noname

Discover All APIs With the Noname API Security Platform

Today, businesses rely on APIs more than ever before, and API usage continues to accelerate. The sheer scale of API usage is staggering. Essentially, every application and device connects or communicates with an API, which is why it shouldn't be surprising that API calls represent 83% of all web traffic.

APIs are also the new cybersecurity battlefield. As more and more companies publish their APIs and connect them to the open web, cyber attackers increased their exploitation of this attack vector. What's more, APIs have been in use for decades — pre-dating AppSec teams, API gateways, and the OWASP API Top 10. It's only a matter of time for bad actors to sniff out legacy or shadow APIs that don't comply with your current processes and standards.

Businesses need to reduce the risk of their growing vulnerabilities of APIs. To support the needs of businesses, Noname Security developed the D.A.R.T. API Security Strategy, which stands for:

Discover

Find and inventory all APIs, including legacy and shadow APIs

Analyze

Analyze the access, usage, configuration, and behavior of all APIs to ensure they are used only as intended

Remediate

Resolve misconfigurations and anomalies to reduce risk

Test

Test APIs before and after they are deployed to ensure confidence and trust

The first component of the D.A.R.T. API Security Methodology — Discover — is the most critical because it precludes Analyze, Remediate, and Test. For example, if you haven't discovered the full depth and breadth of your APIs, the value and effectiveness of Analyze and Remediate are significantly diminished.

What Does it Mean to Discover APIs?

API discovery refers to finding and inventorying APIs, as well as gathering rich data from each API's header and payload. Enterprises need a complete inventory of all APIs, and need to surface the granular details about each API. Simply knowing that an API exists doesn't improve your security posture if you can't analyze the access and behavior of the API.

How to Discover APIs

There are basically two ways to discover APIs: in-band solutions and out-of-band solutions:

In-Band API Discovery: Agents

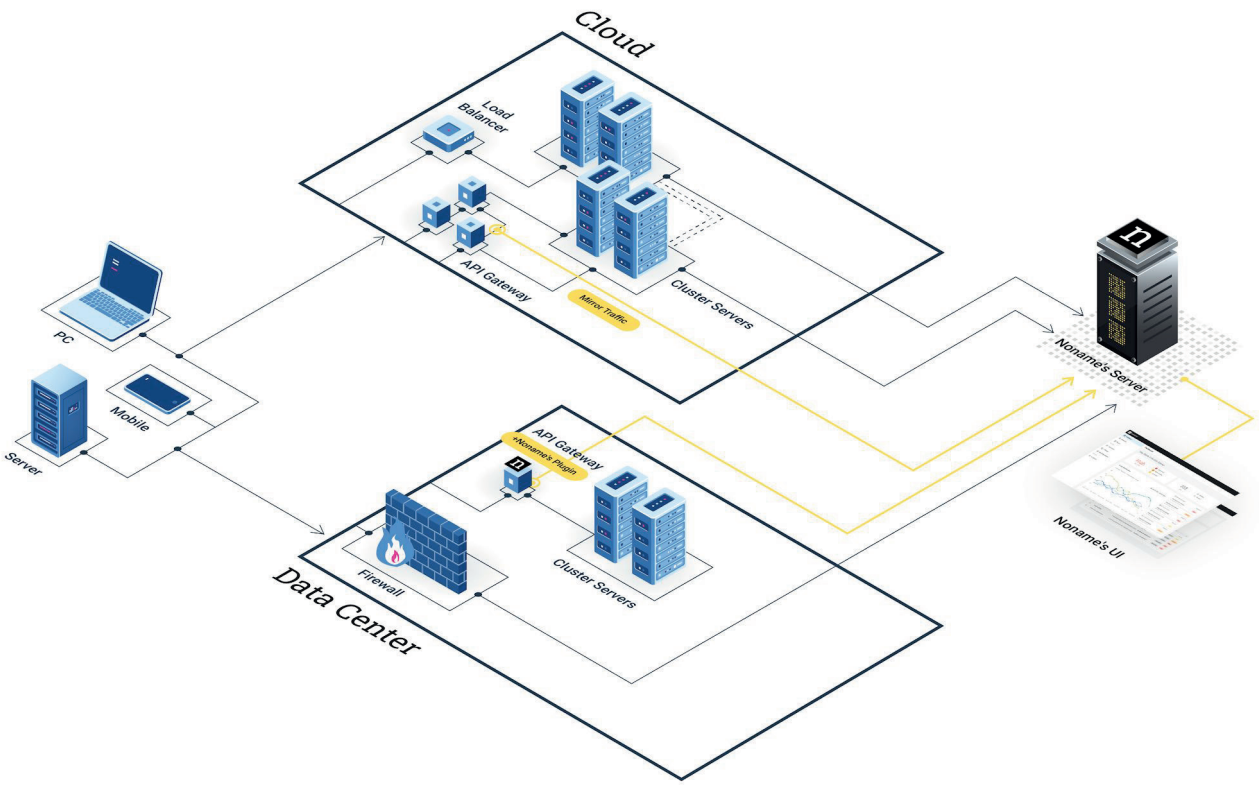
In-band API security solutions rely on information gathered directly from applications and APIs using agents. An agent refers to code deployed within the application, API package, or a strategic position on the network. Agents, sometimes referred to as sensors, aggregate API data that can then be analyzed. As mentioned in the previous section, it's critical that data from the API header and payload are captured.

One of the concerns with agent-based API discovery is the sheer amount of overhead and complexity added to API deployments. The impact to performance and response times is non-trivial. And, as the volume of APIs continues to surge, so does agent upkeep and management. This creates a significant scale challenge for most enterprises.

Additionally, agents can only discover APIs where they are deployed. Shadow APIs, by definition, are APIs that you don't know about. Deploying in-band API discovery solutions, like agents, won't help you find shadow and rogue APIs unless you deploy them everywhere — even where you don't think you need them — and nobody wants to do that. Agent-based API security solutions lead to confirmation bias and a false sense of security.

Out-Of-Band API Discovery

Out-of-Band API security solutions discover APIs without installing agents or creating additional complexity within your existing infrastructure. There are two ways to discover APIs out-of-band. The first is to integrate with API gateways, load balancers, and WAFs. The second is to mirror traffic.



Integrating with API Gateways, Load Balancers, and WAFs

API security platforms should integrate with existing proxies and devices within your infrastructure, like API gateways, load balancers, and WAFs. This method of gathering data utilizes features of the existing devices and is far less complex than using agents.

Hopefully, most APIs are routed through these devices, but often proxies don't provide any visibility or understanding of API behaviour or access. API Gateways, load balancers, and WAFs aren't specifically designed to address the API security challenges associated with misconfigurations, suspicious behavior, and cyber attacks, so integrating an API security platform with your existing infrastructure is important. And, because API gateways, load balancers, and WAFs are deployed across multiple on-prem and cloud environments, an API security platform helps create a single source of truth for all your APIs.

But connecting to your API gateways, load balancers, and WAFs doesn't give you a complete picture.

Traffic Mirroring

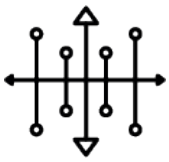
The other method of out-of-band API discovery is called traffic mirroring or virtual TAP (vTAP). Traffic mirroring creates a copy of all network traffic that can be analyzed by an API security platform. This method of API discovery gives you a complete view of all APIs communicating on your network, and doesn't require any agents or network modification.

Most public clouds offer traffic mirroring functionality, and Noname Security has the most advanced capabilities in this area — giving you the broadest and deepest visibility in your API access and behaviour without high complexity or cost. SOAP, REST, gRPC, GraphQL? It doesn't matter. Noname Security sees them all.

Conclusion

API discovery is the first critical function of API security. Enterprises need to build and maintain a complete inventory of their APIs including detailed information from the API header and payload. APIs can be discovered with both in-band solutions and out-of-band solutions, like integrations with API Gateways, load balancers, and WAFs as well as traffic mirroring.

Noname Security recommends the following best practices for API discovery:



For public cloud deployments, use traffic mirroring to get the broadest and deepest look at your API access and behavior.

Integrate with your existing API gateways, load balancers, and WAFs, for both cloud and on-prem deployments and to supplement traffic mirroring.

Only use agents as a last resort and when necessary for extremely unique environments.

Out-of-band API discovery options give you the most clear and objective look at your API landscape without the headaches and false sense of security from agent-based deployments.