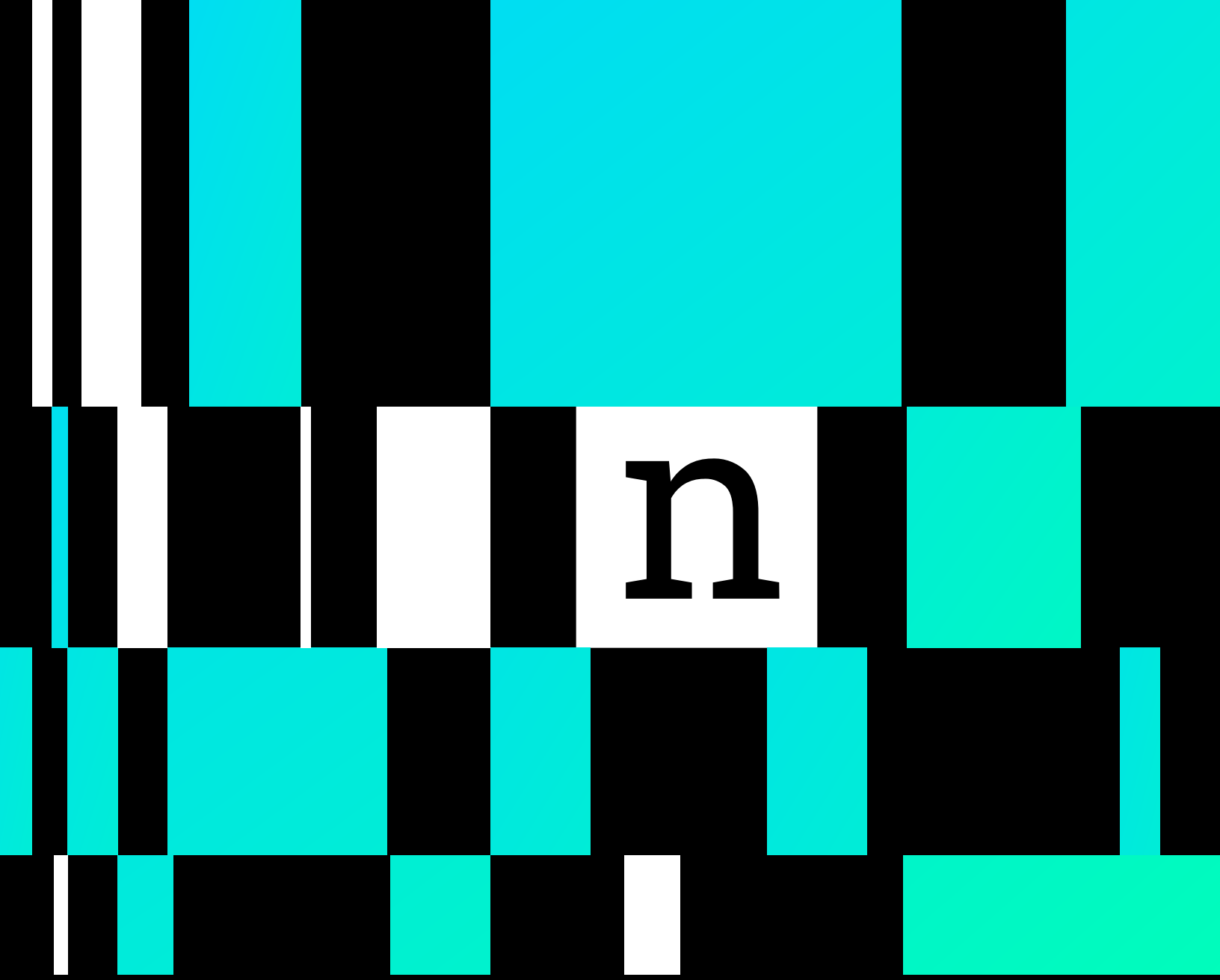


Remote Engine for Discovery & Analysis

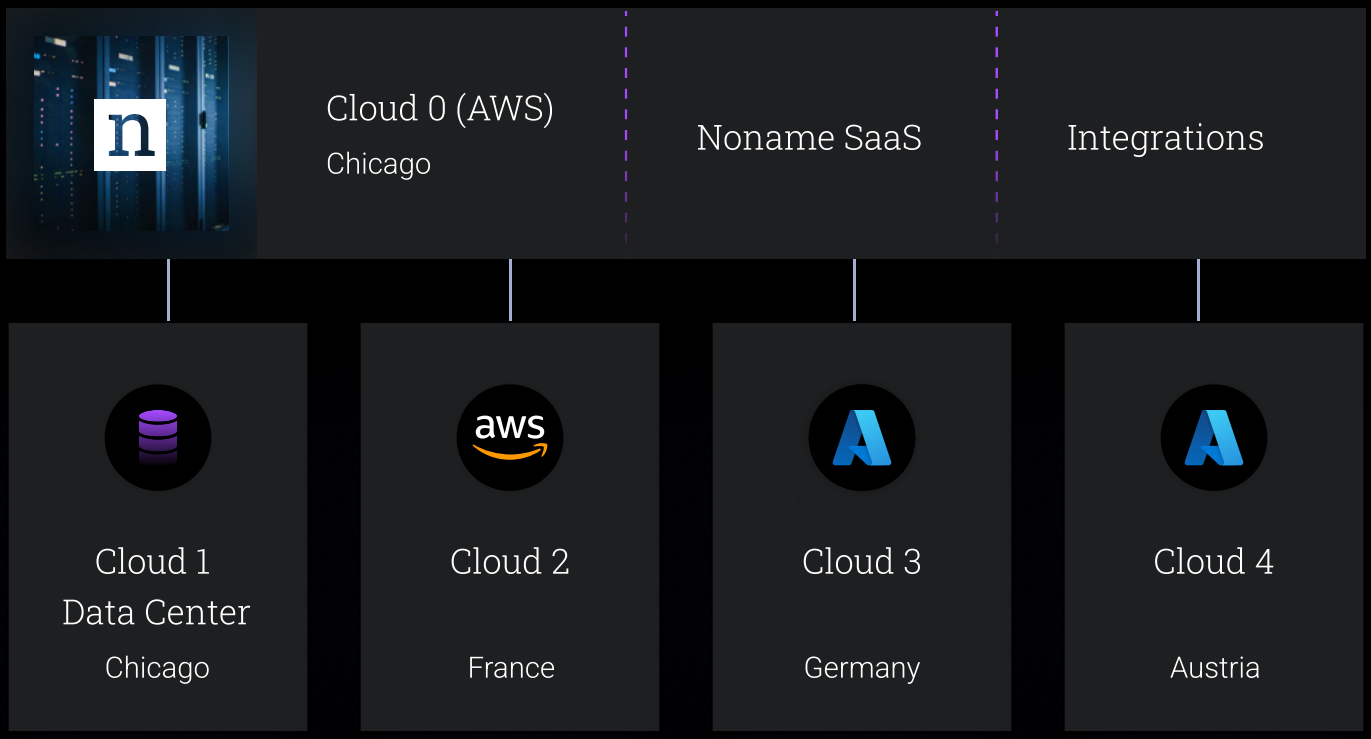
Noname Security is the only company to deliver API security posture management, API detection and response wherever the APIs are located to ensure complete security

Deploy, discover, and secure APIs anywhere

Many organizations have had their digital footprints sprawl across a multitude of cloud and on-prem environments in order to meet operational requirements. These digital footprints depend on APIs in order to interact with intra-organization applications as well as third-party applications and data sources. This scattered framework creates a challenge for identifying and securing API interactions without incurring onerous personnel costs and operational procedures.

The Noname Security API Remote Engine is easily installed and configured on any cloud or on-prem environment to provide localized automated discovery and analysis of APIs. The remote engines are centrally managed by the Noname Security SaaS with just nominal metadata communication.

The Remote Engine provides fast, local discovery and enables your security teams to keep pace with the needs of the organization's strategic objectives.



Scale and accelerate API Security

- Supports a combination of cloud and on-prem environments with management via a single console.

- Real-time discovery and remediation of API risks regardless of the cloud, location(s), or number of APIs.
- Enables compliance with PCI-DSS, PII, data residency and other regulatory requirements with local discovery, analysis and identification of APIs. No critical data identified by Noname Remote Engine ever leaves the perimeter of the cloud or on-prem environment.
- Reduced communication to management platform by 10x to 20x from on-prem and various cloud sites lowers networking costs.
- Automated remediation via integration with ITSM tools to reduce exposure and administrative overhead. Standard Syslog export to any SIEM(s) or SOAR application delivers overall visibility on security threats.

Industry-Leading Approach to API Security

Discover All APIs, Data, and Metadata

Find and inventory every kind of API, including HTTP, RESTful, GraphQL, SOAP, XML-RPC, and gRPC. Discover legacy and rogue APIs not managed by an API gateway, and catalogue API attributes and metadata.

Prevent Attacks, Remediate API Vulnerabilities

Prevent attacks in real-time, fix misconfigurations, automatically update firewall rules, webhook into your WAFs to create new policies against suspicious behavior, and integrate with existing workflows (including ticketing, SIEMs, and SOARs).

Analyze API Behavior and Detect API Threats

Use automated AI-based detection to identify the broadest set of API vulnerabilities, including data leakage, data tampering, misconfigurations, data policy violations, suspicious behavior, and attacks.

Actively Test APIs Before Production

Most applications are tested before they are deployed into production. Most APIs are not. Actively test APIs as part of the software development lifecycle to identify issues before production.

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