THREATX

ThreatX Runtime API and Application Protection

Cloud-Native Solution for Runtime API & Application Protection

Block runtime attacks on APIs and apps with confidence, not complexity

Bringing Real-Time Threat Detection & Blocking to Runtime

Fueled by digital transformation, organizations are transitioning applications and workloads to the cloud. This means security must extend beyond the edge with the ability to detect, track, and block runtime threats.

The cloud offers enormous promise to organizations looking to quickly scale development. The flexibility of the cloud and container environments means it is easy to add new capabilities and services.

At the same time, the use of cloud infrastructure – and, often, multiple cloud providers – creates new sets of risk. Many attackers now prioritize finding backdoors – often by exploiting vulnerabilities in running applications – to circumvent edge and perimeter defenses.

Protecting runtime APIs and applications in real time

With attackers eyeing running APIs and applications, the ability to detect, track, and block attacks – in real time – is an increasing priority. With the patent-pending ThreatX Runtime API & Application Protection (RAAP) capability, CISOs and their teams can bolster runtime security without slowing developers or requiring deep expertise in cloud-native applications. By leveraging ThreatX RAAP, organizations gain comprehensive protection with ThreatX's proven risk-based blocking capabilities at the edge to running applications and APIs.

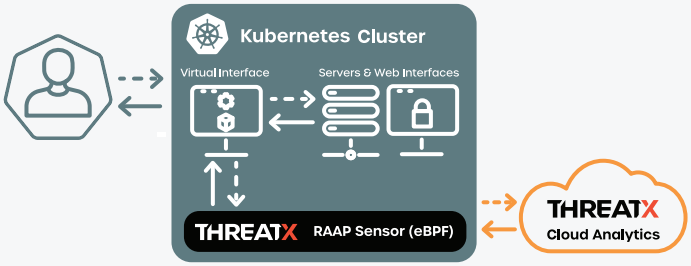
The Rise in Runtime Threats to APIs and Apps

Running APIs and applications offer a ripe target for attackers. While the Log4Shell vulnerability served as a wake-up call, patching these gaps is not easy. 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:

- Detect and track threats across cloud-native and multi-cloud infrastructures
- Extend risk-based blocking to stop runtime threats – in real-time
- Protect against threats beyond the "front door" – e.g., insider threats, malware, malicious rootkits
- Block attacks and insider threats targeting running workloads
- Easily deploy runtime protection for all applications, across Kubernetes environments
- Comprehensively protect APIs and apps against runtime threats coming from the network edge and within cloud workloads



With eBPF, ThreatX RAAP delivers visibility to all network flows, system calls, and processes; the ThreatX runtime sensor supports advanced data collection, profiling, and analytics to identify attacks and take action.

Easy deployment through eBPF technology

The ThreatX RAAP solution is deployed as a sidecar container within a Kubernetes environment. Leveraging extended Berkeley Packet Filter (eBPF) technology, ThreatX RAAP enables deep network flow and system call inspection, process context tracing, and advanced data collection, profiling, and analytics. With eBPF, ThreatX RAAP inspects all network traffic from one place – without requiring an in-line deployment.

Runtime protection for APIs and applications

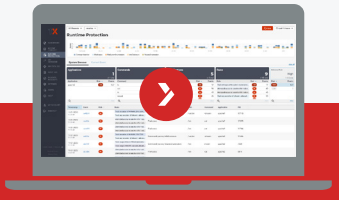
ThreatX RAAP makes protecting running APIs, applications, and their workloads easy. With ThreatX, teams can extend the platform's risk-based blocking to containerized environments -- with confidence, not complexity. Benefits of ThreatX RAAP include:

- Identify threats coming from the network edge or within cloud workloads.
- Investigate high-risk runtime events based on their origin; from the network edge outside and within cloud workloads.
- Detect, track, and block runtime threats to APIs and applications, including insider threats, malware, web shells, remote access software, code injections and modifications, and malicious rootkits.
- Correlate and block threats from the edge to runtime - within one unified view.
- Block high-risk transactions, such as data exfiltration attempts and excessive data exposure.
- Protect transactions within a corporate network (i.e., east-west traffic), including virtual networks and subnets.
- Prevent malware hidden within encrypted data via transparent TLS inspection – without disrupting confidentiality or integration of communications.
- Reduce massive alert fatigue associated with other security tools through ThreatX's risk-based blocking.

You can deploy ThreatX RAAP as a standalone solution to address runtime environments or couple it with the ThreatX API & Application Protection – Edge solution. When used in tandem, these capabilities provide a 360-degree ability to detect, track, and block threats to APIs and applications.

Risk-based, real-time protection – backed by experts who do the worrying for you

ThreatX protects APIs and applications from cyber threats across cloud, on-prem and hybrid environments by delivering precise protection and complete threat visibility. A unique combination of behavior profiling, collective threat intelligence, and deep analytics delivers confident coverage. Our Protection-as-a-Service (PaaS) offering provides on-demand access to security experts 24/7, reducing your costs.



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.