CEQUENCE SECURITY

DATASHEET

Cequence Unified API Protection Solution

Introduction

APIs have become the currency of exchange for everything we do digitally. The apps we use on our devices for work and pleasure, our favorite shopping, money management, and travel web site, all use APIs heavily. Organizations of all sizes are using APIs to increase business velocity and create competitive advantage.

As with all things digital, security risks abound, and APIs are no exception – they are highly visible and well-defined doorways into an organization's data and business processes. Too often they lack sufficient security safeguards and have become the #1 attack target. To ensure business success, security teams must prevent misuse and abuse that can lead to fraud, data loss and business disruption across their APIs as well as their legacy web and mobile applications.

API Security Challenges

Today's security teams lack the visibility and defense capabilities needed to protect their APIs from attacks against perfectly coded APIs and from vulnerability exploits caused by coding errors released to production. Many have adopted a belief that compliance with PCI or SOC 2 combined with a shift left, DevOps mentality supported by existing security technologies is sufficient to identify their API risk surface and exert more management and security controls.

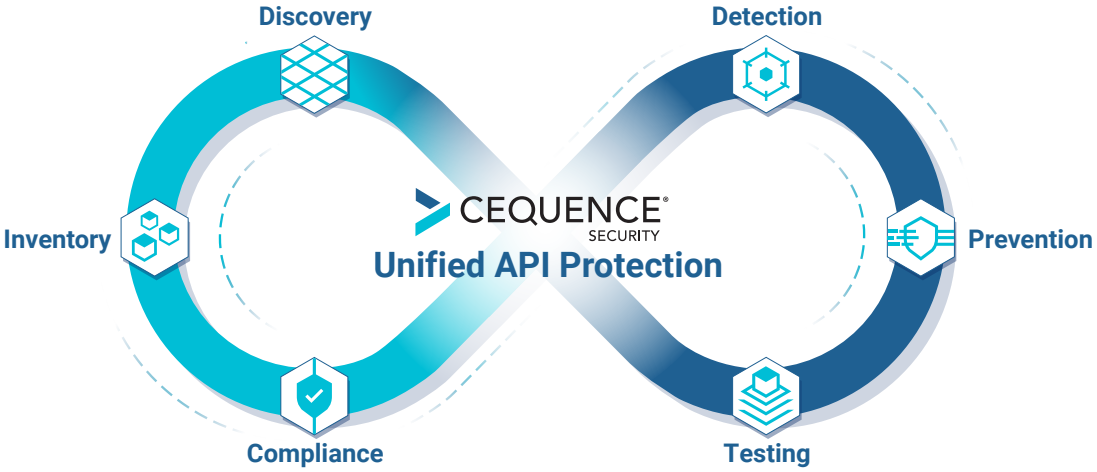
The problem with these strategies is that they don't have a way to "know the unknown", meaning they aren't able to look for all APIs and API vulnerabilities without knowing where to look. Even if all APIs are discovered and "known", attackers can still leverage seemingly legitimate transactions in an attempt to steal data, or commit fraud. Traditional approaches that use WAFs or API gateways depend on easily evadable detection, lack the real-time ability to discern good from bad API activity and are reliant on static, least common denominator protection spread across multiple technology components.

The Ideal Solution: Unified API Protection

The ideal solution is one that addresses every phase of your API security lifecycle, can be deployed quickly without intrusive instrumentation or agents, and scales easily. The solution should provide an outside-in and inside-out view of the API risk surface, enable dynamic vulnerability discovery and remediation while leveraging ML, and threat intelligence to:

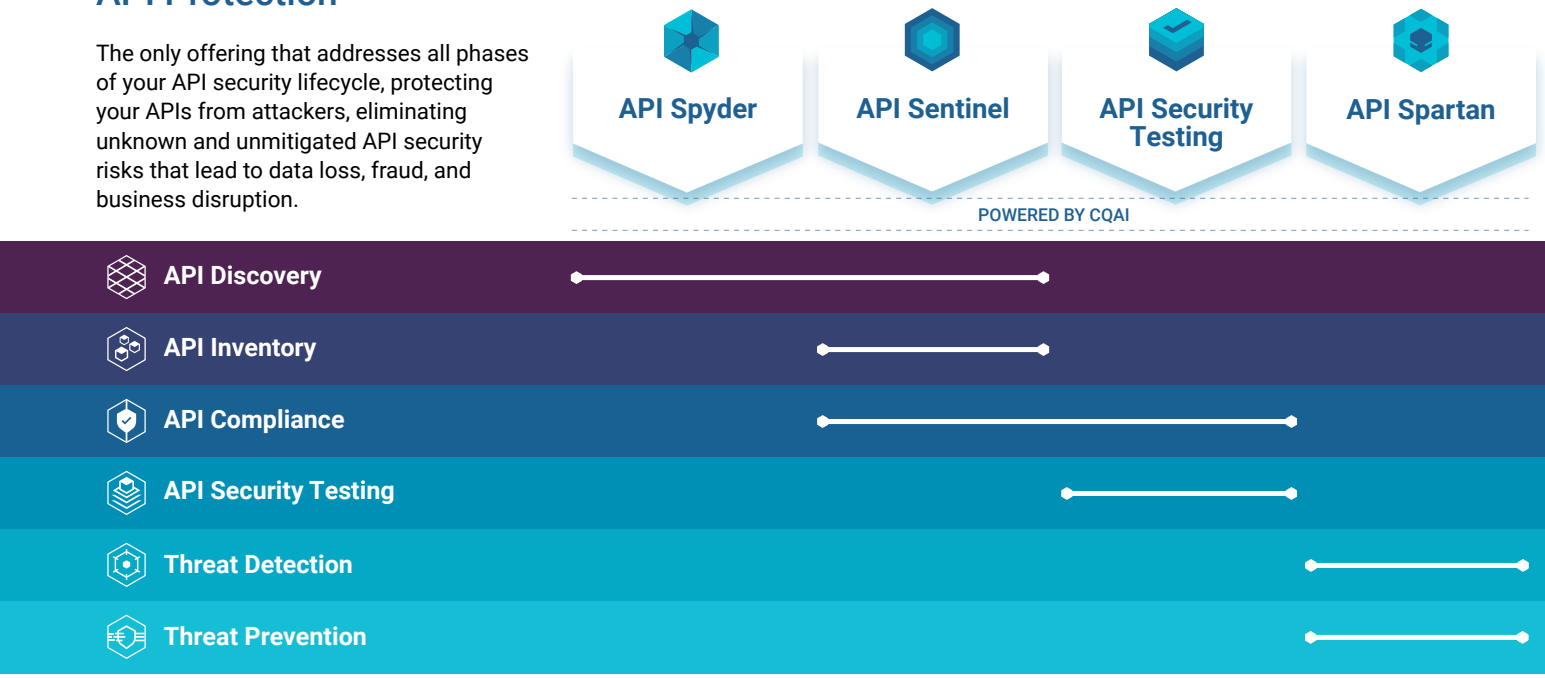
- Discover public-facing APIs and resources, creating a runtime inventory your managed, unmanaged, shadow and zombie APIs.
- Detect vulnerabilities before they become exploits, uncover business logic abuse and API threats hiding in plain sight.
- Mitigate threats with API testing and remediation tasks while blocking attacks natively, in real time, without signaling a 3rd-party solution.

The Cequence Unified API Protection solution is just that.



Cequence Unified API Protection

The only offering that addresses all phases of your API security lifecycle, protecting your APIs from attackers, eliminating unknown and unmitigated API security risks that lead to data loss, fraud, and business disruption.



The Cequence Unified API Protection solution is comprised of:

API Spyder

An API attack surface discovery and management tool that continuously assesses your public facing APIs and resources to show you exactly what an attacker sees from an outside-in perspective. API Spyder discovers public-facing API resources that may be exploitable using vulnerabilities such as Log4j and LoNg4j.

API Sentinel

Provides an inside-out view of your APIs by integrating with any network infrastructure element to create an up-to-the-minute catalog of all your APIs, managed, unmanaged. Predefined risk assessment rules help uncover sensitive data handling, authentication, and specification conformance coding errors.

API Security Testing

Provides security and development teams with a mix of pre-defined, imported or dynamically generated API tests that go beyond the OWASP API Security Top 10+ to help them quickly uncover and remediate API vulnerabilities. View and share test status, summary reports and initiate alerts via email, webhooks and other popular collaboration tools.

API Spartan

Detects and prevents sophisticated automated API attacks and business logic abuse using hundreds of ML rules that leverage an API threat database with billions of malicious behaviors, IP addresses and organizations. Native, policy-based response options ensure that any detected attack is blocked, in real-time, without reliance on a 3rd-party WAF or other security component.

The Cequence Unified API Protection solution is powered by CQAI, an ML-based analytics engine that leverages the largest API threat database of behavioral patterns, known malicious infrastructure and third-party intelligence to accurately detect API threats hiding in plain sight with industry-leading high efficacy rates.

The Cequence UAP enables customers to continuously reap the competitive and business advantages of ubiquitous API connectivity. The Cequence solution results in attack futility, failure, and fatigue for even the most relentless of attackers. It significantly improves visibility and protection while reducing cost, minimizing fraud, business abuse, data losses and non-compliance. Learn more at **www.cequence.ai**

Cequence: Continuous Protection for Ubiquitous API Connectivity

CEQUENCE SECURITY

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