THREATX

Runtime API and Application Protection

ThreatX RAAP

Uniting Persistent Runtime Observability and Scanning with Protection

Vulnerable APIs. Exposed applications. Leaving data at risk – thanks to alert overload, disconnected toolsets, and poorly managed patching.

Enable Development to remediate API and App vulnerabilities – at Runtime

Fueled by digital transformation, application development is moving faster than ever before along with applications transitioning to the cloud. More applications and APIs containing potential vulnerabilities are pushed to production every day – putting user's data and organizations at risk. The flexibility and ease of deploying cloud and containerized environments further makes it easier than ever to add new capabilities but also introduce new vulnerabilities.

Always-Active API Security for DevSecOps

In today's fast-paced world, many DevSecOps teams struggle to manage and prioritize API vulnerabilities. With ThreatX's Always-Active API security capabilities, DevOps and Security teams gain real-time, persistent observability of real API/App ecosystems, traffic data exchanges, threats, and vulnerabilities at runtime. By combining runtime detection and dynamic scanning with protection, ThreatX's RAAP solution detects and remediates vulnerabilities earlier on while protecting vulnerabilities APIs- all within one platform.

Detection and Remediation combined with Protection

You can deploy ThreatX RAAP as a standalone solution for runtime observability and vulnerability remediation or couple it with the ThreatX Edge solution for protection. When used in tandem, these capabilities provide discovery, observability, detection, remediation, and protection for APIs and applications - from the edge to runtime.

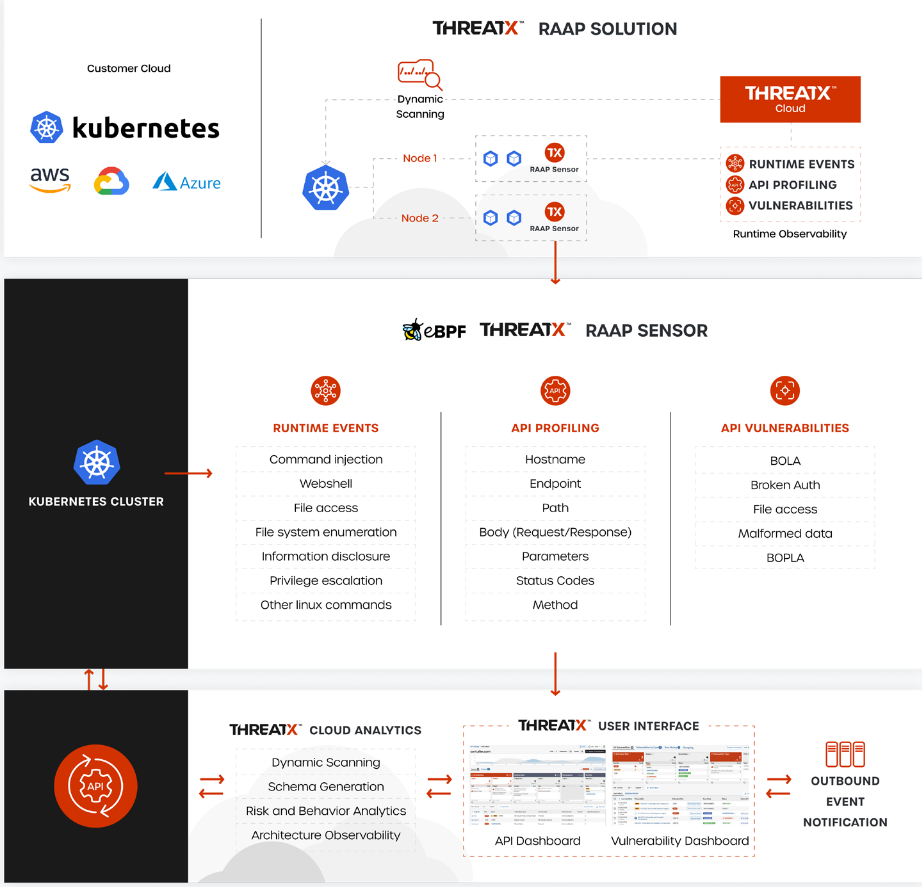
The Rise in Runtime Threats to APIs and Apps

Vulnerable APIs and applications offer a ripe target for attackers. Consider the state of organizations today:

- » 72 percent remain vulnerable to Log4Shell more than a year later (Tenable, November 2022)
- » Only 37 percent have a runtime vulnerability management program (Dynatrace 2022 CISO Report)
- » Only 4 percent have real-time visibility into runtime vulnerabilities in containerized production environments (Dynatrace 2022 CISO Report)

ThreatX RAAP enables you to:

- » Gain observability into API/App ecosystems, system calls, traffic data exchanges, threats, and vulnerabilities
- » Detect threats and vulnerabilities across containerized multi-cloud infrastructures
- » Remediate vulnerabilities earlier on while protecting vulnerable APIs.
- » Empowering Dev to remediate and Security to protect–all within one solution.



Easy deployment through eBPF technology

The ThreatX RAAP solution is deployed as a sidecar container within a Kubernetes environment. With eBPF, ThreatX RAAP inspects all network traffic from one place – without requiring an in-line deployment.

Runtime protection for APIs and applications

ThreatX RAAP secures APIs and applications faster and more effectively than traditional testing solutions. With ThreatX, DevOps and Security teams can easily collaborate through a unified platform. Benefits of ThreatX RAAP include:

» Persistent runtime observability of threats and vulnerabilities coming from the network edge or within cloud workloads.

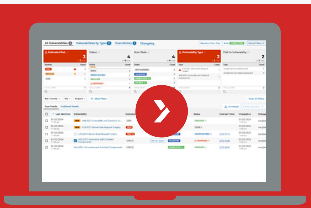
» Detect and remediate vulnerabilities earlier on while protecting vulnerabilities APIs.

» Correlated runtime insights and targeted API test scans for actionable vulnerability remediation.

» Prioritize vulnerabilities on critical systems automatically, ensuring development is focused on high-risk fixes.

» Mitigate vulnerabilities with integrated virtual patching and ticketing systems.

Live Demo



Ready to take a look under the hood?

Take the next step. Request a demo today and see how you can effortlessly protect your APIs and apps against today’s sophisticated threats while reducing the burden on your security team.

THREATX

www.threatx.com | info@threatx.com