noname

Noname Security for Financial Services

Solution Brief

Open Banking, Financial-grade API (FAPI), and Banking Industry Architecture Network (BIAN) with Noname Security

Driven by the rapid advancements in technology and the evolving regulatory landscape, financial institutions are undergoing significant transformations to adapt and thrive in an ever-changing ecosystem. In order to help address these changes in a secure manner, a number of industry standards are emerging, including Open Banking, FAPI, and BIAN.

These interconnected standards play a crucial role in ensuring the security of tomorrow's financial environments. Open Banking, driven by the European Payment Services Directive (PSD2), mandates banks to share customer financial data with authorized third-party providers (TPPs) through secure APIs. The Financial-grade API (FAPI) framework, developed by the OpenID Foundation, provides a standardized set of security protocols for Open Banking APIs, ensuring robust authentication, authorization, and access control mechanisms. Finally, the Banking Industry Architecture Network (BIAN) complements these efforts by establishing a common reference model and API standards for financial services, promoting consistency and interoperability across the industry.

APIs, when implemented and managed effectively, enable controlled data exchange between trusted entities, reducing the risk of unauthorized access and data breaches. FAPI's emphasis on strong authentication and authorization protocols, such as OAuth 2.0 and JSON Web Tokens (JWTs), further reinforces the security of financial transactions. And by adhering to BIAN standards, financial institutions can ensure that their APIs are compatible with industry-wide security practices, minimizing vulnerabilities and enhancing overall protection.

Highlights

API discovery and inventory

automatically discover and catalog all APIs used to share financial information between financial institutions and third-party providers.

API vulnerability assessment and scanning

scan APIs for vulnerabilities and verify API configuration against FAPI specifications.

API governance and documentation

manage and document APIs to ensure adherence to the BIAN framework and guidelines.

API runtime protection

deploy real-time protection against API attacks, including detecting and blocking malicious traffic, preventing data breaches, and enforcing access control policies.

Noname Security provides a comprehensive API security platform that helps organizations of all sizes address BIAN standards and secure their financial environments.

API discovery and inventory

Noname Security's platform can automatically discover and catalog all APIs within an organization, including legacy, dormant, and shadow APIs. This comprehensive visibility enables organizations to identify and manage all of their APIs and ensure that they are compliant with BIAN standards.

API vulnerability assessment and scanning

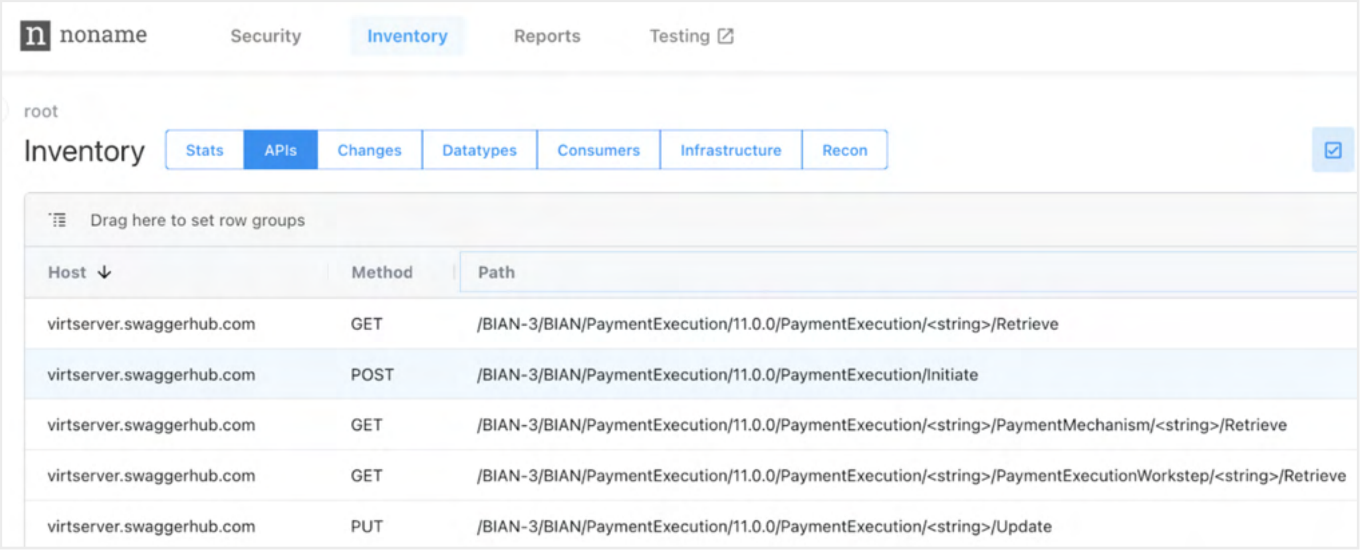
Noname Security's platform can scan APIs for vulnerabilities and misconfigurations. This proactive approach helps organizations identify and remediate potential security issues before they can be exploited.

API governance and documentation

Noname Security's platform can help organizations manage and document their APIs. This includes establishing policies for API usage, creating API documentation, and tracking API changes over time.

API runtime protection

Noname Security's platform provides real-time protection against API attacks. This includes detecting and blocking malicious traffic, preventing data breaches, and enforcing access control policies.



Host ↓	Method	Path
virtserver.swaggerhub.com	GET	/BIAN-3/BIAN/PaymentExecution/11.0.0/PaymentExecution/<string>/Retrieve
virtserver.swaggerhub.com	POST	/BIAN-3/BIAN/PaymentExecution/11.0.0/PaymentExecution/Initiate
virtserver.swaggerhub.com	GET	/BIAN-3/BIAN/PaymentExecution/11.0.0/PaymentExecution/<string>/PaymentMechanism/<string>/Retrieve
virtserver.swaggerhub.com	GET	/BIAN-3/BIAN/PaymentExecution/11.0.0/PaymentExecution/<string>/PaymentExecutionWorkstep/<string>/Retrieve
virtserver.swaggerhub.com	PUT	/BIAN-3/BIAN/PaymentExecution/11.0.0/PaymentExecution/<string>/Update

Noname API discovery of BIAN APIs

Use Cases

Noname Security is a trusted partner to many leading financial institutions around the world. The company's platform secures millions of APIs and has helped organizations prevent countless API attacks and data breaches.

A major financial institution in Europe used Noname Security's platform to discover and inventory over 10,000 APIs. This comprehensive visibility enabled the organization to identify and remediate a number of potential security issues.

A leading payment processor in North America used Noname Security's platform to scan its APIs for vulnerabilities. The platform identified several critical vulnerabilities that could have been exploited to steal customer data. The organization was able to remediate these vulnerabilities before they could be exploited.

A global financial services firm used Noname Security's platform to implement real-time protection against API attacks. The platform has helped the organization block millions of malicious API requests and prevent numerous data breaches.

Noname Security is committed to helping organizations address Open Banking, Financial-grade API, and Banking Industry Architecture Network standards and secure their financial environments with the most comprehensive and advanced API security solution available on the market.

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