KuppingerCole Report

EXECUTIVE VIEW

By Alexei Balaganski

March 26, 2021

Cequence Security API Sentinel

API Sentinel is an API security product focusing on API inventory and usage monitoring, as well as identification, assessment, and mitigation of API-related security risks. As a part of the company's extensible cloud-native Application Security Platform, it provides comprehensive API monitoring and protection for all types of APIs and deployment scenarios.

By **Alexei Balaganski**
ab@kuppingercole.com

Content

1 Introduction

Over the last decade, Application Programming Interfaces (APIs) have evolved from a purely technical concept created for developers into one of the foundations of the modern digital economy. Today, APIs can be found everywhere. They enable business communications with suppliers, service providers, and customers. They ensure that applications from different vendors can exchange data seamlessly, orchestrate massive cloud infrastructures and global networks of smart devices. They can also unlock new business models for companies to offer their core services in innovative ways or to reach new customers.

In short, APIs are no longer just an IT thing -- they have a strong impact on nearly every business's operational efficiency, scalability, and agility and in the end, directly influence its profitability. Unfortunately, in this booming API economy, potential security risks are often underestimated. Alternatively, many companies still believe that traditional security tools like web application firewalls or intrusion detection systems can provide sufficient protection against API-specific attacks. Alas, numerous publications about API-related cyberattacks and data breaches that affect even the largest enterprises like Facebook or Tesla clearly show otherwise.

A proper, well-planned strategy for protecting various internal and external, own and 3rd-party APIs must address every step along the API lifecycle, which, at least for APIs developed in-house, starts with secure design, long before the operational phase. At later phases, several different technologies have to be applied, including but not limited to network security (encryption, firewalling, DLP, etc.), protection against numerous API-specific threats and exploits, strong authentication and fine-grained access control, maintaining sensitive data integrity, as well as monitoring and analytics.

But one could also argue that for all API users, security begins at the discovery stage: without a full inventory, classification, and risk assessment of all known and unknown APIs, consistent protection is simply impossible. And this inventory cannot be a one-time process -- continuous real-time monitoring is needed to reflect the ever-changing IT landscapes and new types of threats that emerge constantly. Security analysts, overworked and stressed by thousands of alerts, expect the API security solutions to match other modern security analytics tools in intelligence -- being able to detect unknown malicious and suspicious activities, perform risk assessments, and offer actionable (or even better, automated) recommendations for mitigating the identified threats.

Cequence Security is a cybersecurity company headquartered in Sunnyvale, California. Founded in 2015 by a group of security industry veterans previously from Palo Alto Networks and Symantec, the company focuses on developing a unified ML-based Application Security Platform. This cloud-native, containerized platform powers several security products ranging from web and mobile app protection to API inventory, monitoring, and risk assessment.

API Sentinel is the company's specialized API security product, a cloud-native, easily deployable solution for

performing real-time API discovery and usage analysis, detection of OpenAPI specification non-conformance, and risk assessment according to multiple metrics and policies, helping users to identify and mitigate API-related security risks before they turn into data breaches. Together with the company's other solutions like Bot Defense and App Firewall, Cequence Security can offer its customers a comprehensive, well-integrated platform for addressing API risks at multiple stages of their lifecycles.

2 Product Description

API Sentinel is Cequence Security's specialized API security product, focusing on API inventory and usage monitoring, as well as identification, assessment, and mitigation of API-related security risks. It is the most recent addition to the company's Application Security Platform, an extensible cloud-native platform that provides comprehensive threat detection and mitigation for web applications, mobile apps, and APIs.

The whole platform is fully containerized and thus supports a variety of deployment scenarios, on-premises, in any public cloud, or as a SaaS offering. With native integrations with multiple content delivery networks (CDN), such as Amazon CloudFront, Akamai, and Fastly, Cequence can ensure that its solution can be deployed within minutes and won't require changes in existing application architectures. However, even for complex custom scenarios, the platform provides deployment flexibility in any environment where containers are supported. The sensors that perform traffic analysis can be deployed both in-line as network proxies or connect to a tap interface for passive monitoring.

The core technology that powers the Cequence platform is CQAI -- a patented machine learning-based analytics engine that processes the transactional data collected by the platform sensors to discover, analyze and monitor web, mobile, and API-based applications. By maintaining behavior profiles of each application or API, the platform can then analyze each transaction to identify not just known malicious actions, but anomalies and other suspicious activities as well. These include bot attacks, vulnerability exploits, credential stuffing, and other types of attacks, as well as identifying behavioral patterns of existing bot management toolkits such as OpenBullet, Snipr, and MBA.

The findings that the AI engine makes across single and multiple transactions, as well as the results of "intent analysis" (in other words, identification of known behavioral patterns such as attack techniques or vulnerability exploits) can be combined with external threat intelligence to allow customers to assess the levels of risk their applications are exposed to, to create security policies that automatically mitigate certain threats or to feed the results into an existing SIEM or SOC platform for a detailed investigation. A built-in data lake based on the Elastic Stack is used to store all collected information.

API Sentinel is built upon this foundation and implements discovery, monitoring, and real-time risk assessment for APIs in a wide variety of environments. As opposed to many competing solutions that typically focus either on edge deployment scenarios (inspecting API traffic only at the ingress point) or on distributed, microservice-oriented architectures (deployed alongside with business microservices and monitoring internal API traffic), API Sentinel, thanks to its flexible container-based architecture and breadth of technology integrations (e.g., API gateways, proxies, ingress controllers, load balancers, etc.) can mix and match both approaches.

By analyzing the application traffic, the product can instantly identify new, not yet managed API endpoints, maintain a comprehensive inventory of all discovered APIs, and collect comprehensive usage statistics for

each of them. The management console provides the tools for analyzing various operational and security metrics of managed APIs, as well as for sorting, grouping, or tagging APIs into logical categories for business or development purposes.

The user interface of the console is designed around a rich set of dashboards that visualize various API metrics, provide aggregate statistics around operations and risk findings, and allow security experts to drill into detailed information about each API or a single transaction. Users can monitor API usage trends based on specific IPs or geolocations as well. Besides, anomalies in API usage are detected automatically, including access from unauthorized clients, known malicious domains or IP ranges, or non-reputable organizations and countries.

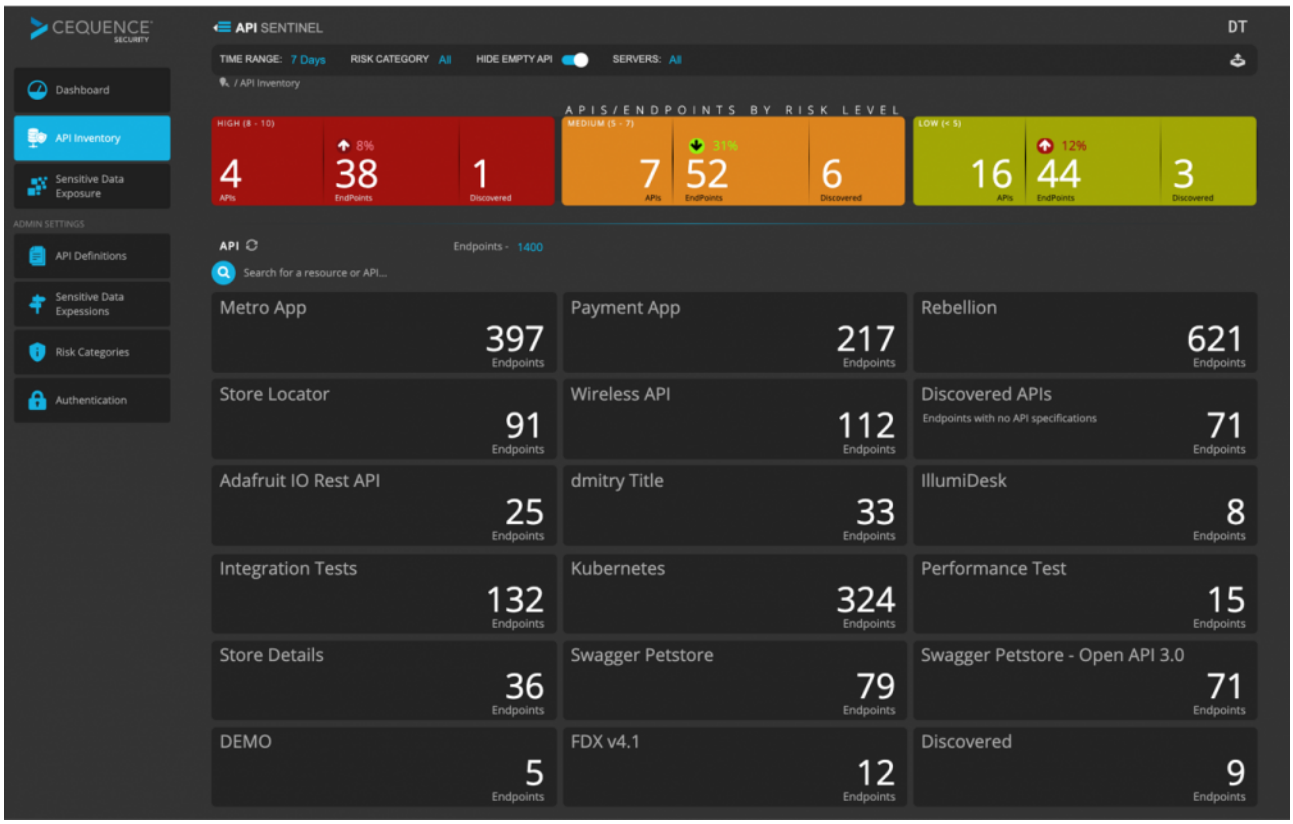

Figure 1: API Inventory Dashboard

A notable feature of API Sentinel is the ability to attach an OpenAPI specification to each managed API, which would provide the baseline for detecting whether an API has drifted from its original schema. In fact, schema non-conformance is one of the three API risk categories built into the platform, the other two being sensitive data exposure and insecure access controls. By detecting the drift from the published API specification, identifying known patterns of sensitive data in network traffic, and exposing weak or non-existent authentication in APIs, API Sentinel calculates dynamic, real-time risk scores for each detected endpoint.

Users that require more additional risk capabilities, can create custom rules based on any combination of API attributes, such as request headers, query parameters, response codes, client details, etc. Complex rules based on scripting are possible. Over 180 pre-defined rules are provided with the product out of the box, which can be enabled to detect additional risks or attack types.

APIs with schema violations or without attached specifications (in other words, unmanaged "shadow APIs") have an especially high risk associated with them and thus are prominently displayed. The product provides detailed information on factors contributing to the risk, such as undeclared methods, parameters, or request headers. Similarly, endpoints leaking sensitive data are presented in a dedicated dashboard that displays the data patterns (social security and credit card numbers or custom patterns using regular expressions) that are being leaked, how they are being leaked (e.g. response body or headers), and the clients (IP addresses and countries) to which the leakage is taking place.

Policy management is defined as an ability for users to combine detection rules with mitigation actions that can be applied to all APIs or certain endpoints or groups. The actions include basic reporting functions like sending an alert over email or pushing events into SIEM tools. However, the sensor modules, when deployed inline, can perform mitigation actions as well, such as stopping malicious bot traffic.

Besides built-in tools, the platform supports many external integrations. Notably, it is possible to integrate with 3rd party API gateways, Web Application Firewalls, or similar tools to implement advanced mitigation capabilities. Additionally, API Sentinel can export its findings into a variety of security analytics platforms. Finally, the platform provides its own set of APIs for further integrations and customizations.

It should be noted, however, that while API Sentinel does offer comprehensive analytics and risk assessment capabilities, it does not provide full protection against all types of attacks it can detect -- at least, not without the company's other products -- App Firewall and Bot Defense. When deployed together, the products provide a unified management console with consolidated analytics across the full range of security findings. Also, Bot Defense provides additional mitigation capabilities for blocking or throttling incoming attackers or even deceiving them into believing that their attacks were successful.

3 Strengths and Challenges

Although API Sentinel is the most recent addition to Cequence Security's product portfolio, it is designed around an existing application platform powered by a sophisticated AI-based security analytics technology. Its flexible and modular architecture allows for deployments into any type of environment, from modern microservice-based applications and cloud-native API infrastructures to legacy on-premises systems, enabling consistent and unified monitoring, analytics, and risk assessment for all types of APIs across whole enterprises.

Ease of deployment and rich reporting functions ensure that even smaller companies without teams of experts trained in the field of API security can start with the platform without a lengthy setup and learning process. Although the number of out-of-the-box risk categories, data classification rules, and security policies is not that impressive, users are free to create their own, which can be quite sophisticated. Perhaps, we will see a kind of an online marketplace for customers to exchange their custom content in future releases.

Together with other products from Cequence's portfolio, any organization can quickly and effortlessly deploy a comprehensive platform that covers multiple aspects of API security ranging from discovery and risk assessment to vulnerability management and threat mitigation yet remains open to additional future expansion and 3rd party integrations.

Strengths

- Integrated application security platform powered by purpose-built AI-driven analytics engine.
- The flexible fully containerized architecture supports all types of deployment, including hybrid, multi-cloud, microservice-based.
- A broad set of technology integrations enable the discovery and protection of both external and internal APIs.
- Automated API inventory simplifies management, creation of policies.
- Real-time API risk assessment with sensitive data leakage discovery and configurable, extensible risk modeling.

Challenges

- Individual modules of the Application Security Platform are not yet integrated into a single management console.
- The number of out-of-the-box content inspection patterns is still quite low.
- No support for API specification validation.

4 Related Research

Leadership Compass: API Management and Security -- 70311

Buyer's Compass: API Management and Security -- 80215

Whitepaper: The Dark Side of the API Economy -- 80019

Advisory Note: The Role of APIs for Business -- 70946

Advisory Note: Connected Enterprise Step-by-step -- 70999

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.