CEQUENCE

Datasheet

Cequence Unified API Protection

API Security and Bot Management Platform

Introduction

We interact with applications in our daily lives in myriad uses from shopping to banking to healthcare and those applications use APIs to interface internally and externally with web apps, mobile apps, even behind-the-scenes microservices. The meteoric growth in API use has seen a corresponding rise in security risks given that APIs are highly visible and well-defined doorways into an organization's data and business processes. Too often they lack sufficient oversight and security safeguards, making them a top target for attackers. Security teams need effective tools and processes in place to prevent API abuse that can lead to fraud, data loss, and business disruption.

API Security and Bot Management Challenges

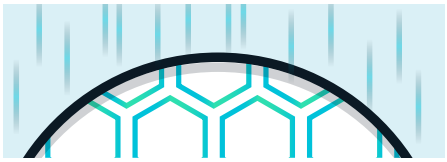
Today's security teams face unique, cross-functional challenges when it comes to protecting critical APIs and applications from cyber attacks.

Lift the Fog

APIs are routinely developed and deployed by disparate teams at lightning speed across a mix of on-premises and cloud infrastructure, creating a "fog of war" that shrouds security team visibility. Discoverable by attackers, these unmanaged and unprotected APIs often contain critical vulnerabilities that lead to exploited applications and data breaches.

Maintain Good Posture

Security and development teams do not have a clear and consistent picture of the security posture of their APIs across their application portfolio. Understanding where a critical vulnerability, sensitive data exposure, or business logic flaw can be exploited empowers security teams on remediating pinpointed areas of security risk.



Protect the Core

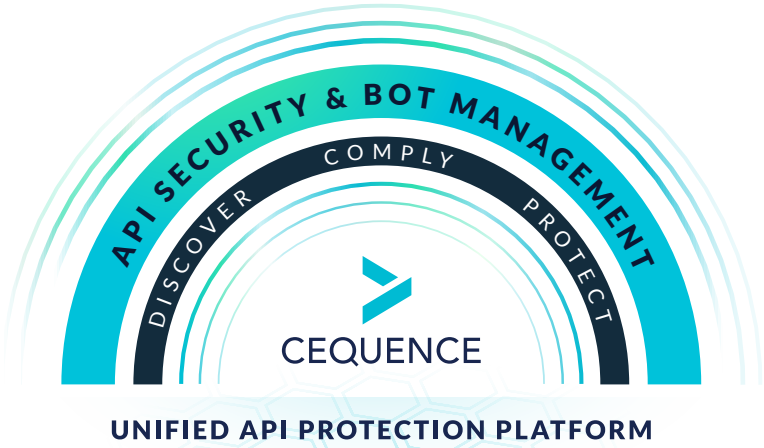
API applications are constantly probed by attackers seeking any opportunity to exploit an application and compromise your organization. The ability to detect and block attacks as they occur can prevent organizations from experiencing fraud, data exfiltration, and business disruption.

Security leaders are now asking fundamental questions:

1. How many APIs do I have and where are they?
2. What risks do my APIs pose?
3. Can I protect *all* of my APIs and applications?
4. Are my applications and APIs under attack?

Answering these questions is critical to a robust security program, a task made more difficult due to the nature of business. New product launches, organic growth, and acquisitions all require a solution capable of keeping up with this constant change.

The Cequence Unified API Protection Platform



To address these security challenges, the ideal solution must continuously engage in complete discovery of your entire API attack surface that includes both external and internal APIs, understand your API risk posture pinpointing which critical security vulnerabilities need remediation, and provide real-time protection that detects and blocks attacks before they reach your applications.

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 applications and APIs from cyber attacks that lead to data loss, fraud, and business disruption.

The Cequence Unified API Protection platform enables customers to continuously reap the competitive and business advantages of secure applications and 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**.

DISCOVER

API Attack Surface Discovery

Discover internal and external APIs | Alert and monitor changes

Discover and inventory your organization's entire API footprint cataloging internal, external, and third-party APIs. Form a coherent picture of your publicly-accessible attack surface, giving you an attacker's view of your organization. Cequence continuously reveals new API servers, endpoints, and hosting providers so that security and compliance teams are aware of their existence.

COMPLY

API Security Posture Management

Monitor posture continuously | Test pre-production APIs | Remediate risks

Manage your organization's API security posture, ensuring its complete API footprint is compliant, conforming to specifications, security test requirements, and governance best practices. Autonomous API test creation identifies vulnerabilities and prevents sensitive data leakage prior to production.

PROTECT

Bot Management & Fraud Prevention

Block application & API attacks | Prevent theft, business logic abuse, fraud

Identify and mitigate bots and prevent fraud, protecting your organization and its applications from the full range of automated attacks. Requiring no agents, JavaScript, or SDKs, multi-dimensional behavioral fingerprints enable identification of even the most sophisticated attacks. Native, real-time blocking ensures protection against business logic attacks, exploits, automated bot activity, online fraud, OWASP API Security Top 10 attacks, and much more.

CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai