

Cequence Unified Application Protection for Retail

Protecting Retail Organizations Against Application, API, and AI Attacks

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 organizations face unique, cross-functional challenges when it comes to protecting critical applications and APIs from cyberattacks. It's not just an IT or security problem; malicious bot attacks on applications and APIs can affect ecommerce, customer satisfaction, marketing and sales analytics, and more.

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 visibility. Teams must know what APIs exist, where they are, who has access, and ensure they have accurate specifications. Failing to do so allows attackers to discover unmanaged and unprotected APIs containing critical vulnerabilities that can lead to exploited applications and data breaches.

Further, security and development teams do not have a clear and consistent picture of their API security posture across their application portfolio. Understanding where a critical vulnerability, sensitive data exposure, or business logic flaw can be exploited enables security teams to work with development teams to remediate pinpointed areas of security risk.

Last, Applications and APIs are constantly probed by attackers seeking any opportunity to exploit them and compromise your organization and its data. 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?
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.

Retail Use Cases



Account Takeover
(ATO)



Content
Scraping



Fake Account
Creation



Loyalty Program &
Gift Card Abuse



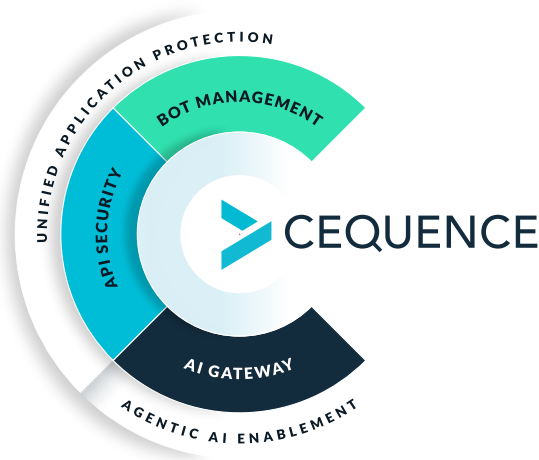
Inject
Attacks



Flash / Hype Sale
Protection

The Cequence Unified Application Protection Platform

The Cequence Unified Application Protection (UAP) platform unites discovery, compliance, and protection to defend an organization's applications and APIs against attacks, business logic abuse, and fraud. Cequence UAP 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. Cequence UAP delivers value in minutes rather than days or weeks and offers a flexible deployment model that requires no app instrumentation or modification.



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 hosts, endpoints, and hosting providers to keep security and compliance teams in the know.

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, malicious bots and AI agents, online fraud, OWASP API Security Top 10 attacks, and much more.

Works with Cequence AI Gateway

The Cequence AI Gateway enables agentic AI access to any internal, external, or SaaS application, in minutes, without coding. API Security can automatically create enhanced API specs that the AI Gateway uses to create MCP servers, eliminating significant manual effort.

Protecting Top Global Retail Brands

\$10T Business value protected



8B Daily API transactions secured



4B User accounts safeguarded

