SACRA

EQUITY RESEARCH

UPDATED
11/16/2024

Noname Security

TEAM

Jan-Erik Asplund
Co-Founder
jan@sacra.com

Marcelo Ballve
Head of Research
marcelo@sacra.com

DISCLAIMERS

Noname Security

Visit Website

Dashboard for enterprise security teams to discover, monitor, and protect APIs at scale

#b2b #cybersecurity

REVENUE
$40,000,000
2023

VALUATION
$1,000,000,000
2024

GROWTH RATE (Y/Y)
135%
2023

FUNDING
$220,000,000
2024

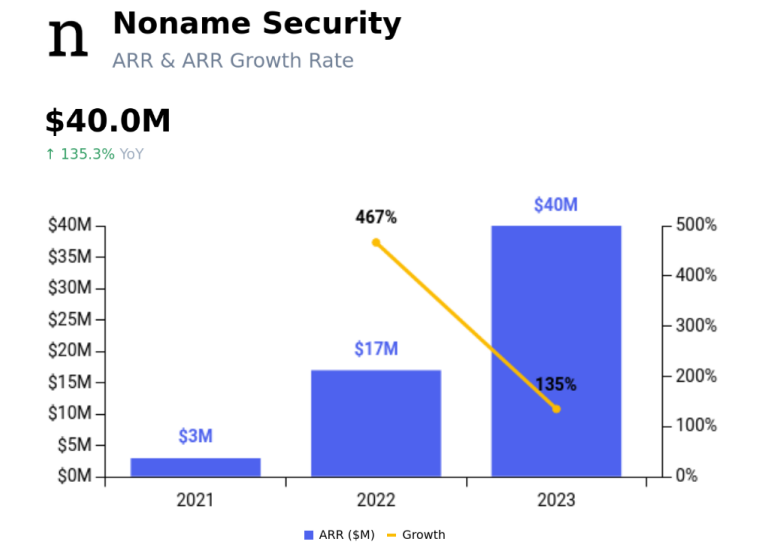
Details

HEADQUARTERS
San Jose, CA

CEO
Oz Golan

SACRA

Revenue



Sacra estimates Noname Security hit $40M in annual recurring revenue (ARR) in 2023, growing rapidly since its emergence from stealth in December 2020. The company has demonstrated exceptional growth velocity in the API security market, with customer and revenue growth exceeding 400% quarter-over-quarter in its first year of operations.

Noname Security primarily generates revenue through enterprise contracts, with approximately 20% of Fortune 500 companies as customers, including two major pharmaceutical firms, one of the largest retailers globally, and a major telecom provider. The company employs a land-and-expand strategy through its Unnamed Partner Program, which includes over 70 value-added resellers, channel partners, and system integrators.

The startup has secured significant funding to fuel its growth, raising $220M across three rounds within just 12 months, achieving a $1B valuation in December 2021. Their platform actively blocks over 1,000 API attacks daily across their customer base, demonstrating strong product-market fit in the enterprise security segment.

Noname competes in the rapidly growing API security market against established players like Palo Alto Networks, though their focus on API-specific security and strong enterprise traction has helped them carve out a significant market position.

Product

Noname Security was founded in 2020 by Oz Golan and Shay Levi, who identified a critical gap in enterprise API security as companies rapidly shifted to cloud-native architectures.

Noname Security found product-market fit as an API security platform for large enterprises, particularly in regulated industries like pharmaceuticals, retail, and telecommunications that needed comprehensive visibility and protection across their growing API ecosystems.

The platform automatically discovers and catalogs all APIs across an organization's environment, including shadow and deprecated APIs that may be invisible to traditional security tools. It continuously monitors these APIs for vulnerabilities, misconfigurations, and potential data exposure risks, providing security teams with real-time visibility into their API attack surface.

When an organization connects Noname to their environment, it creates a complete inventory of APIs and analyzes both API traffic patterns and configurations to detect potential security issues. The platform can identify problems like broken authentication, excessive data exposure, or misconfigured access controls that could lead to data breaches.

The solution integrates with existing security infrastructure to automatically block attacks and remediate vulnerabilities, while also providing API security testing capabilities throughout the development lifecycle to catch issues before they reach production.

Business Model

Noname Security is a subscription SaaS company that provides enterprise API security through a comprehensive platform that discovers, analyzes, remediates, and tests APIs across cloud and on-premises environments. The company monetizes through annual enterprise contracts, with pricing based on the scale of API protection needed.

The platform creates value by automatically discovering and inventorying all APIs within an organization's infrastructure, using AI and machine learning to detect potential threats, misconfigurations, and vulnerabilities. It then integrates with existing security tools to remediate issues and block attacks in real-time, without requiring agent deployment or network modifications.

Noname Security employs a land-and-expand strategy by initially securing critical APIs for specific business units or applications, then expanding coverage across the enterprise as organizations discover more APIs requiring protection. The company drives expansion through its Unnamed Partner Program, which includes over 70 channel partners, VARs, system integrators, and MSSPs who help extend market reach and provide implementation services.

Their competitive advantage stems from their holistic approach that covers the entire API security lifecycle and seamless integration capabilities with existing security infrastructure, allowing enterprises to eliminate API blind spots without disrupting operations.

Competition

Noname Security operates in the API security market, which has seen rapid consolidation as enterprises move more workloads and services to APIs.

Legacy security vendors

Palo Alto Networks and Cisco represent the largest incumbent security vendors, who have acquired API security capabilities through M&A - Palo Alto Networks bought Dig Security while Cisco acquired Lightspin. These companies leverage their existing customer relationships and integrated security platforms to bundle API security features, often offering aggressive pricing to retain customers.

Pure-play API security

Wiz ($396M ARR) and Orca Security ($50M ARR) compete directly in cloud-native application protection, with Orca having sued Wiz for alleged IP theft related to their agentless scanning approach. Both companies emerged from Israel's Unit 8200 intelligence unit and focus on securing cloud infrastructure and APIs without requiring agents. Salt Security, which raised $70M in 2021, specializes specifically in API security.

Infrastructure providers

Cloud providers like AWS, Azure, and Google Cloud offer basic API security features through their API gateway products. While these native tools provide fundamental protections, they typically lack the depth of dedicated API security platforms. Infrastructure monitoring companies like Datadog and New Relic have also added API observability features to their platforms.

The market is trending toward consolidation, with larger platforms acquiring point solutions to build end-to-end security capabilities. This has pushed pure-play vendors like Noname Security ($40M ARR in 2023) to expand horizontally through acquisitions and new product development to compete with full-stack security offerings.

TAM Expansion

Noname Security has tailwinds from the explosive growth in API adoption and increasing API security incidents, with opportunities to expand into adjacent markets like API governance and compliance automation.

API security market expansion

The proliferation of APIs has created an urgent need for comprehensive security solutions. With 80% of internet traffic now flowing through APIs and high-profile breaches at companies like Experian and Peloton highlighting vulnerabilities, Noname's current TAM in API security is expanding rapidly. The company's ability to secure 20% of Fortune 500 companies within its first year demonstrates the scale of enterprise demand.

API governance and management

As organizations struggle with "API sprawl," Noname can expand beyond security into API governance and lifecycle management. This represents a natural evolution from security into helping enterprises catalog, monitor, and optimize their API infrastructure. The company's existing capabilities in API discovery and analysis position it well to capture this adjacent market.

Compliance automation

With growing regulatory focus on API security and data protection, Noname has the opportunity to build automated compliance solutions. Their platform already helps prevent data leakage and tracks API usage patterns - extending this to automate compliance reporting and certification for standards like PSD2, GDPR, and SOC 2 represents a significant growth vector. The compliance automation market for APIs is projected to reach $12B by 2026.

Developer tooling

Noname can expand upstream into the development process by providing API security testing and validation tools for developers. By shifting security left into the development pipeline, they can capture additional revenue from the $25B DevSecOps market while creating a more comprehensive platform that spans the entire API lifecycle.

Risks

Market consolidation pressure: As CISOs look to reduce tool sprawl and reverse the trend of security tool proliferation, there is increasing pressure toward consolidated security platforms. While Noname has started acquiring companies like Gem Security to build a broader platform, larger incumbents like Palo Alto Networks are bundling API security features into their existing platforms and offering aggressive pricing (free for 2 years) to retain customers. This could squeeze Noname's growth as enterprises opt for "good enough" API security from their existing vendors.

Time-limited first-mover advantage: Noname's rapid growth has been driven by being first-to-market with cloud-native API security as enterprises rushed to secure cloud infrastructure during COVID. As the market matures and competitors catch up technically, Noname's ability to maintain its growth rate and justify premium pricing may diminish. The company's high burn rate ($900M raised, 750 employees) assumes continued hypergrowth.

Enterprise sales complexity: Noname's shift toward large enterprise deals creates exposure to lengthy sales cycles and complex procurement processes. While the company has won notable customers like Morgan Stanley and Salesforce, scaling enterprise sales requires building out expensive specialized sales teams and could impact their efficient growth metrics. The "suicide plan" of aggressive hiring and spending may backfire if enterprise sales cycles extend in a tighter spending environment.

DISCLAIMERS

This report is for information purposes only and is not to be used or considered as an offer or the solicitation of an offer to sell or to buy or subscribe for securities or other financial instruments. Nothing in this report constitutes investment, legal, accounting or tax advice or a representation that any investment or strategy is suitable or appropriate to your individual circumstances or otherwise constitutes a personal trade recommendation to you.

This research report has been prepared solely by Sacra and should not be considered a product of any person or entity that makes such report available, if any.

Information and opinions presented in the sections of the report were obtained or derived from sources Sacra believes are reliable, but Sacra makes no representation as to their accuracy or completeness. Past performance should not be taken as an indication or guarantee of future performance, and no representation or warranty, express or implied, is made regarding future performance. Information, opinions and estimates contained in this report reflect a determination at its original date of publication by Sacra and are subject to change without notice.

Sacra accepts no liability for loss arising from the use of the material presented in this report, except that this exclusion of liability does not apply to the extent that liability arises under specific statutes or regulations applicable to Sacra. Sacra may have issued, and may in the future issue, other reports that are inconsistent with, and reach different conclusions from, the information presented in this report. Those reports reflect different assumptions, views and analytical methods of the analysts who prepared them and Sacra is under no obligation to ensure that such other reports are brought to the attention of any recipient of this report.

Published on Nov 16th, 2024