noname

SOLUTION BRIEF

Gateways, WAFs, and API Security

Filling in the Gaps with Noname Security

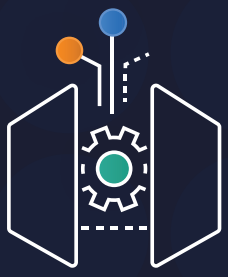
Filling in the Gaps with Noname Security

The pace of digital transformation shows no signs of slowing. Driven by both the need for frictionless hybrid workforces and innovation requirements to drive new revenue streams, digital transformation continues to remain a top initiative for IT leadership teams. At the core of these digital transformation initiatives are APIs.

While APIs are at the key enabling digital transformation, IT security teams still lack proficiency and maturity when it comes to ensuring that APIs are adequately secured. While APIs aren't exactly "new" technology, the tremendous API growth in numbers, data volume, and ubiquity can overwhelm application security teams.

The result is significant gaps in API observability capabilities as well as the application of API-specific security controls.

Contributing to the lack of existing API security proficiency and maturity is the distributed nature of many modern APIs. API security controls are distributed between the delivery technology stack that includes API management, API gateways, web application firewalls (WAFs). While there are other components in the stack, these are the ones that are most notably relied upon for enforcing security policy and controls.



API Management and Gateways

API management and API gateways play a very important role ensuring the delivery of APIs. Each plays a defined role and are tightly linked together with the API management operating at the control plane (management and policy) and the API gateway in the data plane (proxy with policy enforcement). The primary functions of API management and gateways are to publish APIs, ensure API availability, monitor usage, and enforce access controls.

API management is usually delivered as a portal service where developers and API managers can check in their APIs when they are ready to be in production. API management is used to manage and monitor the operations of the API.

As the name suggests, API gateways serve as an access control point in front of an API endpoint. The API gateway provides core functionality to ensure the API is available to its intended consumers. The API gateway also is a control point for the API management policies such as access controls and usage (e.g. rate limiting and quotas). Routing traffic through an APIgGateway is a best practice, especially for open APIs (exposed to the internet), however not all APIs sit behind a gateway. These APIs do not benefit from the controls and visibility provided by gateway and management functions.

Web Application Firewalls (WAFs)

Designed for web applications, WAFs have become part of the core stack for application and API protection.WAFs are proxy-based tools that inspect incoming http(s) web and API requests for attack or unwanted traffic. WAF capabilities vary, however the basic function is to provide an application layer filter for web and API traffic. This filter looks for malicious/unwanted content within incoming requests (headers and payloads) and is also used to ensure that only approved actions can be performed (by policy).

WAFs are utilized to provide rudimentary protections for applications and APIs. They are fairly proficient at detecting known attacks (with signatures) and malicious scripts. Premium WAFs add in anti-automation capabilities broader coverage of the OWASP Top 10 for web apps. Like API gateways, a WAF can only apply policy to traffic that passes through it.

API Security Gaps

Both API gateways and WAFs are important components of the API delivery stack but neither are designed to provide the security controls and observability required to adequately protect APIs.

Full Observability:

Both API gateways and WAFs can only observe API traffic that is routed through them. Gartner predicts that 50% of enterprise APIs will be “unmanaged” by 2025 which means that observability will be limited at best. While some unmanaged APIs are deployed intentionally, others may be unknown “shadow” or “zombie” APIs that could be putting the organization at risk. Even if all APIs are routed through gateways and WAFs, most enterprise organizations will only have fragmented views of their API estate that could span across multiple teams or business units.

Security Posture Management Analysis:

Without full context-aware visibility the API estate the combination API gateways and WAFs simply cannot provide detailed analysis of the API posture. Posture management analysis helps IT teams to efficiently identify and resolve misconfigurations that could result in security risk or compliance violations. Misconfigurations, for example could include inadequate authentication, unnecessary exposure (to the internet), lack of rate limiting or encryption just to name a few.

Accurate Inventory:

Simply knowing the number of APIs within the organization is not very useful for security and IT teams. An accurate inventory needs to include contextual API data that includes data types handled, authentication controls, configurations, traffic mappings, routing details, exposure to the internet, and all other relevant meta-data. Neither API gateways nor WAFs can provide an aggregated and current inventory of the full API estate.

API Specific Runtime Security Controls:

The combination of gateways and WAFs provides basic API security controls, gateways can enforce rate limiting and authentication controls, WAFs apply signature-based attack detection and appropriate user-based session behavior. These controls are very much needed, however are not enough to adequately protect the business from API specific attacks and abuse. For example, broken object level authorization (BOLA) attacks look like “ordinary” API traffic to gateways and WAFs enabling them to pass through these controls undetected. Gateways and WAFs lack contextual awareness between API requests and responses.This gap can leave vulnerable not only to BOLA exploits, but other attacks and business logic abuse that simply cannot be easily identified using standard gateway and WAF controls.

Filling in the Gaps with Noname API Security

The Noname API Security Platform helps to fill in the security gaps left by API gateways and WAFs. The solution helps to accurately inventory all APIs, including internal and shadow APIs, and proactively secure your environment from API security vulnerabilities, misconfigurations, and design flaws. The Noname API Security Platform also integrates with existing API gateways, WAFs, and other API delivery components to automatically identify and respond to API specific threats that would otherwise go undetected.

Full Observability and Accurate Inventory:

The Noname API Security Platform automatically discovers, collects, and aggregates API details from multiple sources including network traffic analysis, API management and gateways, WAFs, application delivery controls and others. The API inventory, including rogue/ shadow and zombie APIs, is automatically classified for more efficient API asset management.

Security Posture Management Analysis:

The Noname API Security Platform performs posture management analysis on the API inventory. The analysis automatically identifies configuration-related vulnerabilities, for example if an API that handles sensitive or regulated data does not have adequate authentication controls enforced. High risk issues are automatically flagged so that security teams can prioritize their efforts where they are most needed. The posture analysis enables proactive risk mitigation and helps to reduce the potential API attack surface.

API Specific Runtime Security Controls:

The Noname API Security Platform provides runtime attack detection to complement existing security controls. Using artificial intelligence (AI) & machine learning (ML) the platform creates API behavior baselines. Anomalous behavior, such as BOLA attacks or business logic abuses, are automatically detected and flagged. Remediation can be automated by policy or initiated through integrations with existing work IT workflows.

Better Together: Get More Value from API Gateways and WAFs with Noname Security

Cybersecurity is a team sport, and securing APIs is no different. There is no single solution that can adequately fulfill all the aspects required for comprehensive API observability and security. API management, gateways, and WAFs all play critical roles, however alone they can leave APIs vulnerable. The Noname API Security Platform integrates seamlessly with these technologies to fill in the gaps. The combination of these technologies helps to provide safe and secure environments for digital business applications. This enables IT teams to not only better protect APIs and critical assets from cyber attacks, but to also build and maintain an effective API security program within the organization.

noname

SOLUTION BRIEF

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 three pillars — Posture Management, Runtime Security, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Silicon Valley, and offices in Tel Aviv and Amsterdam.

Nonamesecurity.com

info@nonamesecurity.com

+1 (415) 993-7371