

# Noname API Security Platform

Proactively Safeguarding Environments From API Security Vulnerabilities

Intel®  
Network Builders  
PARTNER  
networkbuilders.intel.com



**Solution Overview:** In today's data-driven world application programming interfaces (APIs) play a major role in helping drive seamless communication and integration between multiple services. However, APIs are vulnerable to attacks, data leakage, and denial of service (DDoS) incidents. According to Gartner's predictions, by 2025 more than 50% of data theft will be due to unsecure APIs.<sup>1</sup> To address this, Noname Security takes a proactive approach in helping enterprises efficiently deploy APIs at the speed of their operations while ensuring automatic security measures, vulnerability detection, and a significant reduction in their API attack surface throughout the entire lifecycle. The Noname solution architecture delivers four essential capabilities including proper API discovery, posture management, runtime security, and API security testing that complement existing security tools to ensure robust protection against cyber threats. By utilizing 4th Gen Intel® Xeon® Scalable processors, Intel® NetSec Accelerator Reference Design, and other Intel technologies, Noname can accelerate API response times for low latency use cases and enhance the performance of near-real-time machine learning for runtime API security at the edge of the network.<sup>2</sup>

## Business Outcomes



**Strengthen security and risk mitigation** with features that enable proactive identification and mitigation of security risks, reducing the likelihood of successful API attacks.



**Increase operational efficiency** with simplified deployment and automated security measures that reduce the need for manual intervention.



**Gain comprehensive visibility** of the entire API ecosystem with features to locate and inventory all APIs enabling data-driven decisions and continuous improvements to maximize performance.

## Key Features

- API discovery
- Posture management
- Near real-time runtime protection
- Purpose-built API security testing
- Current infrastructure integration

## Intel Products and Technologies

- [4th Gen Intel® Xeon® Scalable Processor Website](#)
- [Intel® NetSec Accelerator Reference Design Solution Brief](#)
- [Intel® Deep Learning Boost Product Overview](#)
- [Intel® Confidential Computing \(Intel SGX, Intel TDX, Amber\)](#)

## Segment:

Network Security

## Industry:

Enterprise

## Country/Geo:

United States, Canada

## Learn more:

- [Noname Security Website](#)
- [Noname API Security Platform Page](#)
- [Noname Security Platform Brief](#)
- [Noname Security Joins Intel® Network Builders](#)

1. [Gartner API Security and Management Report](#), December 2021 2. [Noname Security Joins Intel® Network Builders Article](#), April 2023

**Legal Disclaimer:** Intel technologies may require enabled hardware, software or service activation. No product or component can be absolutely secure. Your costs and results may vary. Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy. Your costs and results may vary. © Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others. [Intel](#)

**Statement on Product Usage:** Intel is committed to respecting human rights and avoiding complicity in human rights abuses. See Intel's [Global Human Rights Principles](#). Intel's products and software are intended only to be used in applications that do not cause or contribute to a violation of an internationally recognized human right.