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 scale and manage APIs effectively remains a challenge. What’s more, APIs present a new and broad attack surface, making them the most targeted attack vector by cyber criminals.

In order 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 and deploy 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 resources
- Establishing alignment and oversight of API security and governance programs
Solution Brief

How Noname Can Help IBM Customers

Discover Your API Estate

Automatically discover APIs, domains, and issues. Build a robust API inventory and easily find exploitable intelligence, such as leaked information, to understand the attack paths available to adversaries. Integrate easily with the most common infrastructure elements adjacent to your API Gateways and Management platforms.

Strengthen Your Security and Governance Posture

Understand every API in your organization’s ecosystem with full business context and enforce corporate standards and policies. Uncover misconfigurations, out-of-policy APIs, find vulnerabilities, protect sensitive data, and proactively monitor changes to de-risk 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 SOC effectiveness.

Deliver Secure and consistent APIs Faster with Active Testing

Add security to your CI/CD pipeline. Ensure adherence to standards, remediate vulnerabilities and deploy more secure APIs faster with Noname’s purpose-built API security testing solution.
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 changes and configuration drift are avoided by rogue build pipelines, contractors, and maintenance updates.

### Analytics Offload directly to the Noname Security Platform
Leveraging Noname, IBM DataPower customers can enable near-real-time threat detection and blocking without experiencing performance or latency impacts – without the need to install any plugins on DataPower gateways.

### IBM API Connect management of Noname Policies for DataPower
The policy decision point (PDP) policies of the Noname Platform can be managed by API Connect. This solves the problem of distributing blocking rules to global clusters of IBM DataPower acting as edge policy enforcement points (PEP) - reducing remediation time from days to minutes or seconds.
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.