CEQUENCE

Datasheet

Cequence Unified API Protection

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 sites, 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

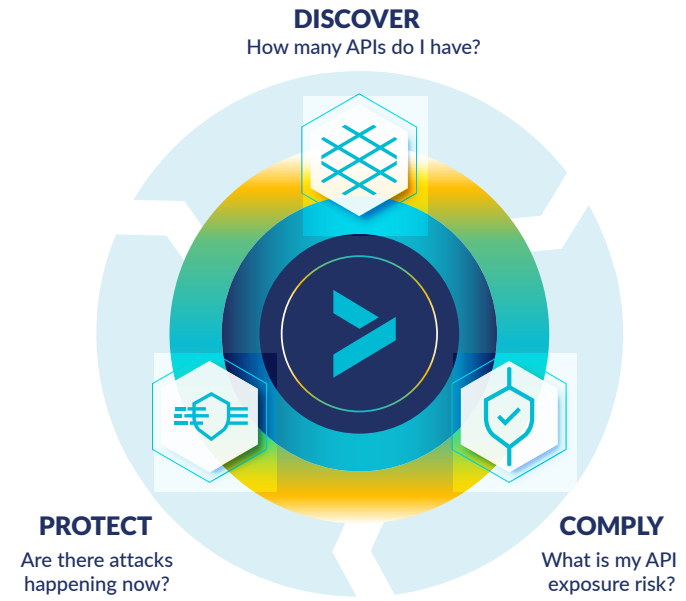
Today's security teams face numerous challenges when it comes to protecting critical APIs and applications from cyber attacks. First, APIs are routinely developed and deployed by disparate teams at lightning speed across numerous cloud providers, creating a "fog of war" that shrouds security team visibility. Discoverable by attackers, these unmanaged and unprotected APIs often contain critical vulnerabilities that can lead to exploited applications and data breaches.

Second, security and development teams do not have a clear and consistent picture of the security posture of their APIs across their application footprint. Understanding where a critical vulnerability, sensitive data exposure, or business logic flaw can be exploited empowers security teams to work with development teams to pinpoint areas of security risk for immediate remediation.

Third, API applications are under constant attack with attackers seeking to find any opportunity to exploit an application and in turn, compromise your organization. The ability to detect and block attacks as they occur can prevent organizations from experiencing fraud, data exfiltration, and business disruption.

Security leaders are now asking three fundamental questions:

1. How many APIs do I have?
2. What risks do my APIs pose?
3. Are my APIs under attack?



The Ideal Solution: Unified API Protection

To address these security challenges, a security solution must provide a complete discovery of your entire API attack surface that includes both external and internal APIs, understands your API risk posture pinpointing where you need to remediate critical security vulnerabilities, and provides real-time protection that blocks API attacks before they reach your application.

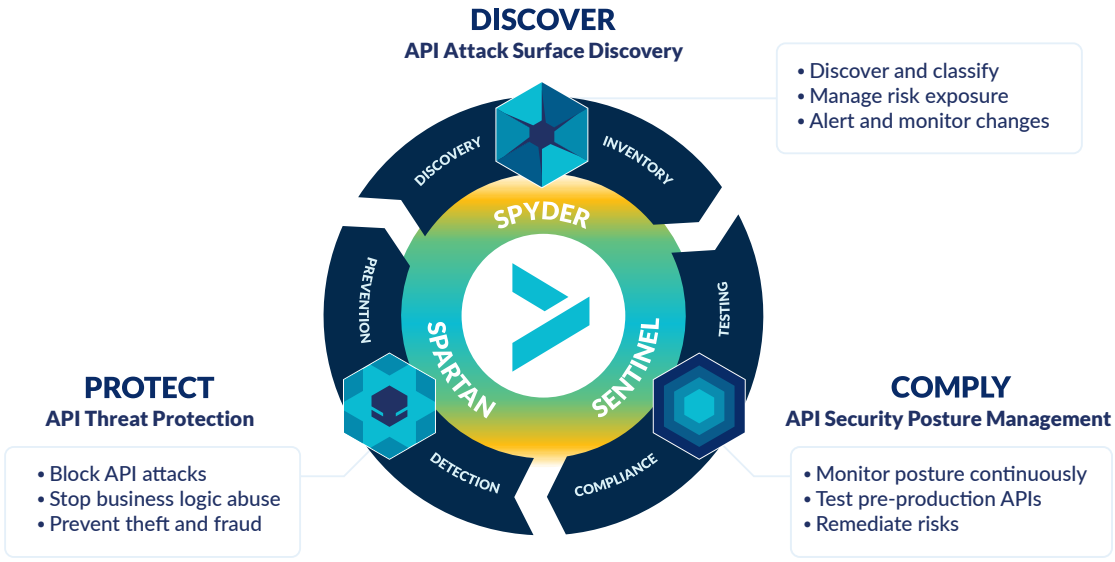
The solution should provide the following capabilities:

- **DISCOVER** Identify all external and internal APIs, ensuring you have visibility into the complete API attack surface of your organization.
- **COMPLY** Ensure that APIs comply with API specifications, security test requirements, and governance best practices.
- **PROTECT** Detect and block API threats in real time that target your APIs and applications, with minimal false positives.

The Cequence Unified API Protection solution provides exactly that.

The Cequence Unified API Protection Solution

The Cequence solution is the only security offering that addresses all phases of your API protection lifecycle, discovers your entire API attack surface, eliminates unknown and unmitigated API security risks, and protects your APIs from cyber attacks that lead to data loss, fraud, and business disruption.



DISCOVER with

API Spyder

An API attack surface discovery management product that provides visibility of publicly-accessible APIs and their vulnerabilities, giving you an attacker's view of your organization. API Spyder continuously reveals new API servers, endpoints, and hosting providers so that security and compliance teams are aware of their existence.

COMPLY with

API Sentinel

An API security posture management solution that discovers an organization's complete API footprint, ensures APIs are compliant, conforming to security and governance best practices, and provides GenAI-powered API testing to identify vulnerabilities and prevent data leakage before production.

PROTECT with

API Spartan

Detects and prevents sophisticated automated API attacks and business logic abuse using hundreds of ML rules that leverage an API threat database containing billions of malicious behaviors, IP addresses, and organizations. Native, policy-based response options ensure that any detected attack is blocked, in real time, without relying on third-party WAFs, API gateways, or load balancers for mitigation.

The Cequence Unified API Protection solution 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, data loss, non-compliance, and business disruption. Learn more at **www.cequence.ai**

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