API Threat Assessment

ThreatX's API Threat Assessment capability analyzes and profiles legitimate, suspicious, and malicious API use to discover and enumerates the API endpoints deployed in the service of ThreatX-protected web sites. While monitoring API interactions in real-time, ThreatX accurately detects real API endpoints and catalogs active tech stacks and markup encodings.

Security administrators and operators will see a new layer of detail—the API endpoints that are actually deployed and exposed in support of their web sites. The risk that those endpoints are subjected to is expressed in actionable terms, precisely where the attacker is aiming.

This brief document gets into a bit more detail about how API Threat Assessment works, and what the future holds for this exciting new ThreatX capability.

How does the ThreatX API Threat Assessment capability detect and profile API endpoints?

The ThreatX next generation web application firewall (NGWAF) sensor sits inline of all HTTP traffic, as a reverse proxy. Because of this architecture ThreatX sees the full content of a site's API requests and responses.

The NGWAF inspects the payload of the HTTP requests to detect and parse any API calls. This information is relayed to the ThreatX back end, where a site-by-site inventory of endpoints is created and maintained, along with usage and attack stats for each endpoint.

How does ThreatX differentiate between legitimate API usage and illegitimate use or malicious attacks?

A common though unsophisticated attack pattern sees attackers "rattling doors" by aiming known exploits at common endpoint names. If not handled correctly, this can produce a falsely inflated inventory of endpoints.

ThreatX API profiling operates at a usage threshold, to prevent erroneous/malicious bot calls and scanners from generating false endpoint detection. ThreatX has to see legitimate traffic fro m a number of different IP addresses in order to flag the target endpoint as a legitimate API.

Does ThreatX profile and protect "private" APIs?

In theory, ThreatX can profile and protect both public-facing and server-to-server private APIs. This requires the deployment of a ThreatX NGWAF between your origin server and your API tier. This will allow the ThreatX sensor to see server-to-server API traffic, and profile those private API endpoints.

In practice this is not a common deployment pattern. ThreatX mostly used on the perimeter, to proxy and safeguard traffic from the Internet to your origin servers and publicly exposed APIs.

What API types does ThreatX profile today?

We profile JSON and XML encoded endpoints today.

What tech stacks will we profile in the future?

In the future we'll extend support to additional use cases, based largely on customer input. Likely candidates for prioritization include JSON over WebSockets, SockJS, and SignalR.

If you're a customer or a prospect, we'd love to hear from you to help us prioritize this list; if there's something in particular that is high priority for your ThreatX deployment, let us know.

Do you detect and profile WebSocket APIs?

Not currently, though JSON over WebSockets is on our roadmap. We protect WebSockets via site-level rules. WebSocket support for API protection has been in the product for several years.

Do you detect and profile SOAP APIs?

We do not at present detect and profile SOAP APIs. We made the decision to deprioritize developing support for this technology stack based on decreasing usage of the SOAP standard. If you're a customer or a prospect and SOAP APIs are a big part of your application portfolio, let us know!

How does ThreatX protect APIs today?

Today, API protection is configured at the Site level, as part of site-level protection. The API endpoints that back a given site are protected by ThreatX WAF, via our rule-based and risk-based blocking.

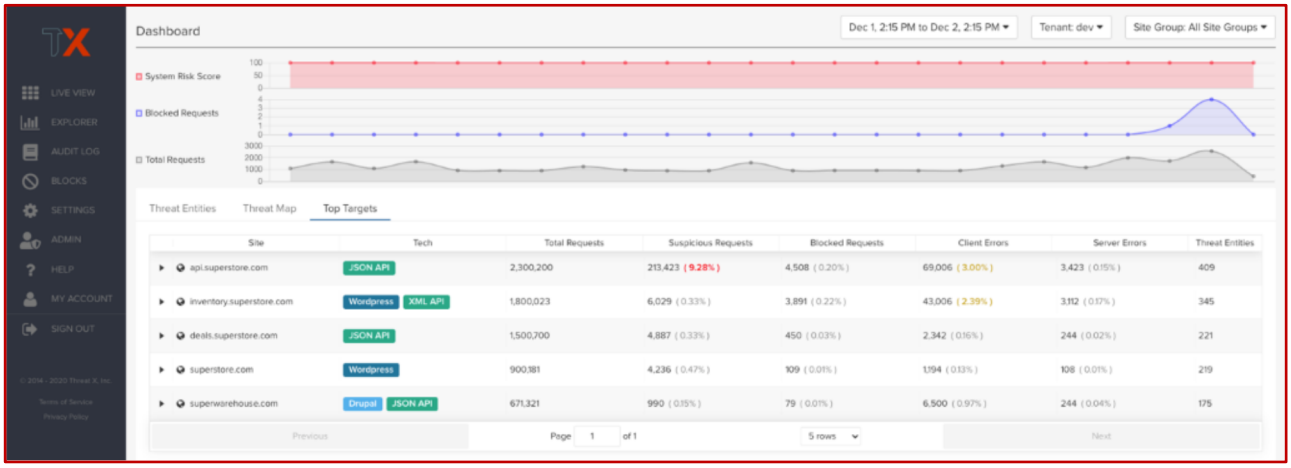
Our reverse proxy architecture supports and protects any and all tech stacks used to build API endpoints, as long as the site FQDN resolves to a ThreatX NGWAF.

End-point specific rules can be crafted today as custom rules, with the help of the ThreatX SOC.

How is the API Endpoint inventory exposed in the ThreatX dashboard?

The first of several API Threat Assessment dashboards is planned for deliver in Q1 of 2021.

This first dashboard provides a high-level overview of site activity, including total requests and suspicious request rates. This view will help users to understand baseline levels of activity, providing context for endpoint-specific drilldowns planned for later releases.



What's planned for the future of ThreatX API Threat Assessment?

ThreatX will continue development of the API Threat Assessment feature, focused in two directions.

First, as mentioned above, we'll expand our supported discovery and profiling tech stacks. This will be prioritized based on customer demand, so if you have a tech stack deployed that would benefit from the insights of our profiling technology, let us know!

Secondly, we'll continue to develop dashboard views, providing endpoint-specific drilldowns into traffic, errors, and attacking entities. This will also expose the ability to select and enable endpoint-specific blocking rules, allowing ThreatX customers to fine-tune protection to the level of individual endpoints.

ABOUT SRC CUBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.