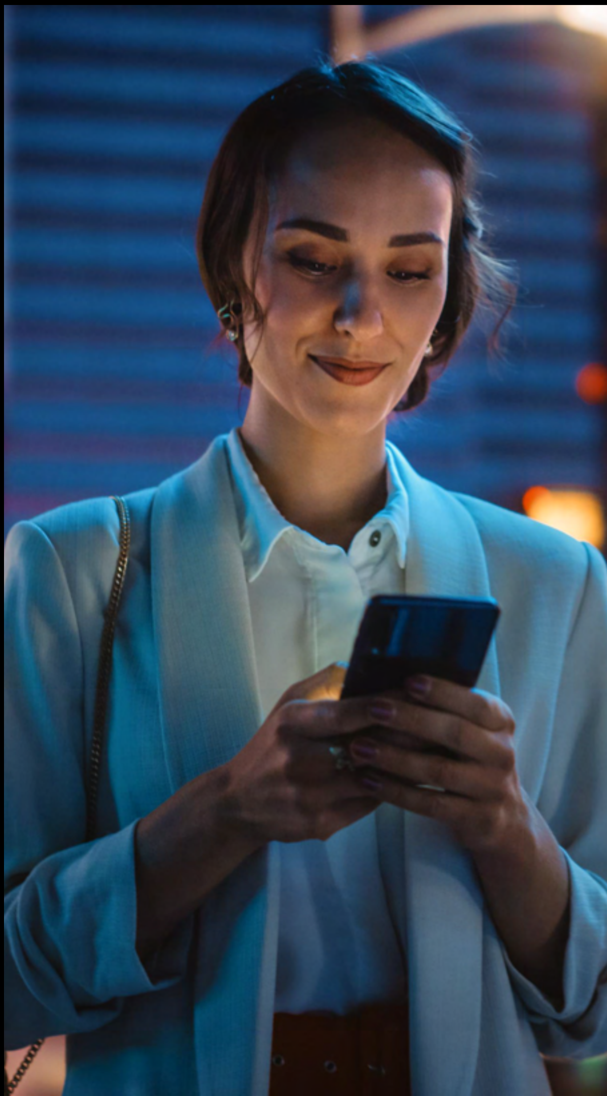
noname

Integrated API Security and Governance for IBM API Connect and DataPower



The Promise and Challenge of APIs

APIs have been the driving force for digital transformation, enabling organizations across every industry to create new services and new business models to accelerate growth.

Although business and engineering leaders have rapidly increased API usage and integration across their organizations, their ability to effectively manage APIs effectively remains a challenge. What's more, APIs present a new and broad attack surface, making them one of the most targeted attack vector by cyber criminals.

To address this challenge, organizations must employ a full-lifecycle approach to both governance and security - including design, development, testing, deployment, operation, and remediation.

Together, Noname Security and IBM enable organizations to quickly develop, deploy, and manage APIs with confidence so they can predictably respond and scale with the business.

Challenges

- ✓ Maintaining an API Inventory across the estate and finding unknown APIs
- ✓ Identifying non-compliant, misconfigured, or vulnerable APIs
- ✓ Detecting and stopping API abuse or misuse, including attacks
- ✓ Building secure and consistent APIs without sacrificing speed or agility
- ✓ Establishing alignment and oversight of API security and governance programs

How Noname Can Help IBM Customers

Discover Your API Estate

You can't protect what you can't see. With Noname Security's Advanced API security, you can automatically discover APIs, domains, and issues to build a robust API inventory that offers visibility into your entire API estate — on average, our customers find 40% more APIs and gain 100% visibility. You can also easily find exploitable intelligence, such as leaked information, to understand the attack paths available to adversaries and enjoy seamless integration with the most common infrastructure elements adjacent to your API Gateways and Management platforms to ensure consistent sharing of security data across the organization

Strengthen Your Security and Governance Posture

Scale your operations and enforce best practices when using Noname's Advanced API Security Platform for API governance — understand every API in your ecosystem with full business context and align with API management best practices. You can streamline communications between development and security teams, uncover misconfigurations and out-of-policy APIs, find vulnerabilities., but you can uncover misconfigurations, out-of-policy APIs, find vulnerabilities, protect sensitive data, and proactively monitor changes to reduce risk in your APIs.

Stop API Abuse and Attacks with Runtime Protection

Detect and block API attacks from edge to core – including data leakage, data tampering, data policy violations, suspicious behavior, and more – with real-time traffic analysis, out-of-band monitoring, inline remediation options, and workflow integrations to increase Security Operations Center (SOC) effectiveness.

Deliver Secure APIs Faster with Active Testing

Seamlessly integrate API security testing into every phase of API development and uncover vulnerabilities, misconfigurations, and compliance problems before APIs are promoted to production. With Active Testing, DevSecOps personnel can execute a comprehensive suite of 150+ API-focused security tests on-demand or as part of the company's CI/CD processes. Active Testing leaves no API untested with a unique ability to find and test every API based on an understanding of the application's underlying business logic, which allows developers to uncover complex vulnerabilities other testing tools could miss.

Specific Noname Capabilities for IBM Users

Advanced Integration with IBM Ecosystem

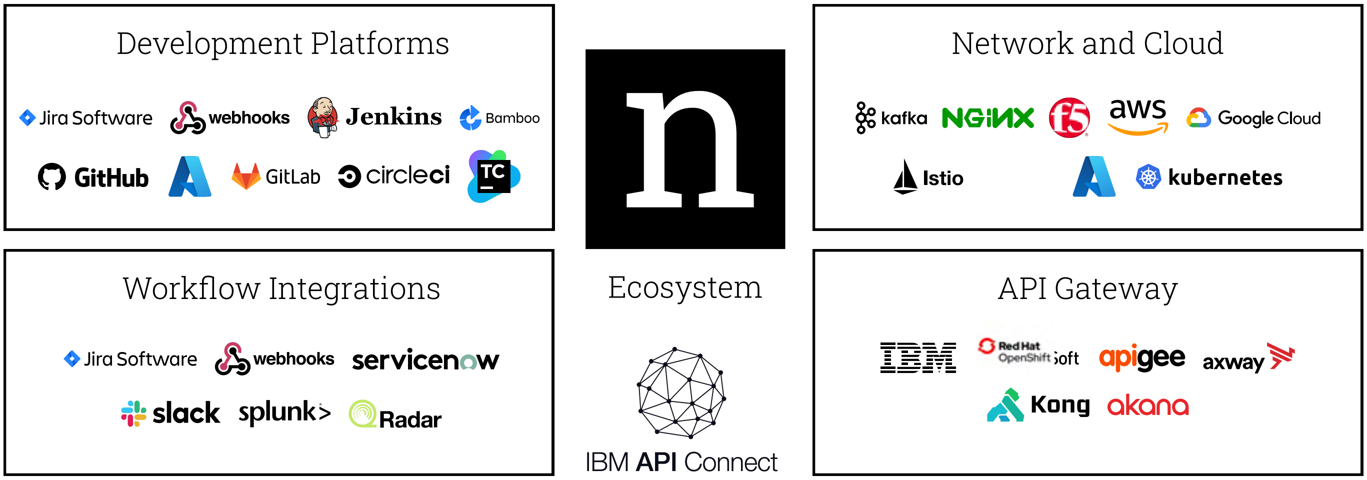
Noname Security integrates with both API Connect and DataPower across multiple cloud platforms and deployment options. Additionally, when API Connect manages DataPower, unilateral configuration changes are made across systems, driving increased operational efficiency while reducing issues like rogue pipelines or contractors.

Analytics Offload directly to the Noname Security Platform

IBM DataPower customers can experience near real-time threat detection and blocking with no performance and latency impact without the need to install any additional plugins on DataPower gateways by integrating with the Noname Security platform.

Seamless policy management for IBM DataPower

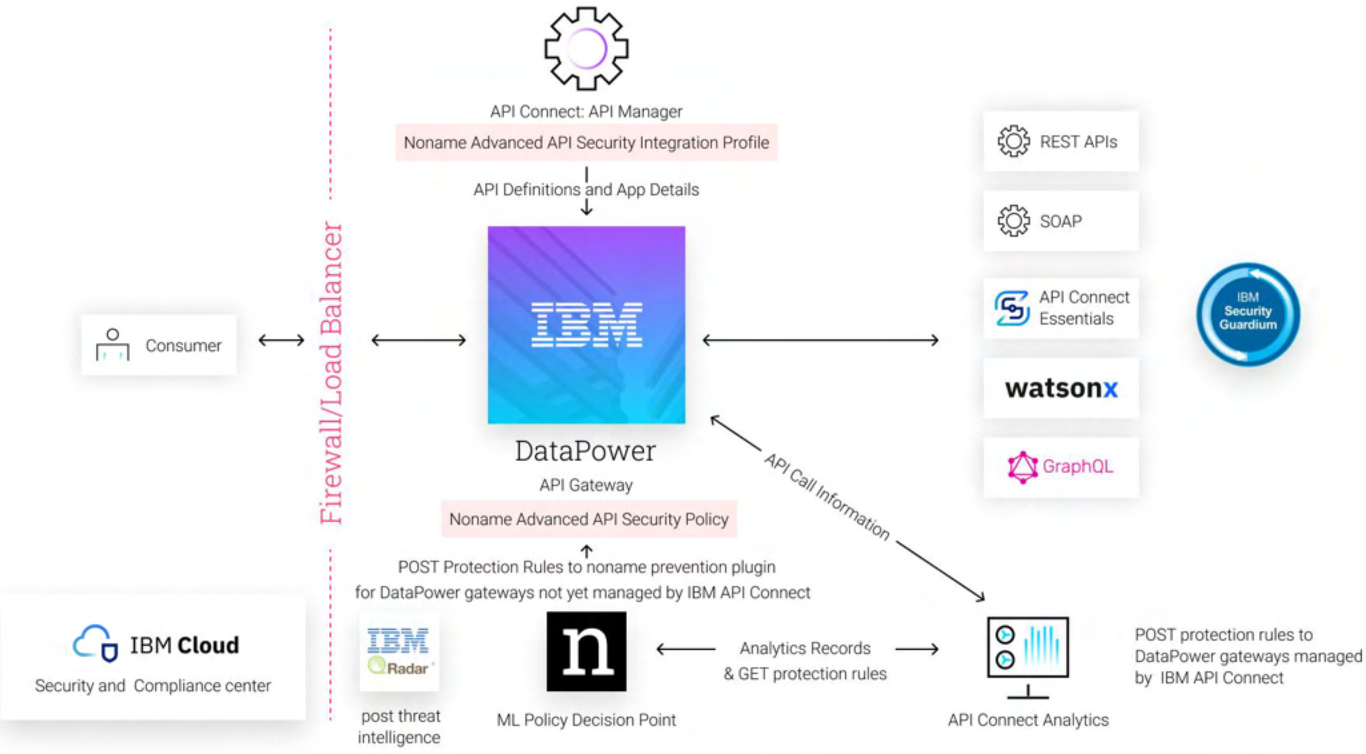
IBM API Connect can evaluate access requests to resources against Noname Security authorization policies and enforce blocking rules across IBM DataPower clusters, reducing remediation times from days to minutes or seconds.

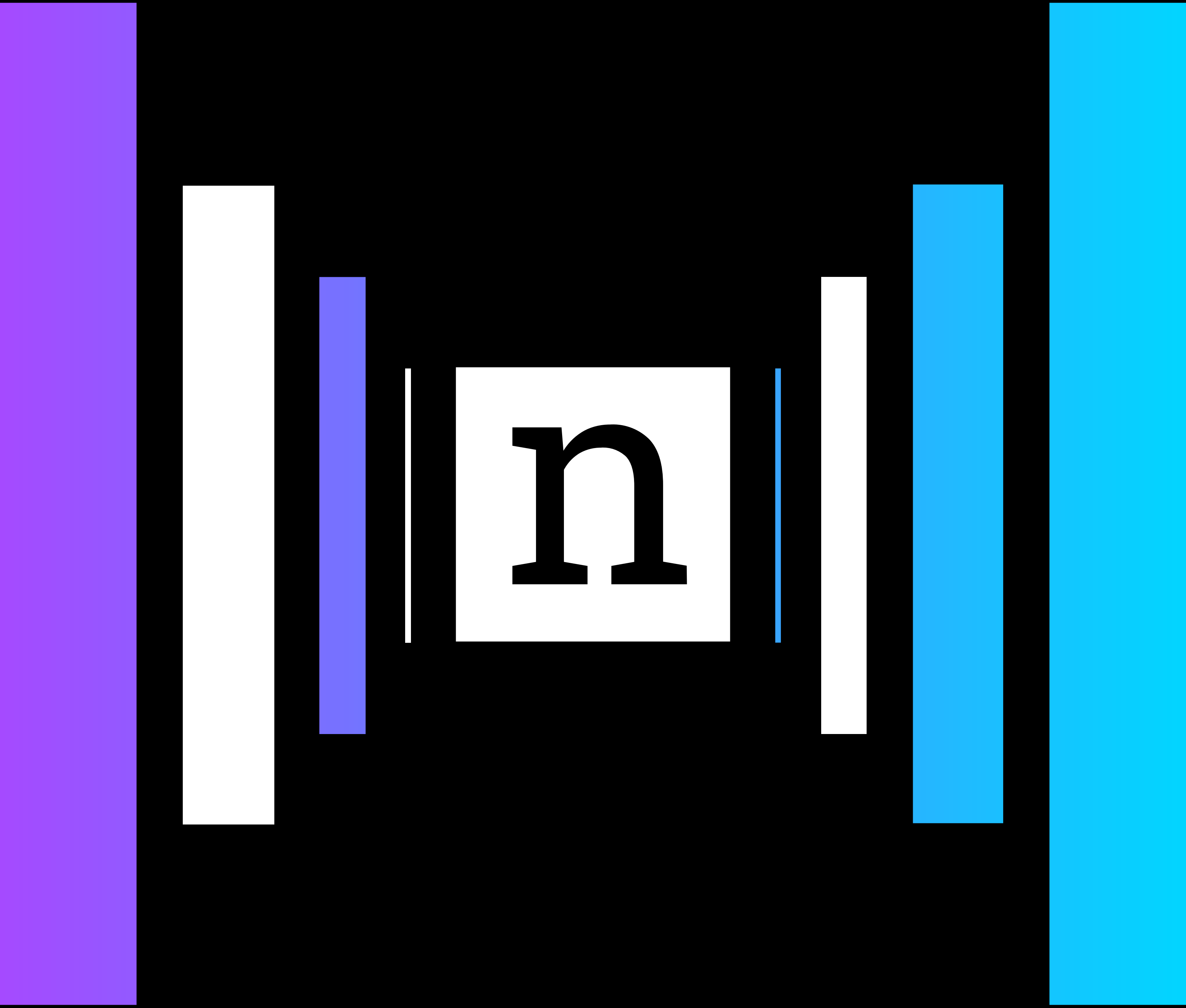


Integration Benefits

Ripping-and-replacing can be costly and time-consuming. With Noname Security, IBM customers can enjoy a robust suite of development, workflow, API Gateway, and cloud and network integrations to augment their existing tech stack and get more return on investment.

In addition to a mature integration with IBM API Connect and DataPower, IBM customers can leverage the Noname eBPF Red Hat OpenShift integration to discover APIs that are not yet managed by API Connect or proxied by Datapower, enabling them to find and protect APIs processing high-risk transactions and confidential data. These capabilities extend beyond on-premises to cloud and hybrid configurations, supporting Amazon Web Services (AWS), Microsoft Azure, and the Google Cloud Platform (GCP).





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