THREATX

DATA SHEET

API Attack Protection: Fully Managed

Blocking Attackers in Their Tracks

APIs Power Digital Transformation

APIs are the foundation of the Internet today; nearly every modern software application uses – or is – an API. As companies drive digital transformation, APIs enable DevOps teams to quickly deliver new services and capabilities. According to Gartner, by 2023, over 50% of B2B transactions will be performed through real-time APIs.

APIs Under Attack

Gartner believes that APIs will soon be the majority of the attack surface for 90% of web-enabled apps. The rapid proliferation of APIs leapfrogged security's ability to protect these assets. Although many APIs are known and documented, others are spun up without authorization ("rogue") or sit in production long after their useful life expires ("zombie"). Many high-profile security breaches – think Peloton, Venmo, Facebook and the U.S. Postal Service, to name a few – resulted from unprotected APIs.

Key Considerations for API Attack Protection

Securing APIs against sophisticated, multi-vector attacks requires organizations to stop attacks in real-time. Doing so requires deep analysis and correlation of multiple indicators of suspicious activity combined with the ability to respond immediately and appropriately.

It's not enough to collect data from APIs for analysis in a mirrored environment. Observing attack data after the fact is a far cry from API security. It is also not sufficient to rely on basic blocking rules to try to combat complicated, multi-step attacks. To protect APIs, you must be able to affirmatively answer the following ***"Can I?"*** questions:

Can I...

- » Detect complex, multi-vector attacks in real-time?
- » Block attacks in real-time?
- » Gain forensic insight into the attack?
- » Understand my API attack surface?
- » Visualize API attack surface risk?
- » Assess API schema compliance?

SAST, DAST & API Gateways

Organizations with AppSec scanning tools and API Gateways often expect these tools can stop API attacks, but this is not the case.

SAST and DAST scanners are an important part of a security program, but serve primarily to identify known vulnerabilities pre-production.

API Gateways, on the other hand, hold an important role in authenticating API calls and authorizing access, as well as managing the interactions of APIs with various services. API Gateways provide very basic levels of security, such as rules and static signatures capable of blocking only very simple request-level attacks.

While helpful, none of these capabilities will stop sophisticated API attacks.

THREATX API Attack Protection

Fully Managed and Real-Time

ThreatX is the only API Attack Protection platform that delivers on the promise of stopping API attacks in real-time. Through the ThreatX platform, customers can:

- Identify and correlate activity to identify threats to APIs more precisely without triggering false positives
- Respond to multi-step attack patterns over time, adjusting to the motions of an adversary
- Block suspicious entities and IPs when behaviors surpass an acceptable risk threshold
- Dramatically reduce false positives to enable security without risking user experience

Core to ThreatX are both our risk engine and Attacker-Centric Behavioral Analytics capabilities (see figure 1). These technologies deliver AI- and ML-powered capabilities to:

Detect and Block Attacks

ThreatX scans all inbound API traffic in real time, identifying and blocking attacks. This real-time monitoring enables ThreatX to execute advanced threat engagement techniques, such as IP fingerprinting, interrogation, and tar-pitting. These capabilities allow ThreatX to identify and stop the most complex attacks, including large-scale bots and DDoS-level threats.

Enable Advanced Attack Forensics

Through advanced risk analysis, ThreatX can identify key attributes of an attack, such as attack patterns over time (e.g., low and slow); use of advanced evasion techniques; and details of the attack target. This insight enables security to understand the goals and nature of a threat to drive a more comprehensive security strategy.

Discover and Defend APIs

Because ThreatX examines all live traffic, the platform can identify APIs you may be unaware of, such as zombie and rogue APIs. For security professionals without a clear handle on their organization's API attack surface, these capabilities fill a critical gap in the security program.

Visualize API Attack Surface

In addition, the API discovery capabilities of ThreatX allow customers to visualize the entirety of the API attack surface. ThreatX's API attack dashboard provides a central view of how and where APIs may be deployed – beyond those known to the organization.

Enforce API Schema Compliance

ThreatX supports customers' efforts to address API schema compliance, ensuring API functionality is aligned with the organization's stated goals and objectives. With our OpenAPI schema support functionality, you can compare what your build system thinks is out there with what's truly in the wild, allowing organizations to quickly pinpoint undefined or unspecified functionality.

In addition, because ThreatX offers a fully managed API Attack Protection platform, customers can direct precious security resources toward managing other imperatives.

FIGURE 1

Attacker-Centric Behavioral Analytics

THREATX

APIs are the holy grail for attackers. These adversaries see great value in these assets and exert significant time and creativity to bypass rules-based detection, including both attack types (e.g., DDoS, bots) and evasion techniques.

ThreatX goes far beyond the basic rules by inspecting the specific adversary behaviors over time.

Leveraging an ML- and AI-powered context engine, ThreatX analyzes key attributes (e.g., IP reputation, TOR exit node status, geo IP, user agent, TLS fingerprint) to identify entities and codify risk.

In addition, ThreatX analyzes behaviors from multiple vantage points – rather than requiring a single, significantly risky event or identifying a known signature – to block a suspicious entity.

As risk rises, ThreatX immediately blocks an attack – stopping the threat in its tracks. ThreatX's blocking modes are designed to block malicious requests and deter suspicious entities from attacking your APIs, while allowing benign traffic and real users through.

KEY FEATURES

- AI/ML/Context Engine
- Detect and block real-time attacks
- DDoS protection
- Bot protection
- Multi-mode protection
- Fully managed SaaS platform
- Fully managed policies, attack defense & threat analysis
- Integrated API attack blocking
- API Discovery
- API Gateway integration
- CDN integration
- Integrated app protection
- Require no agents or collectors