Revolutionizing API Security: Noname Security's Comprehensive Approach

Thank you for downloading this Noname Security solution brief. Carahsoft is the master government aggregator and distributor for Noname Security's Cybersecurity solutions available via NASA SEWPV, NASPO ValuePoint, The Quilt, and other contract vehicles.

To learn how to take the next step toward acquiring Noname Security's solutions, please check out the following resources and information:

For additional resources:
carah.io/NonameResources

For upcoming events:
carah.io/NonameEvents

For additional Noname Security News:
carah.io/NonameNews

For additional Cybersecurity solutions:
carah.io/CyberSecuritySolutions

To set up a meeting:
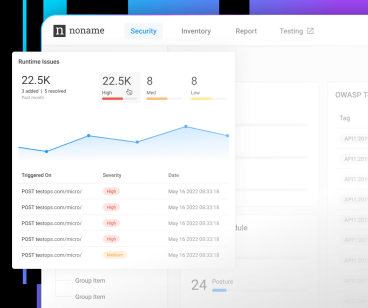PingIdentity@carahsoft.com
703-889-9808

To purchase, check out the contract vehicles available for procurement:
carah.io/NonameContracts

Solution Brief

Noname Security is the only company to deliver API security posture management, provide API detection and response, and secure your API development life cycle.

Noname Security is a cutting-edge solution provider, offering a comprehensive suite of tools and services to fortify the security of your digital ecosystem. In an era where digital transformation is paramount, Noname Security empowers agencies to **safeguard their applications and APIs, ensuring a seamless, secure digital experience for customers while optimizing operational efficiency.**

Digital innovation can be challenging to scale as speed does not equal agility. The nature of today's API landscape makes them very attractive to threat actors.

A Massive New Attack Surface:

API's are everywhere
API's are growing more than 200% per year

API's are changing constantly
28% developers say they deploy APIs into production once a week

API vulnerabilities are easy to exploit
76% of organizations have had an API-related breach in the past year

Existing approaches are not enough as current technologies, and tactics cannot address the API explosion & risk.

"By 2025, less than 50% of enterprise APIs will be managed, as explosive growth in APIs surpasses the capabilities of API management tools"

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 three pillars — Posture Management, Runtime Security, and API Security Testing.

To address API risk, you need complete API security that covers the entire lifecycle of an API. These pillars of API security include the following.

The Pillars of API Security:
Complete API Security Covers the Entire Lifecycle of an API

Discovery	Posture Management
API asset inventory Schema Documentation Data Discovery & Mapping Change & Drift detection Reconnaissance.	Configuration control Vulnerability management Remediation prioritization.
Runtime Protection	**Testing**
Detection and prevention of attackers and suspicious behavior in real time.	Secure APIs in dev to stop vulnerabilities before production.

Noname Security empowers agencies to embrace digital transformation with confidence. By securing APIs, applications, and user identities, while offering automation, visibility, and governance capabilities, Noname Security ensures that your digital initiatives are protected and optimized.