

- These are your shadow or deprecated APIs
- The goal is to discover, track, and control
  - API discovery tools, which we are complementary to, have proactive web crawlers that actively discover and catalogue any unknown APIs. We provide API confirmation, which means we can intelligently catalogue unknown APIs within the domain of the active ThreatX deployment that have been receiving requests
  - We protect a customer's unknown APIs against requests coming from all entities, as long as they are within the domain of the active ThreatX deployment

Challenge

Malicious connections to APIs expose your organization to serious security risks

Solution

Deliver holistic, behavior-based protection for all public API connections and traffic routed through the current ThreatX deployment

Benefits

- Increased API visibility and proactive defense against evolving threats
- Managed SOC expedites threat response and reduces false positives
- Complementary to API gateways and other API discovery tools

Traditional API security focuses on managing known APIs. Forward-looking API security focuses on the proactive discovery of APIs. Our efforts focus on protecting your APIs, known or unknown, from malicious connection attempts, while also enhancing API visibility.

The Solution

The API protection component of ThreatX by A10 Networks allows organizations to secure their in-use, known or unknown, APIs against all sorts of traffic and the entities behind the requests looking to connect with them. ThreatX can also work in tandem with complementary API discovery tools and API gateway tools to further augment API security. ThreatX provides behavior-based protection, continuous risk scoring, and real-time API traffic analysis across sessions, ensuring that APIs are actively being monitored and protected against all sorts of traffic and the entities behind the requests looking to connect with them, as long as the traffic is routed through the current ThreatX deployment.

The ThreatX defense strategy is aligned with the detect, protect, and identify aspects of the NIST cybersecurity framework.

Detect

From a transactional perspective, ThreatX monitors API traffic, and correlates with transaction profiles to detect suspicious patterns and anomalies.

From an entity perspective, ThreatX correlates contextual digital fingerprinting with existing profiles to create a dynamic risk score. This risk score can quickly adapt in real-time to modifications and obfuscations of attacks.

Protect

ThreatX goes beyond traditional mitigation methods and allows for dynamic mitigation. For example, by leveraging the dynamic risk score, ThreatX can observe changes in behavior depending on which entities have been blocked to understand correlation and intention behind questionable transactions from questionable entities.

Identify

With the ThreatX API cataloguing capability, organizations acquire visibility of their current in-use API environment and security posture, helping identify which assets have potential vulnerabilities most likely to be exploited.

The Impact of ThreatX

- **Widen the visibility of your API security, without adding unnecessary workload**. Discovery of all unknown assets and APIs can be important, but start by identifying requests and entities looking to connect with your in-use, known or unknown, APIs.
- **ThreatX comes with a managed SOC.** This means the ThreatX SOC team will manage the API protection portion of the solution for you, and will reduce the noise. This rise in efficiency greatly reduces the meantime to detect and respond, resulting in outstanding time-to-value.
- **ThreatX entity/transaction-based tracking correlates findings in Hacker Mind**, which is a decision engine that shares knowledge across all ThreatX vectors of protection, resulting in a holistic, and high-performing defense strategy across multiple attack vectors.

Always-on, Proactive API Defense

ThreatX allows organizations to confidently protect their APIs and actively protect against all entities that attempt to connect with their APIs. By greatly lowering false positives, and increasing time-to-value, ThreatX helps security teams focus on the most crucial tasks, delivering uninterrupted services, maintaining customer trust, and enabling unhindered 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-19212-EN-01 June 2025