noname | accelerated by intel

Intel

Accelerating Sustainable API Security with Intel’s latest innovations.

Noname Security, member of the Intel Network Builders program, has collaborated with Intel to leverage enhancements from 4th Gen Intel Xeon Scalable processors and Intel NetSec Accelerator Reference Design.

Innovation fueled API Security

The latest enhancements available from 4th Gen Intel Xeon Scalable processors, and Intel Advanced Matrix Extensions (AMX) allow us to provide API Security at scale whilst simultaneously lowering the total cost of ownership for our joint customers.

The performance benefits of Intel's latest CPU data center architecture means we can process more API transactions, at lower latency, using a smaller power envelope. 4th Gen Intel Xeon Scalable processors feature the most built-in accelerators of any CPU in the world for key workloads such as Artificial Intelligence (AI), networking, and security. These sustainable data center processors are optimizing power and performance, making optimal use of CPU resources to help achieve customers' sustainability goals.

When compared with prior generations, customers with 4th Gen Intel Xeon Scalable processor can expect a 2.9x average performance per watt efficiency improvement for targeted workloads when utilizing built-in accelerators, up to 70-watt power savings per CPU in optimized power mode with minimal performance loss for select workloads and a 52% to 66% lower total cost of ownership.

By leveraging the 4th Gen Intel Xeon Scalable processors, the Noname Security Machine Learning (ML) engine achieves up to 10x higher real-time inference performance by optimizing for AMX, compared to cloud virtual machines running 3rd Gen Intel Xeon Scalable processors.

Using a variety of different use case benchmarks across Financial Services (PCI data), Healthcare (FHIR HL7 JSON data), and binary (image JPEG data) API processing, we have determined improvements in processing up to 3x faster than previous generations of CPUs with response times in the sub 0.5ms range for the Noname Security Platform.

	3x		10x
Hybrid, Public Cloud	Up to 3x faster	Extremely low latency	Up to 10x faster ML

The Intel NetSec Accelerator Reference Design, a PCIe add-in card which supports processor intensive workloads provides the functionality of a server and is ideally suited for security workloads and AI/ML, the offload can help improve performance, scale, and efficiency in both edge and cloud deployments of the Noname Security Platform.

With the capability to run the Noname Sensor and Noname eBPF based agent on the accelerator card we enable new use cases for performance hungry, edge locations, and extreme low latency environments, including 5G, satellite communications, military, and intelligence community applications.

Edge Computing

SmartNIC offload

Low latency use cases

"Noname uses automated AI and ML-based detection to identify API vulnerabilities, including data leakage, data tampering, data policy violations, suspicious behavior, and API security attacks. Our anomaly detection is used to identify user anomalous behavior that indicates potentially malicious attempts to exploit the organization's APIs. By establishing a baseline of normal traffic, Noname Security's anomaly detection can compare incoming requests to the baseline and determine if it is likely to be conducted by an attacker."

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 — Discovery, Posture Management, Runtime Protection, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Silicon Valley, California, and offices in Tel Aviv and London.

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