CEQUENCE

Datasheet

Cequence Unified API Protection for Retail

Protecting Retail Organizations Against Application & API Attacks

Introduction

The retail industry has undergone dramatic changes over the years, driven by advances in technology, shifts in consumer behavior, and globalization. Omnichannel retail now engages customers across multiple digital and physical touchpoints, striving to provide a seamless and consistent brand experience regardless of whether they are shopping in-store, online, or via a mobile app. Digital wallets like Apple Pay, Google Pay, and others have made checkout faster and more convenient. With these shifts have also come significant changes in retail supplier and partner relationships, depending on a real-time flow of data-driven insights and decision-making capabilities. With all these changes come an exponential increase in cybersecurity threats that puts customer relationships and the organization's financial well-being at risk, necessitating a fresh approach to how applications and APIs are protected.

Application and API Security Challenges

Today's security teams face numerous challenges when it comes to protecting critical applications and APIs from cyber attacks. First, 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 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 portfolio. Understanding where a critical vulnerability, sensitive data exposure, or business logic flaw can be exploited empowers security teams to work with development teams to remediate pinpointed areas of security risk.

Third, 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. How can I protect all of my applications and APIs from abuse and 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.

Retail Use Cases

Account Takeover (ATO)

Content Scraping

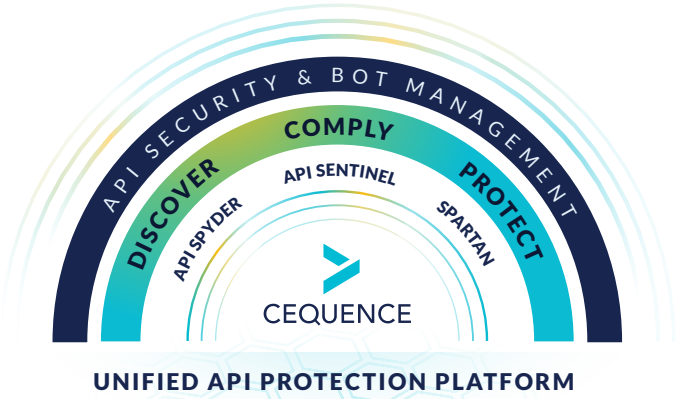
Fake Account Creation

Loyalty Program & Gift Card Abuse

Inject Attacks

Flash / Hype Sale Protection

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, discovering your entire API attack surface, eliminating unknown and unmitigated API security risks, and protecting 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 with API SPYDER

API Attack Surface Discovery

Discover and classify | Manage external exposure | Alert and monitor changes

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

API Security Posture Management

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

An API security posture management solution that discovers an organization's complete API footprint, ensures APIs are compliant, conforming to specifications, security test requirements, and governance best practices, and provides autonomous API test creation to identify vulnerabilities and prevent data leakage before production.

PROTECT with SPARTAN

Bot Management & Fraud Prevention

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

A bot management and fraud prevention solution that protects organizations and their applications from the full range of automated attacks. Requiring no agents, JavaScript, or SDKs, it utilizes multi-dimensional behavioral fingerprints to identify and natively block attacks in real time. It mitigates business logic attacks, exploits, automated bot activity, online fraud, OWASP API Security Top 10 attacks, and much more.

Protecting Top Global Retail Brands

$10T Business value protected

8B Daily API transactions secured

3B User accounts safeguarded

ULTA BEAUTY · narvar · POSHMARK · houzz · e-global

CEQUENCE

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