CEQUENCE® SECURITY

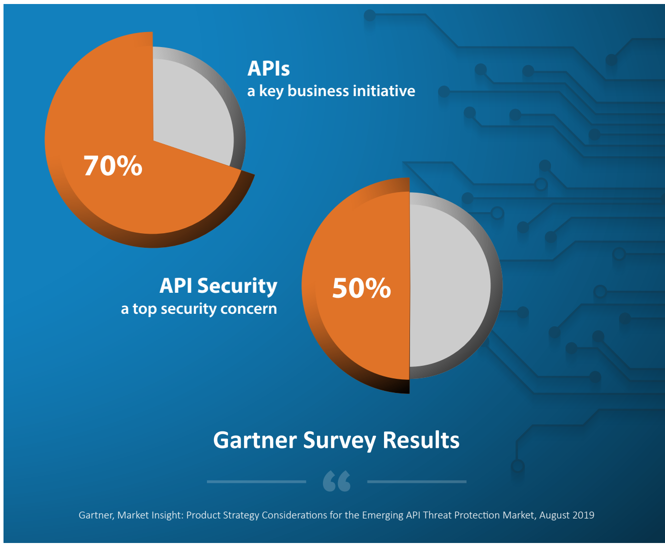
API Sentinel: Continuous API Discovery and Inventory Tracking

Discover and Remediate API Security Gaps at Runtime

Contents

Introduction

APIs are at the heart of the ongoing enterprise digital transformation, acting as conduits for data exchange between applications, infrastructure and IoT devices. For many organizations, they have become primary business enablement pillars, as evidenced by a recent Gartner survey where 70% of the respondents indicated that APIs are a key business initiative. APIs are key to the move towards modular applications and the use of Containers; they are integral to the expansion of partner ecosystems and act as the connective tissue for most all mobile applications. APIs, like many new development trends introduce security challenges, as evidenced by data from the same Gartner survey that that says API security is a top concern for 50% of the respondents.

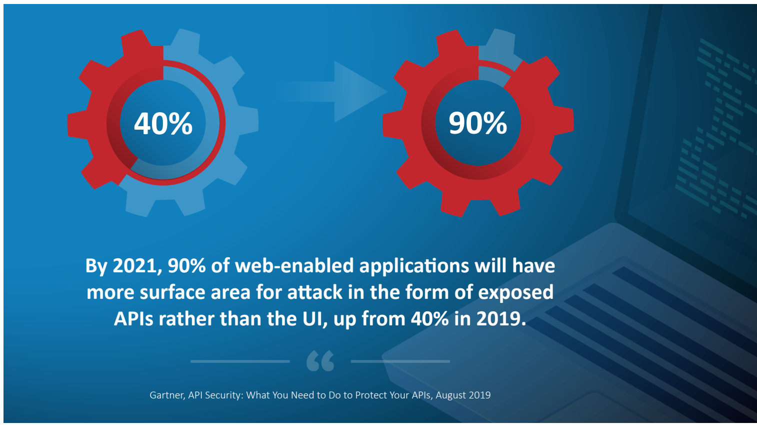


Gartner Survey Results

Gartner, Market Insight: Product Strategy Considerations for the Emerging API Threat Protection Market, August 2019

Today, most organizations expose APIs for internal use, for customers and for partners that are a published using both in-house and open-source resources. Often times, APIs are published by different teams, using different application stacks, and following various DevOps and lifecycle procedures, often without consistent security and oversight. These factors make APIs a double-edged sword and introduce a range of security challenges, including:

- Shadow, deprecated, or hidden APIs that fall outside of the security teams' visibility are left unprotected. These APIs may transmit sensitive data and jeopardize regulatory compliance.
- Hidden parameters that can lead to privilege escalation by allowing an attacker to change a user profile to "admin" that can then lead to data loss, fraud or worse.
- Exposure of confidential or sensitive data in response codes or error messages that can be used to steal data or as a form of reconnaissance for a larger scale attack.
- Application business logic flaws that enable bad actors to commit fraud through account takeovers, scraping, fake account creation and other forms of API abuse.



By 2021, 90% of web-enabled applications will have more surface area for attack in the form of exposed APIs rather than the UI, up from 40% in 2019.

Gartner, API Security: What You Need to Do to Protect Your APIs, August 2019

Some examples of business logic flaws include an that API might expose too much information when a request is made, providing attackers with insights they can use to further breach a system. Or, an API might lack proper access authentication or inadvertently grant users with elevated privileges, such as administrative rights, which could be used to exfiltrate or change the data.

To address this along with the other security challenges highlighted above, organizations need to understand and rein in their API footprint. However, when researching solutions to solve the API visibility challenge a young, fragmented market is revealed that, when combined with an increase in decentralized development, has created a situation where most enterprises lack a basic understanding of their API landscape much less its associated security exposure.

Security Recommendations: OWASP API Security Top 10

As an validation of the API growth, popularity and associated security concerns, OWASP released their inaugural API Security Top 10 list in December 2019 resulting in additional emphasis on the need to create and publish secure APIs. Much like the previous Top 10 lists produced by OWASP, the API Security Top 10 list helps both security and development work towards the unified goal of secure API coding practices. Unlike traditional monolithic applications, APIs are stateless, include the entire transaction and execute functionality, which means developers need a deep understanding of the API and its surrounding functionality. A quick summary of the OWASP API Security Top 10 is shown below.

OWASP API Top 10	Typical Root Cause
API1: Broken Object Level Authorization	Weak Access Control
API2: Broken User Authentication	Weak Access Control
API3: Excessive Data Exposure	Business Logic Abuse
API4: Lack of Resources & Rate Limiting	Insufficient Traffic Management
API5: Broken Function Level Authorization	Weak Access Control
API6: Mass Assignment	Business Logic Abuse
API7: Security Misconfiguration	Business Logic Abuse
API8: Injection	Application Vulnerability
API9: Improper Assets Management	Lack of Holistic Visibility
API10: Insufficient Logging & Monitoring	Lack of Operational Security Readiness

Table 1: OWASP API Security Top 10

As organizations expand their use of APIs and formalize associated security and management efforts, the OWASP API Security Top 10 can be a valuable resource to help guide security and development team members towards the end goal of better security.

Runtime, DevOps, or Somewhere in Between?

In most organizations, APIs are developed and published by many different groups, which raises the question of where does the task of securing and managing APIs reside? One school of thought is that API security is the responsibility of developers. While all would agree the task of secure coding is the developers' responsibility, but security beyond that introduces several obstacles. First, it may inject friction into the development process. Second, it might not provide security teams with the data they need to improve protections or assess compliance.

An alternative school of thought is that the security team should own API visibility because it is a foundational step towards finding and eliminating gaps that may lead to incidents if discovered by an attacker, but with fast moving development cycles some APIs can be overlooked leading to gaps in security coverage. The ideal approach must include a runtime API security solution that provides both security and development teams with the means to consistently and accurately answer the following API-related questions:

- How many knowingly published, shadow or deprecated APIs do we have?
- What are they used for, can we see and analyze traffic patterns?

- Do our APIs adhere to specification definitions and how do we maintain conformance?
- Are there any hidden headers, parameters or response codes in our APIs?
- Is encryption enabled for APIs to transmit PII or sensitive data securely?
- Are any APIs accessing regulated data in a way that will jeopardize compliance?

API Security Begins with Runtime Visibility and Monitoring

Effectively protecting your APIs from threats that may lead to data loss, fraud or network compromise begins with visibility – you cannot protect what you cannot see. The stateless nature of APIs combined with the fact that they typically include the entire transaction makes understanding how many APIs you have, their usage patterns and respective risk levels critical API visibility elements that contribute to a strong and comprehensive API security posture.

API Sentinel accelerates the runtime discovery and remediation of external and internal APIs leaking sensitive data, using weak forms of authentication or not conforming to published schemas. Support for Kubernetes integration and a broad set of management APIs allows DevOps and security teams to deploy a comprehensive layer of application security in a wide range of environments including service mesh, data center, cloud or hybrid.

API Sentinel API Visibility and Monitoring Features

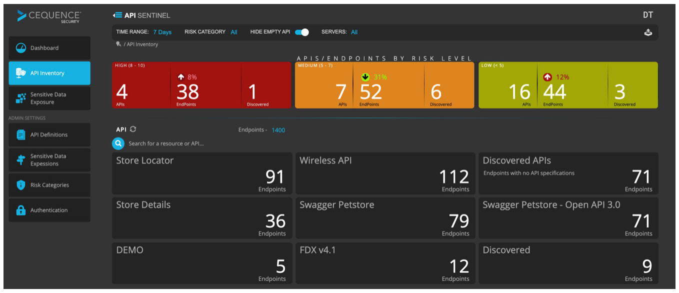
1. Continuous API discovery and inventory.
2. Sensitive data discovery and remediation.
3. Detailed API traffic analysis.
4. Continuous API schema analysis and conformance enforcement.
5. Authentication and access control confirmation.
6. Automatic risk monitoring, alerting and remediation.

API Sentinel Feature Summary

Continuous API Discovery and Inventory

Most organizations struggle to understand how many APIs they actually have. A recent Aite Group report showed that 48% of the surveyed companies could not specify the number of internal or external APIs that had been created, deployed, or managed, with 13% reporting no inventory whatsoever of their internal and external APIs. Listed as #9 in the OWASP API Security Top 10, Improper Asset Management can be the result of shadow, deprecated, end-of-life APIs deployed outside of security view introduce new attack vectors. Additional factors can include the lack of a documented API publication process that allows different groups to publish APIs without oversight.

API Sentinel addresses the glaring need to discover, track and manage APIs with an agnostic approach that integrates with your API management infrastructure, be it a proxy, an ingress controller or a gateway, to provide complete runtime visibility and monitoring of all your APIs – both external and internal. Visibility is all encompassing, discovering APIs with well-published specifications (managed), legacy or future implementations without API specifications (unpublished, pre-production) and those with hidden endpoints or methods not documented in API specifications (shadow APIs). Additional discovery elements include headers and parameters in use.



TIME RANGE: 7 Days RISK CATEGORY All HIDE EMPTY API SERVERS: All

/ API Inventory

APIS/ENDPOINTS BY RISK LEVEL

HIGH (8 - 10): 4 APIs, 38 EndPoints (8%), 1 Discovered

MEDIUM (5 - 7): 7 APIs, 52 EndPoints (31%), 6 Discovered

LOW (< 5): 16 APIs, 44 EndPoints (12%), 3 Discovered

API Endpoints - 1400

Search for a resource or API...

Store Locator 91 Endpoints	Wireless API 112 Endpoints	Discovered APIs Endpoints with no API specifications 71 Endpoints
Store Details 36 Endpoints	Swagger Petstore 79 Endpoints	Swagger Petstore - Open API 3.0 71 Endpoints
DEMO 5 Endpoints	FDX v4.1 12 Endpoints	Discovered 9 Endpoints

Image 1: API Sentinel continuously discovers and tracks your API inventory.

API Sentinel inventory and usage analysis can help identify traffic spikes that may indicate anomalous behavior as outlined in #9 of the OWASP API Security Top 10: Improper Asset Management.

Sensitive Data Discovery and Remediation

Too often, APIs are treated differently from traditional applications when it comes to security and management, so existing best practices may be ignored. A lack of encryption can expose sensitive data, resulting in unwanted publication or discovery of a security gap that can jeopardize regulatory compliance.

Listed as #3 in the OWASP API Security Top 10, Excessive Data Exposure is often caused by a published API exposing more data than it should, relying (too) heavily on the client app to perform the necessary filtering before displaying it to the user.

APIs are all-inclusive, meaning the functionality and the payload are included with each transaction, making the use of encryption a critical, yet sometimes overlooked requirement. Using the default API Sentinel Sensitive Data Dashboard, security and development teams can close the encryption usage security gap before an API is published (or discovered) by identifying endpoints that are transmitting sensitive data (e.g., credit card, social security numbers and custom data patterns) that is subject to PCI, PHI or other PII related compliance mandates. Custom reporting graphically displays APIs the results and can be configured to initiate an alert for remediation using predefined integrations with Slack, PagerDuty, Email and other tools.

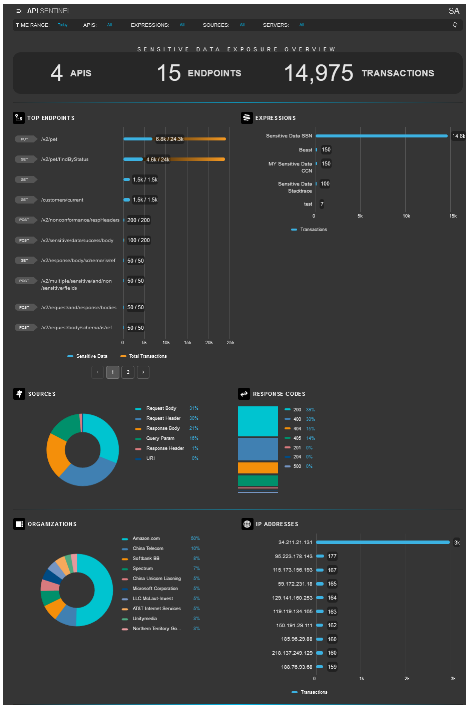


Image 2: The Sensitive Data Dashboard enables discovery and remediation of all APIs that may be leaking sensitive data.

Sensitive data analysis and discovery by API Sentinel can help customers discover and remediate #3 on the OWASP API Security Top 10: Excessive Data Exposure.

API Traffic Analysis

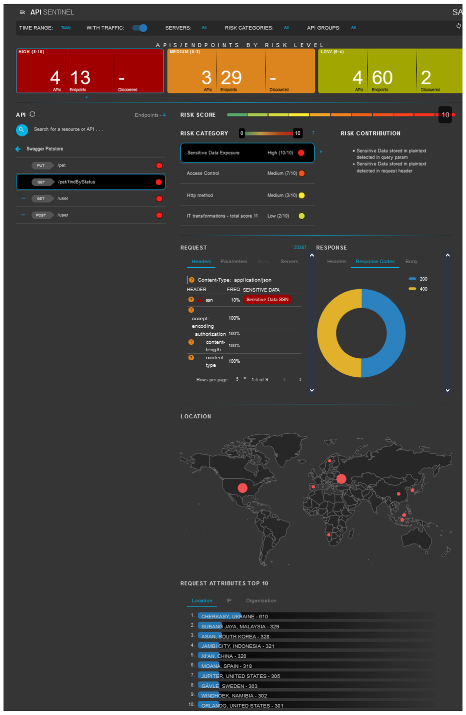
An API inventory can tell you how many APIs exist with the next logical step being a better understanding of the API usage – the volume of traffic, the source, destination as well as details such as headers, response codes and query parameters. With visibility into usage patterns, security teams can identify potentially malicious use and recommend removing those APIs that are inactive.

A lack of visibility into API usage patterns, endpoints, paths, IP addresses, (including country and organization) can result in APIs with Broken Object Level Authorization, #1 on the OWASP API Security Top 10, to go undetected. Enhanced visibility can also uncover traffic spikes that may indicate a lack of, or insufficient rate limiting covered in #4.

API Sentinel provides your security and development team with insight into the breadth of your API footprint, including how every API endpoint, external and internal, is being used. This data helps your security team evaluate ways to reduce attack surface area and minimize your exposure. For all of the APIs discovered by API Sentinel, you can quickly see the API traffic and usage related datapoints:

- What IP addresses are connecting to your APIs?
- Where is the API traffic coming from geographically?
- Which organizations own the IP addresses?
- Is sensitive data exposed in the query parameters?
- What headers are in use/exposed by the API?

Each of these data points provided by API Sentinel is an invaluable decision-making element that your security team can use to begin building an API usage profile. The ultimate goal is to gain tight control over your API footprint and reduce your security exposure. In addition to usage statistics, API Sentinel performs real-time discovery of API endpoint request and response characteristics (e.g., response codes, names of query parameters and headers). Acting as a final check before publication, or as a periodic check against those already published, developers can use visibility into API usage patterns, endpoints, paths, IP addresses (including country and organization) to discover and remediate APIs that have been published with insufficient validation or authorization of an object access request.



Sensitive Data Exposure	High (10/10)
Access Control	Medium (7/10)
Http method	Medium (3/10)
IT transformations - total score 11	Low (2/10)

- Sensitive Data stored in plaintext detected in query param
- Sensitive Data stored in plaintext detected in request header

Content-Type: application/json

HEADER	FREQ	SENSITIVE DATA
ssn	10%	Sensitive Data SSN
accept-encoding	100%	
authorization	100%	
content-length	100%	
content-type	100%	

Rows per page: 5 1-5 of 9

1. CHERKASY, UKRAINE - 610
2. SUBANG JAYA, MALAYSIA - 329
3. ASAN, SOUTH KOREA - 328
4. JAMBI CITY, INDONESIA - 321
5. XI'AN, CHINA - 320
6. MOANA, SPAIN - 318
7. JUPITER, UNITED STATES - 305
8. GÄVLE, SWEDEN - 303
9. WINDHOEK, NAMIBIA - 302
10. ORLANDO, UNITED STATES - 301

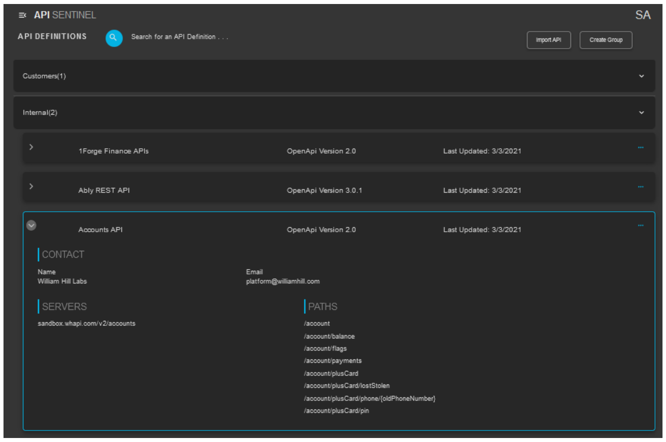
Image 3: API Sentinel continuously tracks API traffic to help discover anomalous traffic patterns.

API Sentinel inventory and usage analysis can help address #1 OWASP API Security Top 10: Broken Object Level Authentication and #4 Lack of Resource and Rate Limiting.

API Schema Analysis and Conformance Enforcement

Moving towards an API-centric development methodology should coincide with the adoption of an API specification framework such as OpenAPI 2.0/3.0, RAML or others. The benefit of using an established framework will be consistent and secure APIs. The challenge most organizations face is centrally enforcing conformance across a widely distributed development team.

Lack of specification conformance exposes your organization to two of the OWASP API Top 10 risks: Mass Assignment (#6) and Security Misconfiguration (#7). Mass assignment occurs when the API includes server-side variables that should be restricted but aren't and can be initialized or overwritten (i.e., user privileges). The result is the discovery of modifiable parameters (user.is_admin) by bad actors who then exploit them by creating new users with administrative privileges. Security misconfiguration is commonly a result of insecure default configurations, incomplete or ad-hoc configurations, misconfigured HTTP headers, unnecessary HTTP methods, permissive Cross-Origin resource sharing (CORS), and verbose error messages containing sensitive information.



Customers(1)

Internal(2)

1Forge Finance APIs	OpenApi Version 2.0	Last Updated: 3/3/2021
Ably REST API	OpenApi Version 3.0.1	Last Updated: 3/3/2021
Accounts API	OpenApi Version 2.0	Last Updated: 3/3/2021

CONTACT

Name
William Hill Labs

Email
platform@williamhill.com

SERVERS

sandbox.whapi.com/v2/accounts

PATHS

/account
/account/balance
/account/flags
/account/payments
/account/plusCard
/account/plusCard/lostStolen
/account/plusCard/phone/{oldPhoneNumber}
/account/plusCard/pin

Image 4: API Sentinel flags non-conforming APIs to eliminate gaps before they are published or discovered.

Using an API specification uploaded from your code repository or pushed from your CI/CD framework tools, API Sentinel continuously analyzes your APIs to identify and flag API endpoints that deviate from published specifications and can potentially be exploited by attackers. Once the API specification has been uploaded to API Sentinel, you can modify the title, owner, description and the server names or create groupings to simplify management.

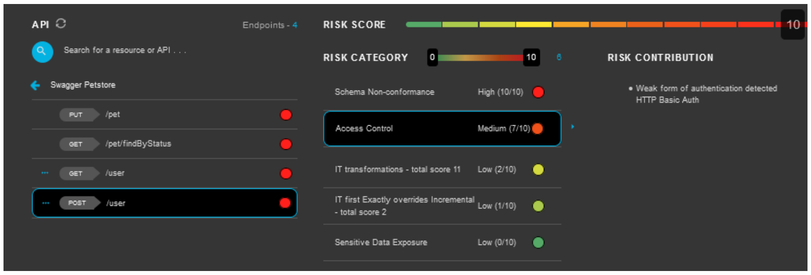
Examples of conformance deviations include weak authentication/access control, sensitive data exposure, and the use of undocumented response codes, headers or query parameters. Once API Sentinel discovers and flags non-conformant elements, they can be addressed by development, eliminating potential security gaps before they are published, or discovered by attackers.

API Sentinel continuously compares your APIs to your OpenAPI specification to help you discover and address security gaps like those outlined in the OWASP API Security Top 10: Mass Assignment and Security Misconfiguration.

Authentication and Access Control Confirmation

Controlling who has access to different resources would seem to be common practice, yet each week it seems a new API related security incident is announced that were the result of poor authentication or access control. Authentication, or the act of validating who you say you are and controlling access to user information should be defined in your API specification to ensure your APIs and the associated data and systems are protected.

Authentication, access control and authorization errors are common enough that they rank #2 and # 5 on the OWASP API Security Top 10. These errors can be introduced by unprotected authentication APIs (login, registration, password reset), use of weak passwords, a lack of encryption or error messages returning too much information.



PUT /pet ●
GET /pet/findByStatus ●
GET /user ●
POST /user ●

Schema Non-conformance	High (10/10)	●
Access Control	Medium (7/10)	●
IT transformations - total score 11	Low (2/10)	●
IT first Exactly overrides Incremental - total score 2	Low (1/10)	●
Sensitive Data Exposure	Low (0/10)	●

- Weak form of authentication detected HTTP Basic Auth

Image 5: API Sentinel flags APIs using weak or non-conforming authentication and access control.

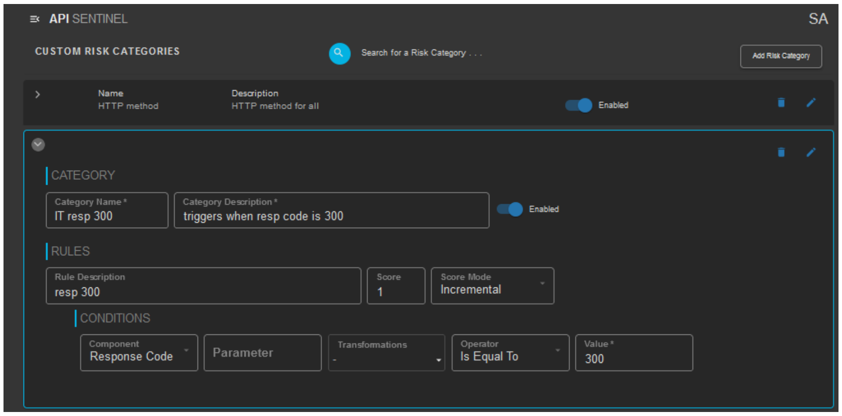
API Sentinel continuously and unobtrusively monitors your APIs to discover endpoints that are using weak forms of authentication and access control, flagging them for remediation by development to eliminate security gaps before they are published or discovered. This runtime approach helps ensure that your APIs, and the data behind them, are accessed only by your intended users and not cybercriminals.

API Sentinel helps address security risks introduced by Broken Level Authentication, #2 and Broken Function Level Authorization #5 on the OWASP API Security Top 10.

Continuous Risk Monitoring and Alerting

APIs allow developers to rapidly bring new features to market, and therein lies the challenge. Speed can introduce errors, resulting in security gaps. Ensuring security and development teams keep pace with API risk levels without injecting friction into the development process becomes a critical requirement for protecting your APIs. Unobtrusively yet continuously monitoring your API risk will help your team achieve a strong yet consistent security posture.

API Sentinel continuously assesses your API security risks based on either predefined criteria for consistency, or customized criteria, specific to your organization's policies and requirements.



CUSTOM RISK CATEGORIES

Search for a Risk Category . . .

Name: HTTP method — Description: HTTP method for all — Enabled

CATEGORY

Category Name *: IT resp 300

Category Description *: triggers when resp code is 300

Enabled

RULES

Rule Description: resp 300

Score: 1

Score Mode: Incremental

CONDITIONS

Component: Response Code

Parameter

Transformations: -

Operator: Is Equal To

Value *: 300

Image 6: API Sentinel allows you to create and manage custom risk categories.

The API risk score ranging from 1-10 is summarized in the dashboard, with high-risk items flagged for action by development. Using predefined criteria includes presence of sensitive data, specification conformance, and authentication levels allowing you to monitor risk levels in a consistent manner.

Customized risk criteria can include items such as headers in use, or response codes, allowing your team to be more granular in determining and managing API risk levels and prioritizing any needed remediation. Each risk category is displayed visually and includes the number of endpoints discovered with drill down for additional analysis. Flagged APIs can initiate an alert for remediation via integration with Slack, PagerDuty, Email or other collaboration tools.

API and Network Ecosystem Interoperability

API Sentinel is deployed as a Kubernetes application in your data center, in managed cloud environments like Amazon EKS and Google GKE or as a SaaS. API Sentinel integrates with your API management infrastructure including CDNs, Proxies, Load Balancers, Ingress Controllers and API Gateways to ensure that all your external and internal APIs are discovered, inventoried, analyzed and tracked, regardless of department owner, or which network infrastructure management infrastructure component they flow through. A broad set of APIs allow you to configure API Sentinel to ingest API specifications from development frameworks, receive API traffic from other network sources, and export data to external tools for analysis and fraud remediation.

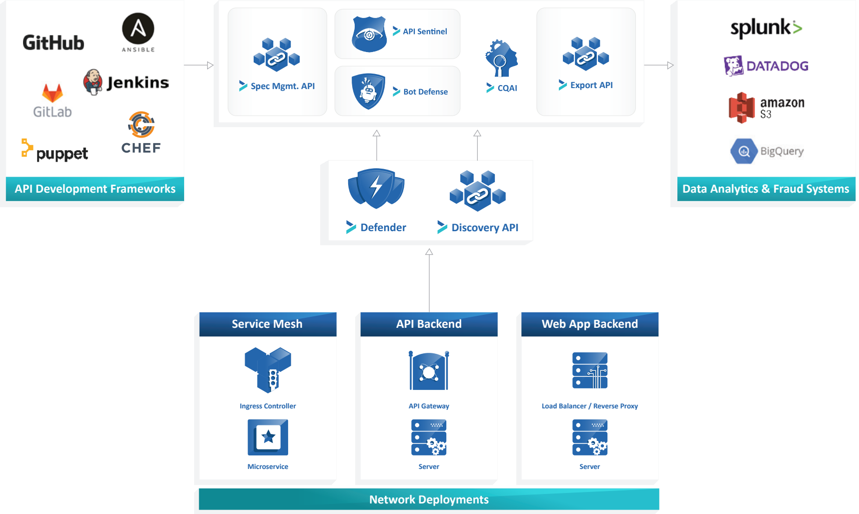


Image 7: API Sentinel integrates with your existing API and network ecosystem to discover and protect all your external and internal APIs.

Summary

Most security professionals are strong supporters of the saying, "Knowledge is Power." With API Sentinel, that knowledge begins with creating an inventory of your growing API footprint begins with continuous, runtime visibility into how many APIs you may have, who is accessing them, where they are located and how they are being used, allowing you to apply that principle to API security. Extending beyond the visibility a comprehensive API inventory ensures security teams can work in partnership with development to provide a continuous risk assessment, uncovering security gaps and addressing them long before they become security incidents.

CEQUENCE® SECURITY

100 S. Murphy Avenue, Suite 300, Sunnyvale, CA 94086
1-650-437-6338, info@cequence.ai, www.cequence.ai