Product Brief

noname

API Discovery

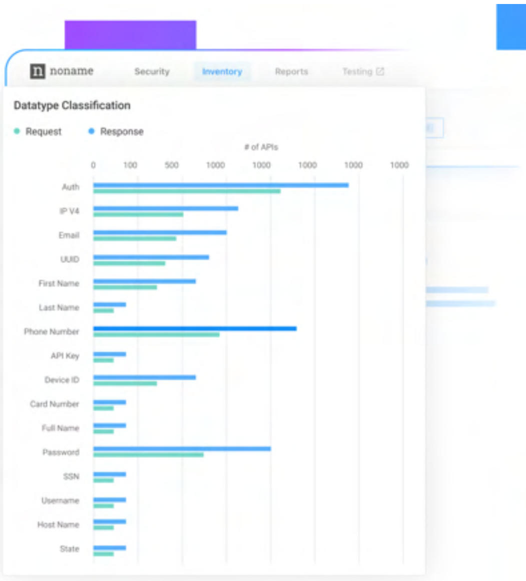
API Posture Management

API Runtime Protection

API Security Testing

Posture Management

Next to providing a complete inventory of APIs using Discovery, Noname Security Posture Management will assess your APIs and broader infrastructure for misconfigurations and vulnerabilities to identify potential risks and understand their true attack surface.



Why you need API Posture Management

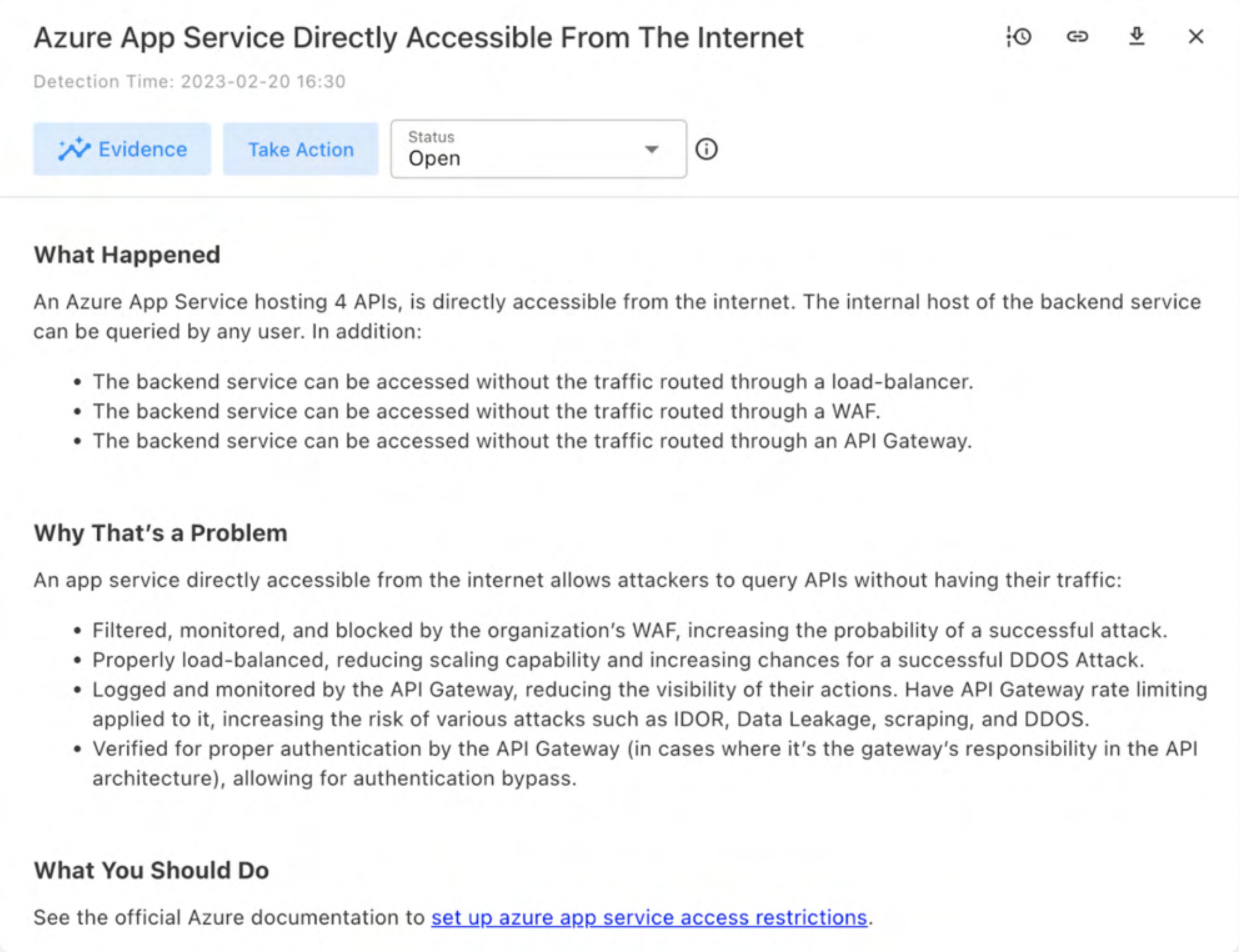
APIs increasingly manage sensitive data and govern privileged access to systems, it is paramount to detect misconfigurations and vulnerabilities before they lead to exploitation. According to analysts and practitioners, misconfigurations are the leading cause of security breaches across industries. By identifying and classifying these vulnerabilities, we present a path for quick and easy remediation.

Noname Security API Posture Management

Noname provides wider visibility and deeper insights: Noname finds APIs, domains, and related issues from both inside and outside the customer's network perimeter, and uses intelligent data classification and context-aware analysis to create the most accurate and complete inventories, and identifies inherent misconfigurations.

By using Noname Security API Posture Management, you can:

- ✓ Identify potential risks and understand their true attack surface
- ✓ Reduce costs of remediation by catching vulnerabilities and issues earlier
- ✓ Bolster existing security investments by spotting and remediating misconfigurations in the end-to-end API flow.
- ✓ Enhance compliance with regulatory requirements, internal policies, and OWASP API Top 10



Azure App Service Directly Accessible From The Internet

Detection Time: 2023-02-20 16:30

Status: Open

What Happened

An Azure App Service hosting 4 APIs, is directly accessible from the internet. The internal host of the backend service can be queried by any user. In addition:

- The backend service can be accessed without the traffic routed through a load-balancer.
- The backend service can be accessed without the traffic routed through a WAF.
- The backend service can be accessed without the traffic routed through an API Gateway.

Why That's a Problem

An app service directly accessible from the internet allows attackers to query APIs without having their traffic:

- Filtered, monitored, and blocked by the organization's WAF, increasing the probability of a successful attack.
- Properly load-balanced, reducing scaling capability and increasing chances for a successful DDOS Attack.
- Logged and monitored by the API Gateway, reducing the visibility of their actions. Have API Gateway rate limiting applied to it, increasing the risk of various attacks such as IDOR, Data Leakage, scraping, and DDOS.
- Verified for proper authentication by the API Gateway (in cases where it's the gateway's responsibility in the API architecture), allowing for authentication bypass.

What You Should Do

See the official Azure documentation to set up azure app service access restrictions.

Remediation

Identifying misconfigurations and vulnerabilities is one thing, we subsequently need to implement specific remediation as quickly as possible. Once we identified an issue we then provide insights into:

- What exactly happened, providing more context on the issue at hand
- Why it is a problem and what the potential impact of the issue could be
- What you should do about it, including remediations of third-party environments like Public Cloud services

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