



API Discovery



API Posture Management



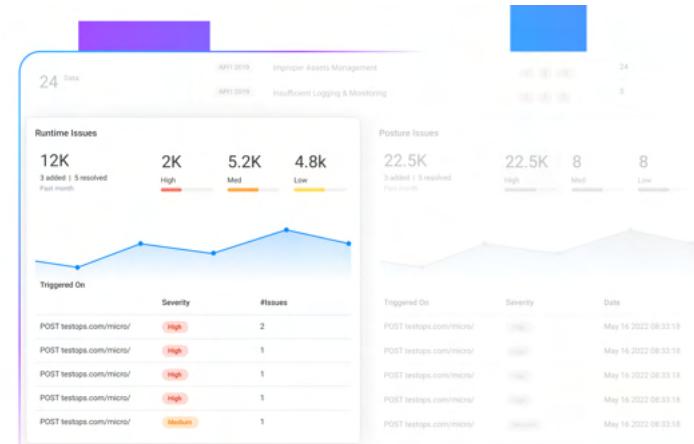
API Runtime Protection



API Security Testing

Runtime Protection

One of the unique and complicated properties of APIs is that usage patterns differ greatly depending on the functionality of the API. To adequately detect malicious traffic during runtime, you need to successfully differentiate between normal and abnormal behavior.



Why you need API Runtime Protection

Runtime Protection detects the most complex API business logic-based attacks like BOLA – where the incoming request demands access to objects which do not match the authenticated client – and blocking attacks in real-time. Successful Runtime Protection is based on differentiating normal versus abnormal behavior.

Noname Security API Runtime Protection

Noname employs unsupervised offline Machine Learning to perform anomaly detection based on historical behavior on a per-API basis. We will first learn the expected behavior of each API endpoint and, subsequently, evaluate each additional request against the baseline to detect outliers indicating malicious intent.

By using Noname Security API Runtime Protection, you can:

- Reduce risk by stopping attacks immediately
- Reduce costs by identifying and remediating vulnerabilities before exploitation
- Reduce lost revenue from downtime
- Enhance compliance with regulatory requirements and internal policies

The screenshot shows the Noname Security API Runtime Protection interface. The top navigation bar includes tabs for 'Security' (which is selected), 'Inventory', 'Report', and 'Testing'. On the far right are icons for 'Label', 'Settings', 'Notifications', and a user profile.

The main content area has two main sections: 'Attackers' on the left and 'Attacker Details' on the right.

Attackers Section:

- A search bar at the top left.
- A filter bar below it with 'Groups' and 'Domains' tabs, and a dropdown menu showing 'Root'.
- A table listing various identifiers (e.g., 1234-1234) with their identifier types (User ID, IP Address).

Attacker Details Section:

- A large button labeled 'Block Attacker'.
- Attacker Information:** Displays the Identifier (1234-1234), Identifier Type (User ID), Risk level (Med), and a summary of Issues (10 High, 6 Medium, 1 Low).
- Location:** Germany (+3 attempts).
- Last Attempt:** Thu May 12 2022 13:22:55.
- Is Blocked:** False.

Issues Section:

- A table showing a list of issues across different modules (Posture) and types (Path Traversal). The columns include Module, Type, Country, IP, Severity, Detection Time, and Status.

| Module | Type | Country | IP | Severity | Detection Time | Status |
|---------|----------------|----------------|------------------|----------|------------------|----------------|
| Posture | Path Traversal | United Kingdom | 1.1.1.1, 2.1.1.1 | High | 2022-01-12 11:18 | Open |
| Posture | Path Traversal | US | 1.1.1.1 | Medium | 2022-01-12 11:18 | In Progress |
| Posture | Path Traversal | Australia | 1.1.1.1 | Low | 2022-01-12 11:18 | False Positive |
| Posture | Path Traversal | China | 1.1.1.1 | Low | 2022-01-12 11:18 | False Positive |
| Posture | Path Traversal | China | 1.1.1.1 | Low | 2022-01-12 11:18 | False Positive |

Remediation

Once the Runtime Protection module identifies a malicious user, we offer the possibility to either manually or through automated policies block the active attacker while simultaneously identifying the root cause so future exploitation can be avoided.

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.

