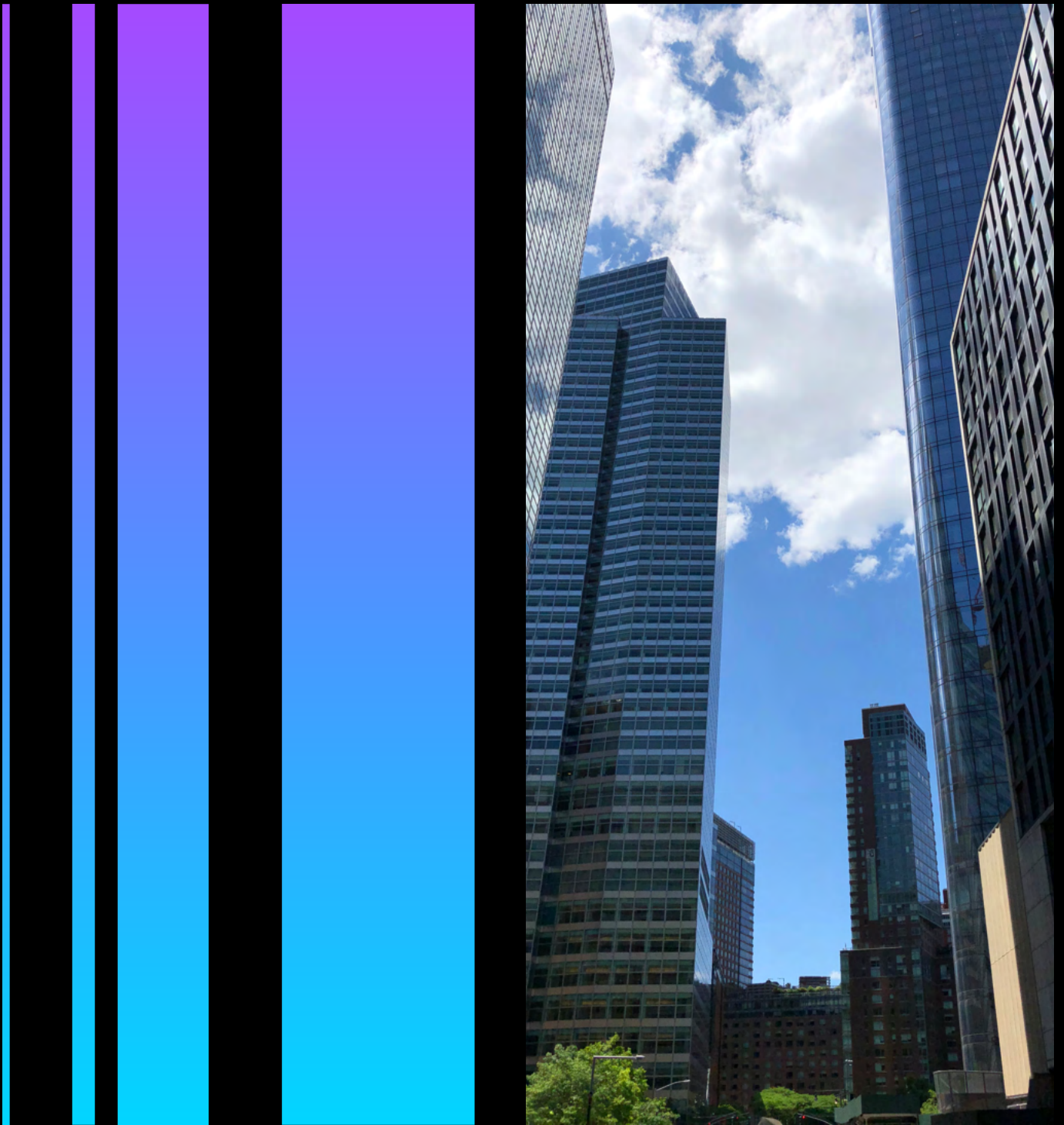


API Security for Financial Services



API Security for Financial Services

Discover how Noname Security helps financial institutions identify and defend against API threats.

The introduction of open APIs has ushered in an era of multi-vendor access that has revolutionized the financial services industry. This has opened the door to new methods of mobile transactions and cross-platform payments. However, despite the myriad of benefits APIs present to the banking industry, APIs also expand the attack surface. And with the number of applications using APIs growing quickly, banks and brokerages alike are facing increasing challenges when it comes to security. Noname Security helps institutions uncover how many APIs they have, the types of data that traverse those APIs, and provides them with the means to protect that data at any given time.

Many in financial services unfortunately look at APIs as a part of traditional application security. The reality is, AppSec and DevOps personnel need to think about APIs separately with their own security considerations. APIs present their own unique risks which legacy tools cannot address. Organizations need to partner with the right API security vendor in order to build a complete governance and security program.

Noname Security helps institutions uncover how many APIs they have, authentication methods, the types of data that traverse those APIs, and provides them with the means to protect that data at any given time. Our API security platform includes asset management, sensitive data analysis, anomaly detection, API security testing in development with CI/CD integration, and manual/automatic remediation with integration into third-party workflows.

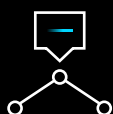
How Noname Security Addresses API Threats

Noname's platform is purpose-built to help financial institutions protect their API estate.



Discover All APIs, Data, and Metadata

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



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.



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 and SIEMs).



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.

