ThreatX Introduces API Threat Assessment Capabilities to Web Application & API Protection Platform

ThreatX Delivers Never-Before-Seen Levels of Visibility and Protection for API Endpoints

DENVER, COLORADO, USA, December 15, 2020 /EINPresswire.com/ -- ThreatX, the leading web application and API protection platform, today announced new API Threat Assessment capabilities. These capabilities deliver unprecedented visibility and enhanced manageability into publicly exposed and vulnerable API endpoints that underly web sites protected by the ThreatX Platform.

> The security use cases we'll build on the foundation of ThreatX's new API Threat Assessment are going to make 2021 a great year for our customers."
>
> *Gene Fay*

ThreatX's API Threat Assessment can analyze and profile legitimate, suspicious, and malicious API use to discover and enumerate the API endpoints as well as the calls they serve. While monitoring API interactions in real-time, ThreatX can accurately detect real API endpoints and determine active tech stacks and markup encodings. Security administrators and operators 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 in the tech stack it manifests.

"API protection must be a core capability of web application firewalls. Enterprises increasingly demand a single solution that protects all web applications and APIs from today's many blended and evolving threats," said Tom Hickman, Chief Product Officer at ThreatX. "Our founders architected the ThreatX platform to deliver reliable API protection. Our new API Threat Assessment is a natural extension of that original vision, not something that we've cobbled-together or bolted on. And like everything in the ThreatX Platform, it's easy to deploy, cheaper to run, and it just works."

ThreatX's API Threat Assessment discovers and profiles API endpoints by assessing the risks

those endpoints face in the wild. This visibility enables ThreatX customers to protect their most important—and therefore, most attacked—assets.

Assess and Manage API Traffic
ThreatX API Threat Assessment enables fine-grained security policy, down to individual calls made to specific endpoints. Risk-based and rule-based blocking, tarpitting, and even business logic tests combine to protect even the most critical and vulnerable aspects of web sites, delivering unprecedented granularity.

"The API endpoints that comprise web sites are inseparable from the sites themselves," said John Grady, senior analyst at ESG. "As a result, APIs have become a popular avenue of attack, both due to their criticality and the fact that many organizations lack the visibility required to properly protect them. Allowing security administrators to see details about exposed endpoints—tech stacks, real-world attack patterns, and attacking entities—opens new possibilities for fine-grained management of the traffic hitting those endpoints."

Gartner predicts brisk adoption of web application and API protection. "By 2023, more than 30% of public-facing web applications and APIs will be protected by cloud web application and API protection (WAAP) services, which combine distributed denial of service (DDoS) protection, bot mitigation, API protection and web application firewalls (WAFs). This is an increase from fewer than 15% today." (1)

“While WAAP adoption is growing rapidly, development teams are relying on API-driven development to increase their pace of delivery. This means more APIs are deployed, exposing more risk, and requiring more and better protection” said Gene Fay, CEO at ThreatX. "OpSec staff can’t protect what they don't know about. ThreatX API Threat Assessment provides that visibility, dropping below the threshold of web sites to expose and quantify risk against individual APIs. The security use cases we’ll build on this foundation are going to make 2021 a great year for our customers.”

About ThreatX
ThreatX is the only SaaS-based NGWAF/Web Application and API Protection (WAAP) solution that helps enterprises secure all web applications and APIs and offers Bot Management and DDOS Mitigation. Purpose-built for the hybrid-cloud, ThreatX delivers complete visibility and comprehensive lifecycle protection by combining progressive behavior profiling, collective threat intelligence with deep analytics with 24/7 AppSec expertise. ThreatX eliminates false positives, false negatives, and maintenance burdens associated with traditional and legacy WAFs. Visit ThreatX.com to learn more. Schedule a ThreatX demo to see how we can protect the web applications and APIs that run your world. Follow ThreatX on Twitter and LinkedIn.

(1) Gartner, “Magic Quadrant for Web Application Firewalls”, Jeremy D'Hoinne, Adam Hils, Rajpreet Kaur, John Watts, 19 October 2020.

Jackie Fredericks
ThreatX
jackie.fredericks@threatx.com
