CHECK POINT™

THE LEADING CYBER SECURITY PLATFORM

Why API Discovery is Essential for Your Organization's Cloud Security

APIs are an indispensable component of any organization's cloud infrastructure. However, ensuring the security of APIs is critical and begins with gaining comprehensive visibility into their location, functionality, and performance

CloudGuard
WAF

Top API Security Concerns

SHADOW APIs

Rapid updates to the API ecosystem make it difficult for organizations to monitor and regulate all APIs operating in the cloud application. As a result, unmanaged or unknown APIs, often referred to as "Shadow API," become a critical vulnerability that can be easily exploited.

PUBLIC EXPOSURE

Publicly exposed APIs are highly susceptible to attacks, especially in the case of managing large applications with a significant number of APIs. Such scenarios are prone to public exposure misconfigurations such as unintentionally configuring an internal API (e.x internal management portal) as public-facing. Understanding which endpoints are vulnerable can significantly reduce the potential risks associated with such exposures.

SENSITIVE DATA

It is essential for organizations to differentiate between the appropriate placement of sensitive data and its misplacement. Modern web applications rely on APIs to exchange sensitive information, which can result in unnecessary dissemination of this information across your API network. This poses a significant risk that could easily be mitigated through continuous mapping of API metadata.

400% INCREASE IN API ATTACKS IN THE FIRST HALF OF 2023

31% OF ALL MALICIOUS REQUESTS TARGET SHADOW APIS

34% Y/Y INCREASE IN ATTACKS ON CLOUD-BASED NETWORKS

Gartner

"By 2025, fewer than 50% of enterprise APIs will be appropriately managed."

You Can't Ignore API Security Forever

The reliance on APIs has made them a popular target for attackers. This has resulted in insecure APIs costing businesses an estimated $130 billion annually.

API ZERO-DAY EXPLOITS CAUSE SERIOUS DAMAGE TO UNPROTECTED BUSINESSES

One of the biggest risks of having unsecured APIs running in your cloud is the unauthorized access to large amounts of sensitive data.

A well-known example is the Twitter breach which exposed 5.4 million user data, and occurred due to a vulnerability in API in January 2022. Furthermore, in December 2022, the attacker sold 400 million Twitter profiles on the dark web.

In July 2023, a significant cyber security incident involving Ivanti Endpoint Manager Mobile (EPMM) was reported. The attackers exploited a zero-day vulnerability, which allowed unauthorized access to API endpoints.. This vulnerability impacted on average 1 in every 31 organizations worldwide per week during 2023 (after it was disclosed.)

HOW YOUR ORGANIZATION CAN BE AFFECTED BY INSECURE APIs

1. DATA BREACHES
As API connects external applications and users with your internal apps. They are a possible route to your sensitive data.

2. SERVICE DISRUPTIONS
If an API is not properly maintained, it might be easily compromised or simply not able to handle legitimate requests. This might cause considerable service outages.

3. BUSINESS IMPACTS
Security breaches can bring litigation, fines, and direct financial damage. A single data leak can result in irreparable damage to your brand.

Gartner

"Enterprises are producing a massive number of APIs at a rate that far outpaces the maturity of network and application security practices."

Visibility Is The Key To API Security

By identifying and analyzing all of your APIs, including Shadow APIs, public endpoints, and sensitive data, you can improve control of your attack surface and reduce the risks of breaches.

DISCOVER YOUR APIS AND META DATA

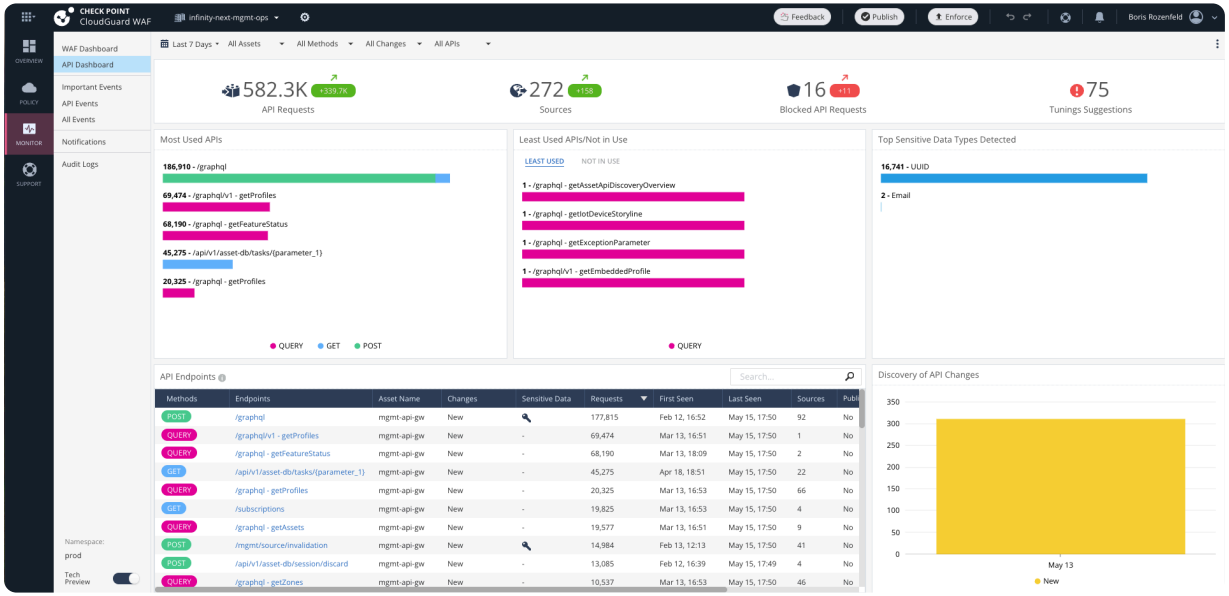
Detect ALL APIs running in your cloud and eliminate Shadow APIs. By differentiating the various assets in your cloud, such as API endpoint, type, public-facing vs. internal or new vs. old, you can tailor your security to meet critical needs.

PROTECT YOUR SENSITIVE DATA

Monitor sensitive data usage, such as PII, financial data, and login credentials, to comply with relevant regulations and standards and minimize the risks of improper exposure.

MONITOR API CHANGES

Regular monitoring and testing of APIs are essential to detecting any misplaced data, drift or misconfigurations that may arise over time.Security teams are notified each time an API is added or modified to ensure contiuous compliance and posture.



CLOUDGUARD WAF PROVIDES EXTENSIVE & AUTOMATED DISCOVERY, CONTROL AND PROTECTION FOR APIS BASED ON MACHINE LEARNING TO EFFECTIVELY MONITOR AND PROTECT YOUR ENTIRE API LANDSCAPE

Gartner

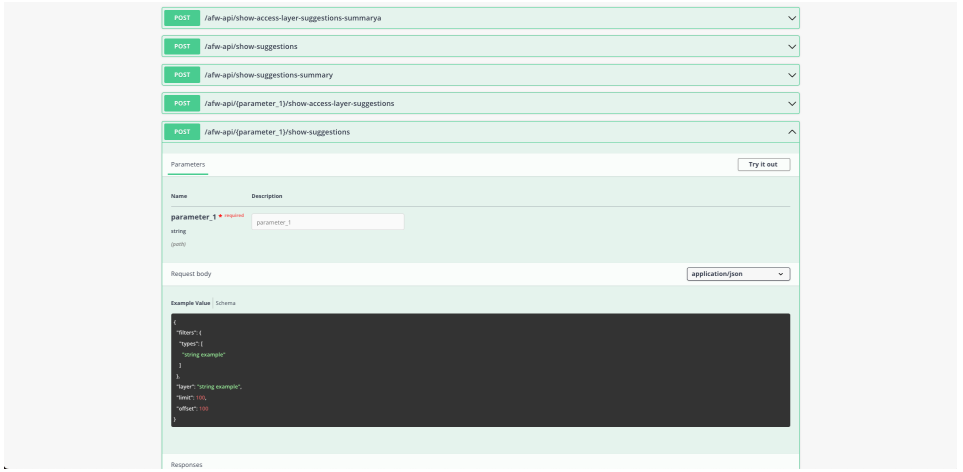
"By 2025, more than 50% of enterprises will use GraphQL in production, up from less than 10% in 2021."

Auto Generated SWAGGER Schema Provides Full Visibility and Strict Enforcement

Using OpenAPI (Swagger) specifications generated from actual traffic, you can gain full visibility and enable **simple evaluation** of your APIs. We use machine learning to continuously optimize schema clustering of all your APIs by end-point and additional meta data to ensure precise documentation and better access for your security team.

AUTO GENERATED OPENAPI SECURITY SCHEMA

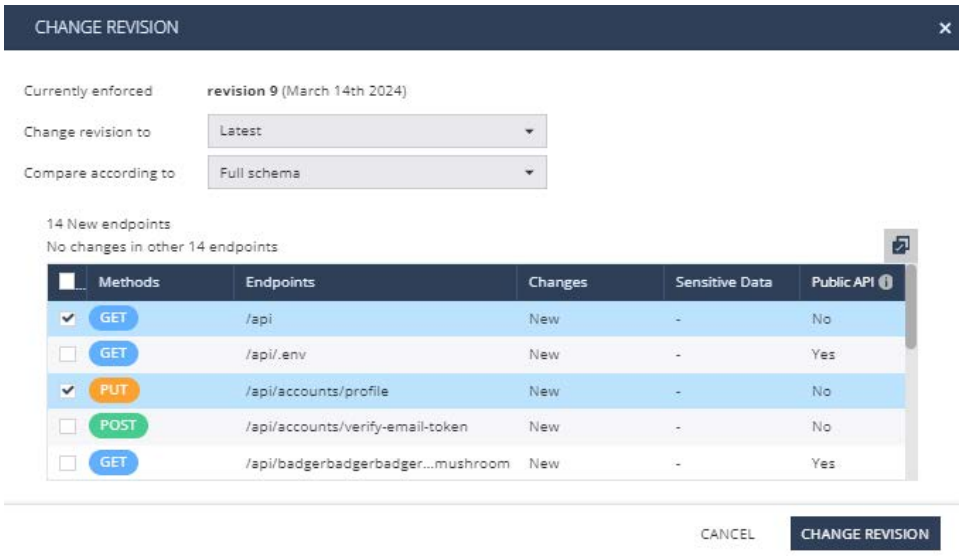
You can prioritize your API security efforts and minimize the risk of breaches and compliance violations by identifying, tracking, and remediating high-risk API endpoints that process sensitive data such as PII and login credentials, based on OpenAPI specifications generated from actual traffic or uploaded by the development team.



SCHEMA VALIDATION AND ENFORCEMENT

The OpenAPI schema defines which API requests are valid based on several request properties like target endpoint, path or query variable format, and HTTP method as well as any associated data in the body of the API.

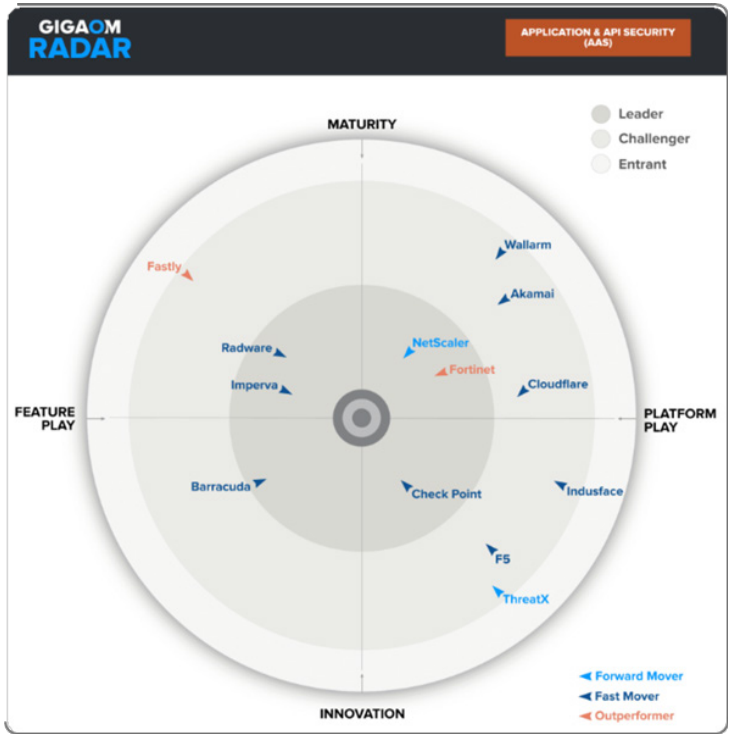
Schema Validation allows you to check if incoming traffic complies with a previously supplied API schema. When you provide an API schema or select from a list of learned schema, CloudGuard defines which traffic is allowed and which traffic gets logged or blocked.



CLOUDGUARD NAMED LEADER IN GIGAOM 2024 RADAR REPORT FOR APPLICATION AND API SECURITY FOR 2 YEARS IN A ROW

"The biggest strength of the CloudGuard WAF solution is API protection. While All Vendors can either import or detect APIs and most vendors can do both, CloudGuard is able to do both and generate sample protection rules based upon the definition and information gleaned from traffic. ***This earned them our highest score on the API import and discovery key feature."***

Don Mcvittie, Analyst | GigaOm



Available for

Kubernetes · NGINX Ingress · NGINX · KONG · NEW! Nginx Proxy Manager · SOON ENVOY · SOON Emissary Ingress

CloudGuard CNAPP

UNIFIED, PREVENTION-FIRST CLOUD SECURITY PLATFORM

CloudGuard CNAPP serves as a unified platform dedicated to securing your cloud environment. With its prevention-first approach, it allows for consistent and repeatable enforcement across cloud providers. We cover you from risks, regardless of their origin, before they reach production and at runtime, known and unknown alike.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391
www.checkpoint.com