Advanced API Security with IBM and Noname Security

Eileen Lowry

VP, Product Management,
IBM Integration

Shay Levi

Co-Founder and CTO,
Noname Security

APIs are a key enabler of digital transformation & integration

Full lifecycle API management is critical to ensuring a flexible, scalable and secure architecture.

API-led integration provides a modern way to integrate applications and data through the most common and re-usable building blocks of today

Reduce cost by leading with APIs as the building blocks of integration
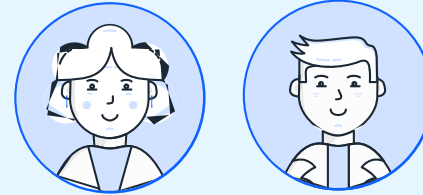
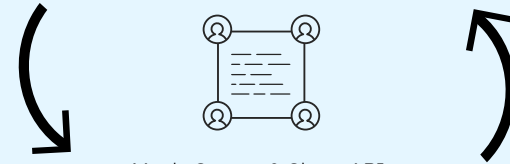Quickly adapt to changing business needs by leveraging OpenAPI standards

Manage, secure, & share your APIs more efficiently & effectively

Business & IT Integrators

Design, Implement, Deploy APIs & Flows

Mock, Secure & Share APIs

API Developers

API Management

IBM API Connect powers
digital applications by unlocking
business data and assets as APIs

Create

Automatically create APIs to expose data,
microservices, enterprise applications,
and SaaS services using open standards

Manage

Rapidly organize, publish and analyze any API
through the full lifecycle from design to retire

Secure

Easily apply built-in and extensible policies
to secure, control and mediate the delivery
of APIs protecting data and business assets

Socialize

Empower application developers to explore and
consume your APIs using branded self-service portals
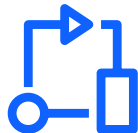
Gateway

IBM DataPower Gateway is an industry leading, high security gateway for modern, traditional and hybrid cloud workloads

Secure
Easily apply built-in and extensible policies to secure access to a full range of API, Mobile, Web, SOA, B2B, and Cloud workloads at all stages.

Integrate
Combine modern event-based and API workloads with traditional services with advanced protocol bridging and message transformation support.
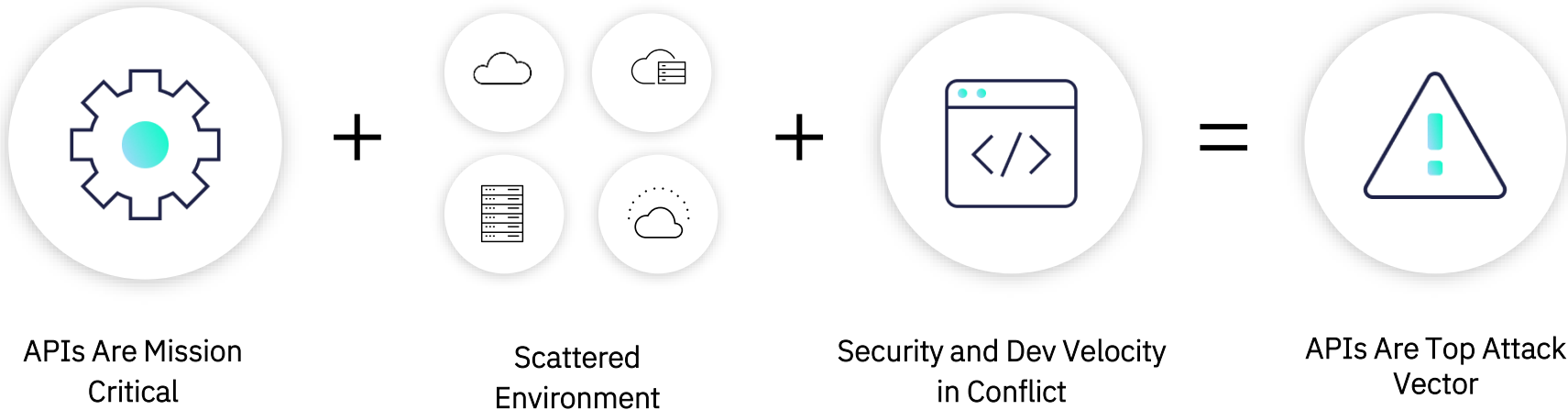
Control
Protect applications from over utilization with traffic control and quota enforcements.

Optimize
Improve response times and throughput by controlling message traffic with application caching and advanced routing.

With increased importance to digital strategies, APIs have become a top attack vector

APIs Are Mission Critical

+

Scattered Environment

+

Security and Dev Velocity in Conflict

=

APIs Are Top Attack Vector

Announcement: IBM and Noname Security are partnering to provide the most secure and intelligent API management solution

IBM

API Connect

DataPower

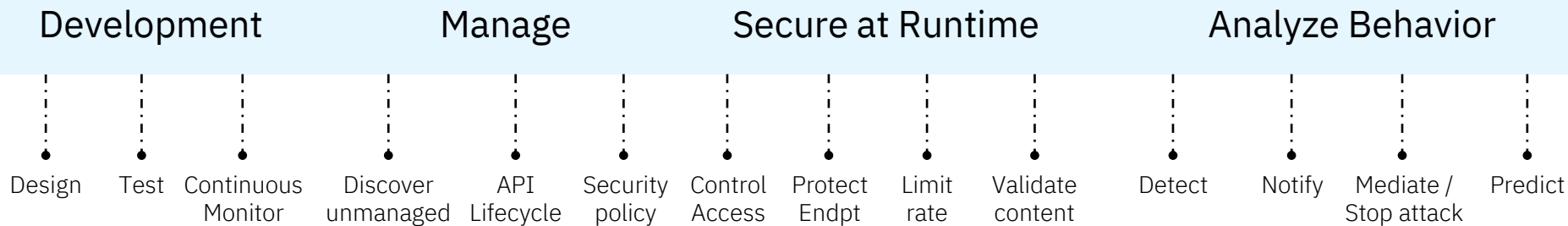✓ Market-leading API Management
✓ Enterprise-grade API runtime protection

Noname Security

Discovery

Posture Management

Behavioral Threat Detection

✓ Analyze, Detect, Notify & Remediate Threats with AI
✓ Discover the unmanage – APIs across your landscape
✓ Inventory & report API security posture

This partnership will expand our security capabilities to cover the entire API lifecycle

Development   **Manage**   **Secure at Runtime**   **Analyze Behavior**

Design   Test   Continuous   Discover   API   Security   Control   Protect   Limit   Validate   Detect   Notify   Mediate /   Predict
                  Monitor   unmanaged   Lifecycle   policy   Access   Endpt   rate   content   Stop attack

The Company

2020	**$220M**	**250+**
Founded	Raised	Employees

Category Leader

- Largest and fastest-growing API security company

- $220+ million in funding from leading investors

- Award-winning comprehensive platform, from code to run-time

Global Presence

- 250+ employees

- NA, EMEA, APJ & IL locations

- Follow-the-sun 24-7 support

- SOC2, STAR Level 1, PCI DSS Compliant

Strong Partner Ecosystem

- Alliances with all major cloud providers and key API platforms

- Global GTM partnerships

- 75+ certified integrations with network security, CI/CD tools, SEIM, and workflow platforms

Impressive Customers

- Working with over 20% of Fortune 500

- 3 of 5 largest US telcos

- 2 of 5 largest pharmaceuticals

- Major global financial, insurance, consumer & entertainment leaders

Best in API Security   Fastest Growing   Microsoft Preferred Solution

With increased importance to digital strategies, APIs have become a top attack vector
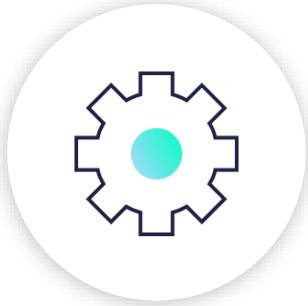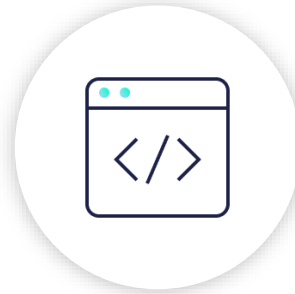
APIs Are Mission Critical + **Scattered Environment** + **Security and Dev Velocity in Conflict** = **APIs Are Top Attack Vector**

Why API security is critical

> ## Concerns Over API Security Grow as Attacks Increase
>
> Some 66% of organizations say they have slowed deploying an app into production because of API Security concerns.

> ## By 2022, API abuses will become the most-frequent attack vector.
>
> **Gartner**
>
> Gartner, API Security: What You Need to Do to Protect Your APIs, 28 August

25,592 APIs

The Avg # of APIs in companies with over 10k employees was over 25,000 APIs

81% incident rate

81% of CISOs reported an API security incident in the last 12 months

35% projects delayed

Survey respondents who said projects were specifically delayed due to API security concerns

87% want Shift Left

Security leaders believe effective API security testing in dev pipelines can solve most delays and breaches
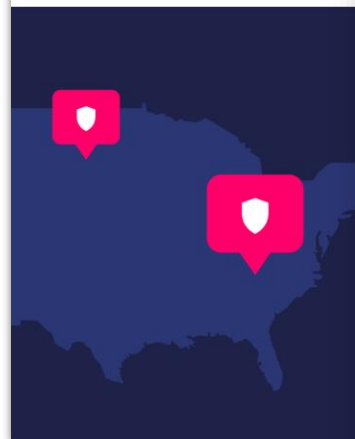
What is being offered?

Noname Advanced API Security for IBM

Discovery

Locate and inventory all of your APIs regardless of configuration or type

Host	Method	Path	Issues	Datatypes
Noname Demo	POST	/apis	🔴 High	
Noname Demo	POST	/apis	🔴 High	
Noname Demo	POST	/user	🟠 Medium	
Noname Demo	POST	/register	🟠 Medium	
Noname Demo	POST	/user	🟡 Low	
Noname Demo	POST	/user	🟡 Low	
Noname Demo	POST	/user	🟡 Low	

Posture

Uncover vulnerabilities and misconfigurations to speed remediation and ensure compliance

Data Classification

Data Type	Data Tags	Query Count	Records
💳 Credit Card	🏦 Financial	56M	5M
💳 CCV	🏦 Financial	6M	1M
SSN	🏦 Financial	26M	3M
🏛 Bank Name	👤 Personal	53M	6M
First Name	👤 Personal	2M	6M

Runtime

Detect and block API attacks with real-time traffic analysis powered by machine learning

Custom Policy

Detection Time: 2022-06-19 15:33 | Updated at: 2022-06-19 15:33

Evidence Take Action

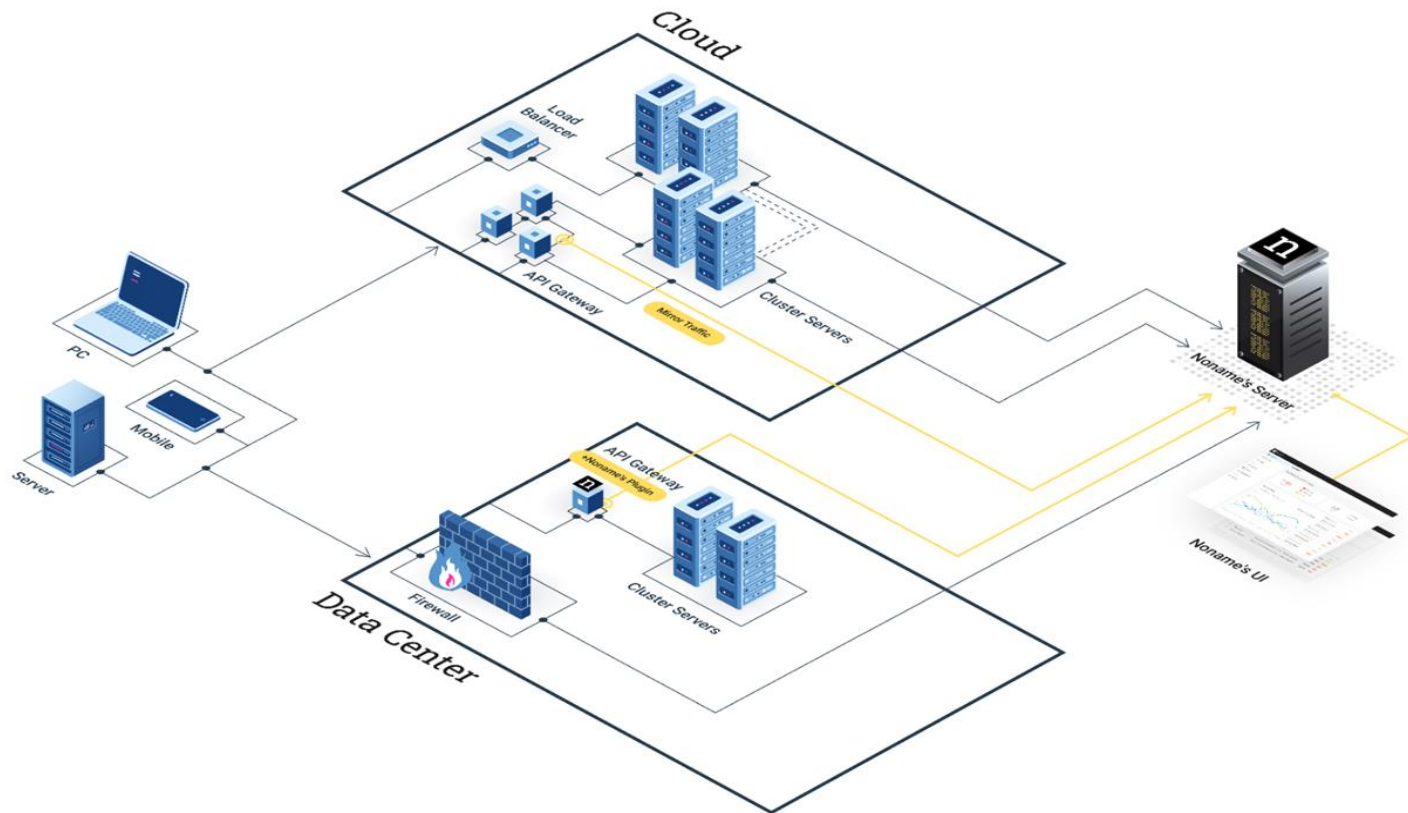**Description** Severity Module
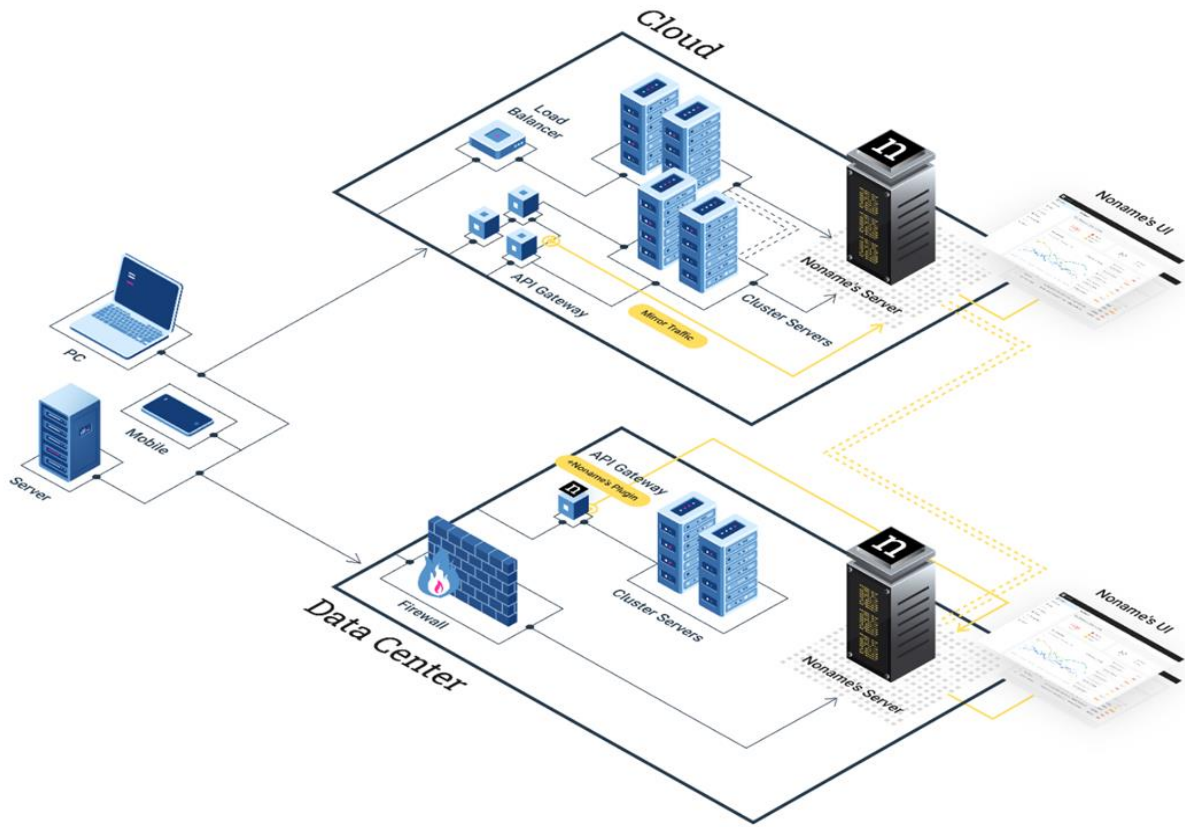
Not Available [DB] Medium 🐛 Posture

API Information

Triggered on

POST research.nonamesecurity.com/transactions/add-transaction

How does it work?

Deployment - SaaS

Deployment - OnPrem

Integrations

amazon web services	**Microsoft Azure**	**Google Cloud**	**apigee**	**M**
AWS	Azure	Google Cloud Provider	Apigee	MuleSoft
ADD NEW	ADD NEW	ADD NEW	ADD NEW	ADD NEW
Kong	NGINX	IBM	PCAP	Network Interface
Kong	NGINX	IBM	PCAP	Network Interface
ADD NEW	ADD NEW	ADD NEW	ADD NEW	ADD NEW
axway	Amazon API Gateway	f5	Kubernetes	paloalto
Axway	Amazon API Gateway	F5	Kubernetes	Palo Alto
ADD NEW	ADD NEW	ADD NEW	ADD NEW	ADD NEW
WSO2	akana	Istio	Bosh	Microsoft IIS
WSO2	Akana	Istio	Bosh	IIS
ADD NEW	ADD NEW	ADD NEW	ADD NEW	ADD NEW

Development Platforms
- Jenkins
- CircleCI
- Bamboo
- Azure DevOps
- Gitlab
- Github
- TeamCity
- Webhooks
- Jira

Network and Cloud
- aws
- Azure
- Google Cloud
- NGINX
- Istio
- kafka
- Kubernetes
- WSO2
- f5
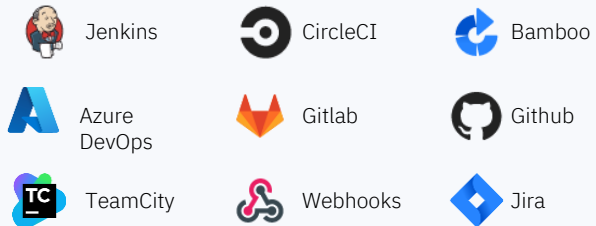
noname
Ecosystem

Workflow Integrations
- Splunk
- QRadar
- Webhooks
- ServiceNow
- Slack
- Jira

API Gateway
- MuleSoft
- apigee
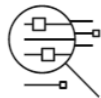- IBM
- Kong
- axway
- akana
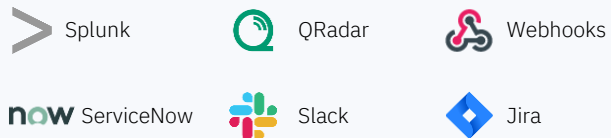
Noname Security extends the capabilities of IBM DataPower and IBM API Connect to enable organizations to provide advanced security of APIs throughout their lifecycle.

Find API security issues faster

Intelligently identify and prioritize potential vulnerabilities. Remediate manually, semi-automatically or fully-automatically.

Discover the unmanaged

Catch vulnerabilities and issues earlier, and prioritize based on impact to reduce remediation costs.
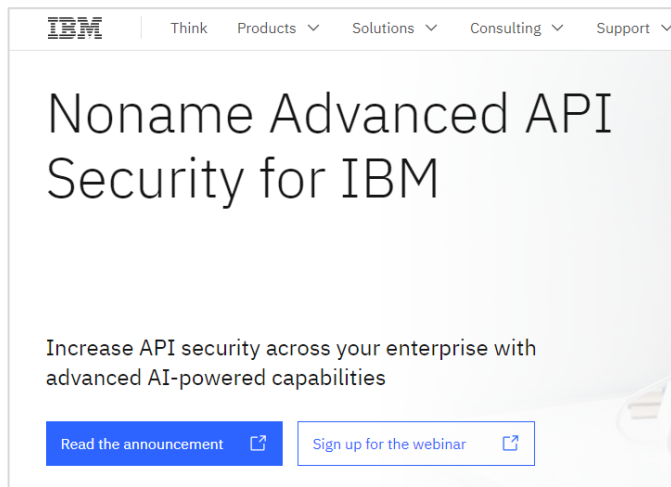
Ensure compliance

Continuously monitor for compliance with regulatory requirements, industry standards and internal policies.
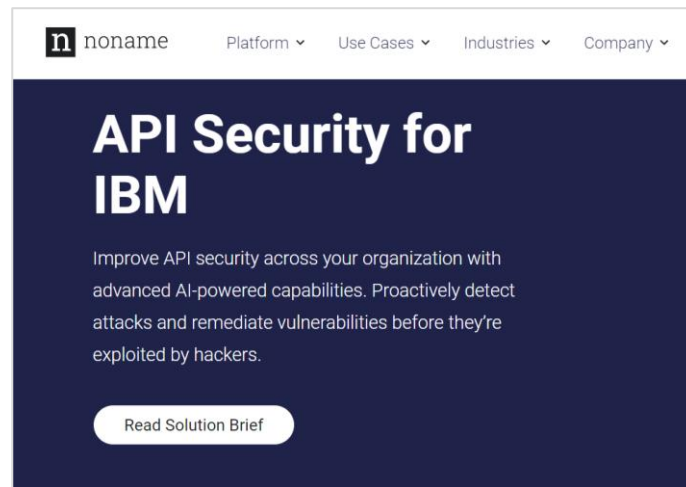
See through the noise

Conduct real-time traffic analysis with automated AI and machine learning detection, and use automated remediation to stop attacks in real time.

Intelligent asset management

Learn more

Visit the IBM product page:
ibm.biz/api-security

Visit the partner page at Noname:
nonamesecurity.com/ibm