THREATX

DATA SHEET

API Threat Protection:

Blocking Attackers in Their Tracks

APIs Power Business Today

APIs are the foundation of the Internet today; nearly every modern software application uses – or is – an API. As companies undergo digital transformation, APIs enable DevOps teams to quickly deliver new services and capabilities. According to Gartner, by 2025, over 75 percent of organizations will directly or indirectly monetize APIs.

APIs Are Under Attack

Gartner believes that by 2024, API abuse and related data breaches will nearly double. The proliferation of APIs leapfrogged security's ability to protect these assets, resulting in many high-profile security breaches such as Peloton, Venmo, Facebook, and the U.S. Postal Service, to name a few. Organizations continue to struggle to track all their APIs, protect all their APIs, and, now more than ever, identify which security vendors can deliver on the promises and capabilities they claim.

Key Considerations for API Threat Protection

Protecting APIs against modern attacks requires organizations to detect and stop a variety of threats. Doing so requires deep analysis and correlation of multiple indicators of suspicious activity, combined with the ability to respond instantly 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. To protect APIs, you must be able to affirmatively answer the following "Can I?" questions:

Can I...

- » Discover all APIs and their endpoints receiving traffic, anywhere?
- » Visualize my API attack surface, including high-risk APIs containing sensitive information?
- » Understand normal API usage vs. API abuse?
- » Detect various types of attack, like recon or automated threats?
- » Track risky behavior before the onset of an attack?
- » Block malicious attempts instantly, without manual intervention?

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.

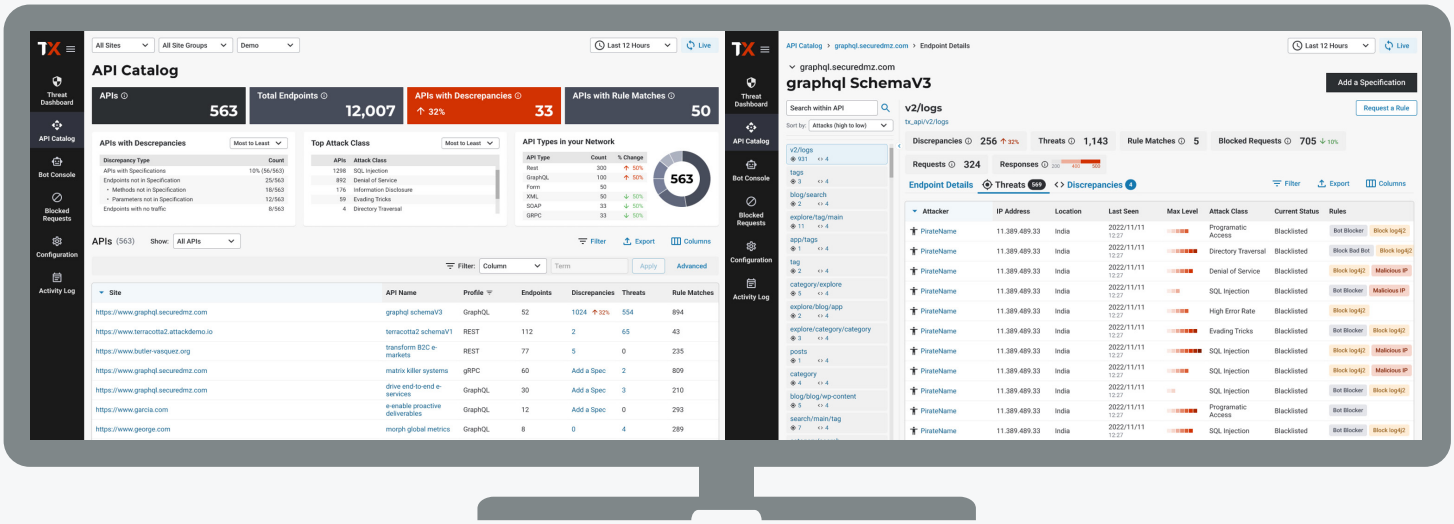
SAST and DAST scanners are an important part of a security program, but serve primarily to identify known vulnerabilities pre-production.

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 Threat Protection

API Monitoring & Threat Investigation



APIs are the holy grail for attackers. They see great value in these assets and exert significant time and creativity to bypass rules-based detection, including combining attack types (e.g., DDoS, bots) and using evasion techniques. Through the ThreatX platform, customers can:

- Discover every active API endpoint and sensitive transaction – with no extra work from you.
- Detect threats and correlate activity no matter what stage of the attack cycle – recon, brute force, or exploitation attempts.
- Track threat behaviors from every angle over time – not just in a single event.
- Block attackers with confidence automatically – based on their risk score.
- Investigate threats with the confidence of knowing that our real-time, risk-based blocking has already thwarted attackers.

Discover & Visualize All Active APIs and Sensitive API Transactions

Because ThreatX examines all live traffic, the platform can discover APIs you may be unaware of, such as zombie and rogue APIs. For security professionals without a clear understanding of their organization's API usage or high-risk transactions, these capabilities provide visibility into your API attack surface to boost the security of high-risk APIs and top attack targets. ThreatX's API catalog provides a comprehensive solution to protect APIs and sensitive API transactions, and investigate the threats targeting them.

Detect & Block Attackers Instantly, Based on Risk

ThreatX is always monitoring, assessing, and blocking attacks – automatically. The platform learns what threats to your APIs and applications look like, tracks attacker behavior over time, and stops them based on their risk level – keeping sites available, your customers protected, and business humming.

Investigate API Threats With Confidence

ThreatX's API catalog provides the visibility needed to quickly identify spikes in risky behavior to help differentiate suspected abuse from normal usage. With the ThreatX API catalog, you can further investigate the threats targeting your APIs and their endpoints without the pressure of having to take action yourself.

To learn more, get a demo of ThreatX API Threat Protection.