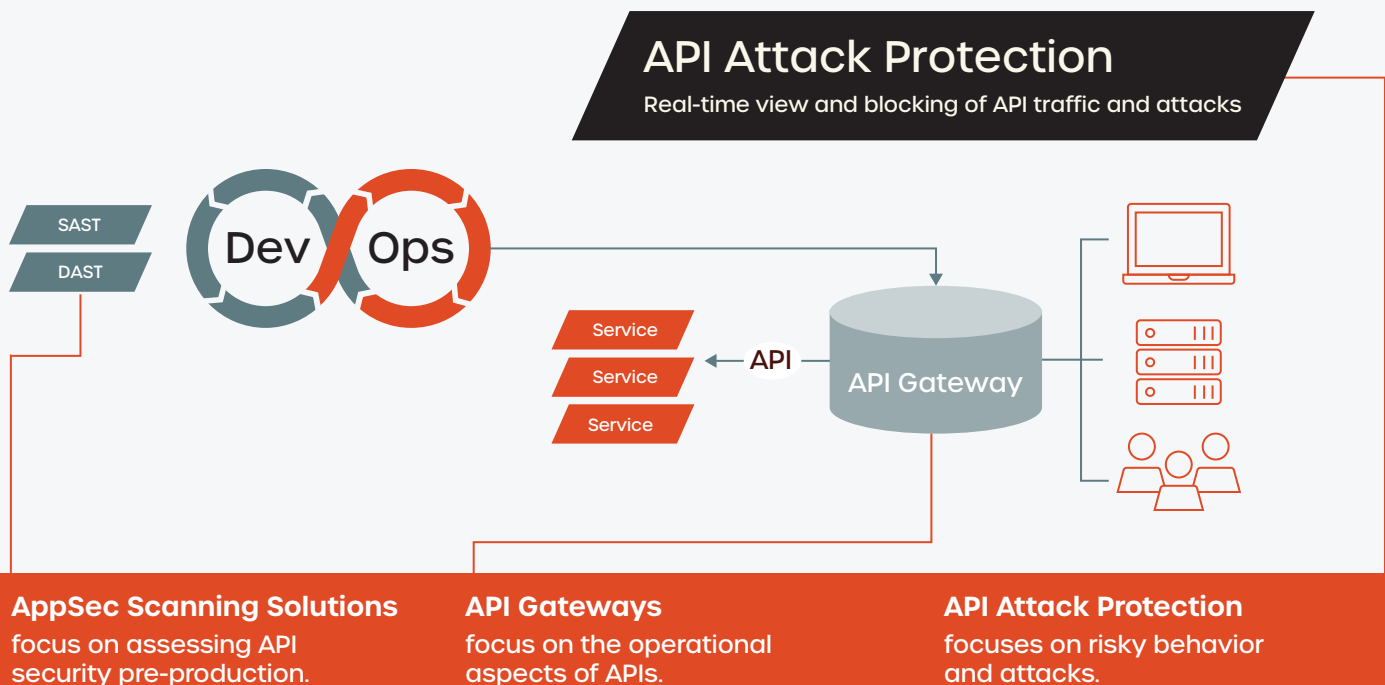# THREATX

API Attack Protection
vs. API Gateways and AppSec Scanning Solutions

API attack protection, API gateways, and AppSec scanning solutions have some complementary capabilities.. However, they also have very different core purposes and perspectives.

API Attack Protection
Real-time view and blocking of API traffic and attacks

AppSec Scanning Solutions
focus on assessing API security pre-production.

API Gateways
focus on the operational aspects of APIs.

API Attack Protection
focuses on risky behavior and attacks.

What AppSec Code Scanning Solutions do:

» Scan for known vulnerabilities in code, such as SQL injection or XSS

» Enable developer remediation of found vulnerabilities

What API Gateways do:

» Authenticate API calls

» Authorize API use access

» Handle translation: For instance, translating a RESTful request to SOAP

» Manage deployment/provisioning

» Scale resources: For instance, if there is a spike of traffic hitting an API

What API Attack Protection does that API Gateways and Scanners do not:

» Detect and block real-time attacks

» Protect against 0Day threats, DDoS, bots, and multi-mode attacks.

» Identify and protect undocumented and unknown APIs (aka zombie and rogue APIs)

» Provide a complete view of the API attack surface

---

www.threatx.com | info@threatx.com