noname

Noname Security eBPF Support

Solution Brief

Background

In recent years, the use of APIs (Application Programming Interface) has skyrocketed, transforming how businesses operate and collaborate in the digital era. Unfortunately, many enterprises' API ecosystems are riddled with vulnerabilities, and IT security teams only discover these issues after a breach. According to research by Enterprise Strategy Group, 92 percent of cybersecurity professionals have experienced at least one API security-related incident in the last 12 months.

To reduce the risk of breaches, comply with regulations, and protect digital assets, enterprises must invest in a defense-in-depth approach with various technologies that can capture API security-related data from application environments. One of the recent developments in this area is API security tools deployed with eBPF, also known as extended Berkeley Packet Filter.

eBPF technology

Extended Berkeley Packet Filter (eBPF) is a technology that enables companies to create programs that leverage Linux operating system capabilities to monitor application environments without requiring elevated privileges, increasing the risk to the host or applications, or needing in-line components. By using this controlled access to the operating system, companies can gain extended visibility into inter-application traffic and gather contextual application data without impacting system performance, security, and stability.

How Noname Security uses eBPF

Noname Security deploys the Noname Sensor - a lightweight eBPF-based component operating at the host level that inspects real-time traffic and passes it through to a Noname Security Platform for analysis.

Highlights

Gain insight

Integrate Noname Security with nearly every environment and gain unprecedented visibility into encrypted and unencrypted inter-application traffic.

Deploy at scale

Deploy eBPF-based sensors across on-premises data centers, virtualized infrastructure, and cloud platforms with near-zero overhead.

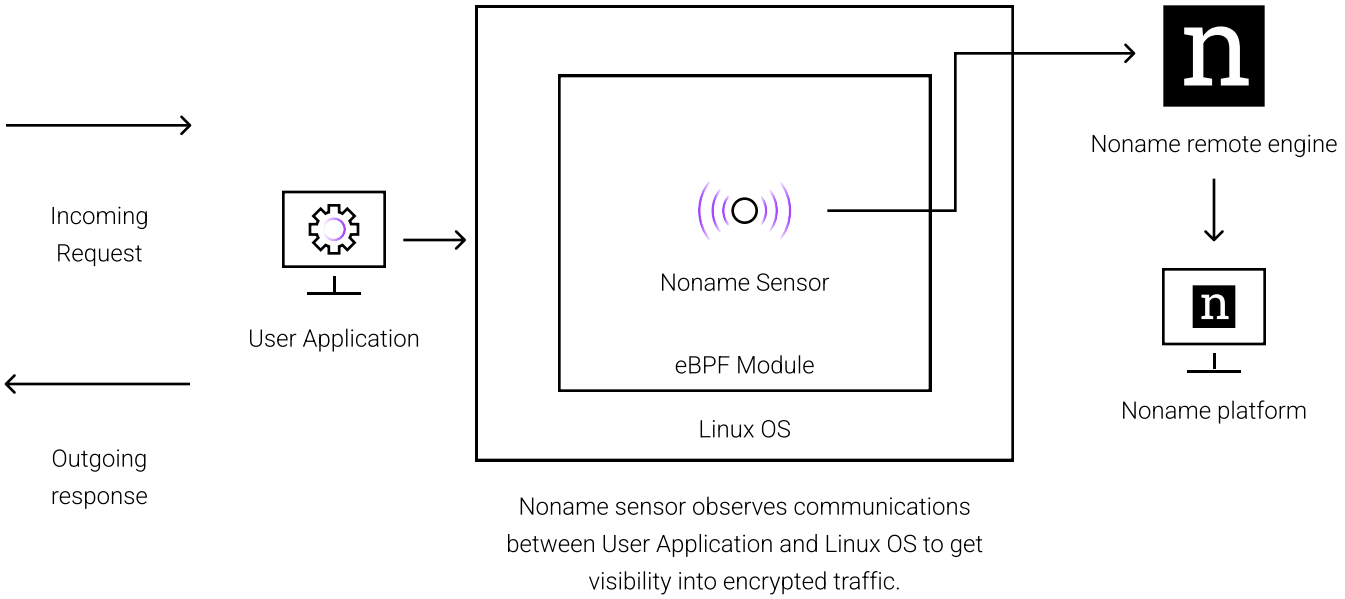
Improve stability

Safely run Noname Sensor in a protected environment within Linux OS without making code changes or incurring maintenance downtime

Enhance security

Implement granular policies for better governance and control over outbound and inbound API transactions.

[1] https://research.esg-global.com/reportaction/515201654/Marketing



Noname sensor observes communications between User Application and Linux OS to get visibility into encrypted traffic.

With Noname Security eBPF-based sensor, you can gain the following benefits:

Deeper visibility

Listen to all the host-level traffic in the application environment, including traffic encrypted with Transportation Layer Security (TLS).

Visualized insights

Generate graph visualization of your K8S cluster-hosted APIs, detect misconfiguration and vulnerabilities in Kubernetes-based APIs, and conduct risk assessments to enhance the security posture of your cluster.

Scalable security

Safely deploy the Noname Sensor in heterogeneous environments without making code changes and eliminate the need for maintenance or patching.

Unimpeded performance

Perform traffic analysis with near-zero overhead even in the most large-scale and complex environments where efficient monitoring of numerous APIs and applications is required.

The Noname Security platform supports eBPF-based sensors and out-of-band API traffic analysis to provide enterprises the flexibility to design API Security programs suitable for the most complex and large-scale environments where efficient monitoring of numerous APIs and applications is required.

About Noname Security

Noname Security is the only company taking a complete, proactive approach to API Security. Noname works with 20% of the Fortune 500 and covers the entire API security scope across four pillars — Discovery, Posture Management, Runtime Security, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Silicon Valley, California, and offices in London.

nonamesecurity.com | info@nonamesecurity.com | +1 (415) 993-7371