CEQUENCE

Datasheet

Cequence API Security

API Security Posture Management, Testing, and Remediation

Today's software-driven world runs on applications connected through APIs. These APIs provide access to an organization's network and sensitive data, becoming a top target for attackers. Organizations need visibility and control over their API footprint as part of a robust security program. The rapid proliferation of APIs has exposed a broad range of security challenges that can lead to data loss, compliance violations, and fraud:

- Shadow, hidden, deprecated, and third-party APIs
- Exposure of confidential or sensitive data
- Coding errors that lead to privilege escalation
- Business logic abuse

These challenges require a purpose-built solution that can discover and inventory new and existing APIs, assess them for compliance with specifications and applicable regulations, and protect them throughout their lifecycle – from development to production.

Cequence API Security at a Glance

- **Complete API discovery** through infrastructure integration and/or inline sensors and domain scanning
- **Sensitive data** masking, exposure detection, and leakage prevention
- **Continuous risk visibility** identifying coding errors and misconfigurations
- **Integrated API security testing** in pre-production and runtime
- **Application and API protection** to prevent data loss, theft, and fraud

API Security Overview

Cequence discovers, monitors, and tests APIs, assessing a broad range of risks that often lead to compliance or governance issues, data loss, and business disruption. Providing complete visibility and monitoring of internal and external APIs, Cequence helps organizations keep up with API and service changes, uncovers sensitive data exposure, and identifies OWASP API Security Top 10 vulnerabilities and security risks. API security testing is a core component of API Security, enabling organizations to test their pre-production and runtime APIs against specifications – and automatically generate them if specs are not available. API Security can be deployed as SaaS, on-premises, or hybrid.

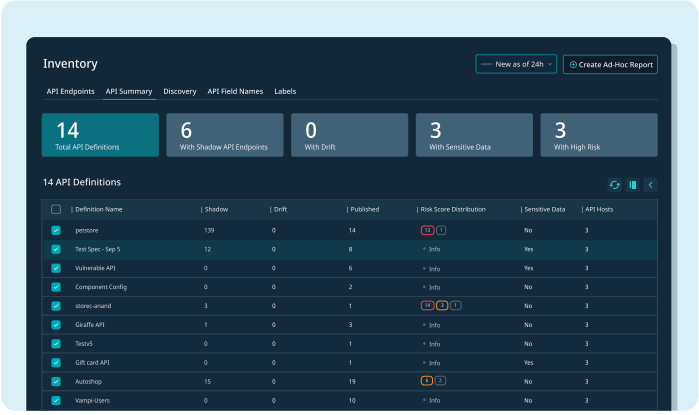
Cequence enables organizations to:

- **Discover all APIs** in use including shadow and zombie APIs without requiring API specifications
- **Gain insight into API usage**, including geographical location, headers, query parameters, and body elements
- **Automatically generate** OpenAPI specifications from discovered APIs and ensure compliance
- **Dynamically assess risk** based on predefined and customizable OWASP API Security and Automated Top 10 Risk categories
- **Test APIs in pre-production environments** with synthetic traffic to surface OWASP and other risks
- **Protect APIs from attacks** through integration with third-party infrastructure like WAFs and API gateways

Cequence API Security Features

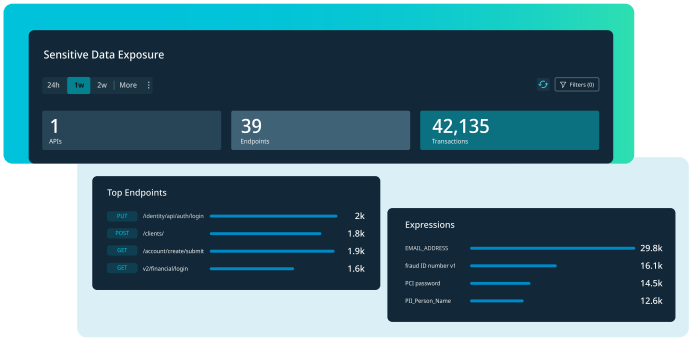
Gain Complete & Continuous API Footprint Visibility

One of the biggest API security challenges organizations face is knowing what APIs they have, where they are, and who has access. Cequence takes a unique approach to providing full and continuous visibility to an organization's runtime API footprint by deploying at the network level with purpose-built sensors as well as integrating with your existing infrastructure including CDNs and API gateways. Cequence API Security also provides an outside-in perspective, scanning your domains and subdomains to identify public-facing API hosts and endpoints even if they're not in use. This "attacker's view" technique also discovers edge, infrastructure, and hosting providers.



Continuous discovery, inventory tracking, and risk categorization help you reign in your API footprint

API Security requires no server- or client-side agents, JavaScript, or SDK integration, ensuring API discovery is not limited to software that has been instrumented, which also eliminates downstream penalties such as extended development cycles, slow page loads, and increased cloud costs. The solution creates a runtime API catalog and automatically generates API specs if they don't already exist, dramatically reducing manual efforts. Dashboards display APIs categorized by risk with drill-down metrics that include the geographic distribution of API usage by country, IP address, and organization.

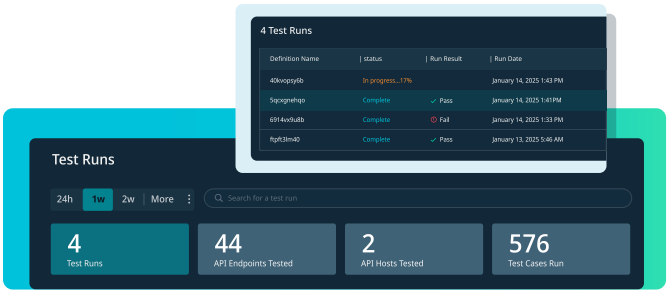


Avoiding Sensitive Data Exposure

Cequence includes a Sensitive Data Exposure dashboard to quickly identify and remediate API endpoints transacting sensitive data based on predefined (e.g., credit card or social security numbers) and customizable data patterns. Natural Language Processing (NLP) machine learning complements predefined patterns and reduces false positives by identifying sensitive data through contextual clues such as the presence of keywords close to the actual detected value. The results are graphically displayed in an interactive dashboard with details such as the API source and response codes leaking the data, the pattern found, and the underlying IP address details. Notifications can be sent to development teams for rapid remediation using predefined alerts for tools such as Slack, PagerDuty, or email. Cequence also provides sensitive data masking, which is applied before the product sees the data, ensuring sensitive data stays private.

Intelligent API Security Testing

Cequence enables IT and development teams to thoroughly test their APIs in pre-production and runtime, identifying coding errors, vulnerabilities, and other deviations from specifications. If specifications are not available, autonomous test creation generates API specs without human involvement, potentially eliminating hours or weeks of manual work. These security testing capabilities can be integrated into the CI/CD pipeline and IDEs, or run stand alone as needed at runtime.



Visualize API Traffic Flows

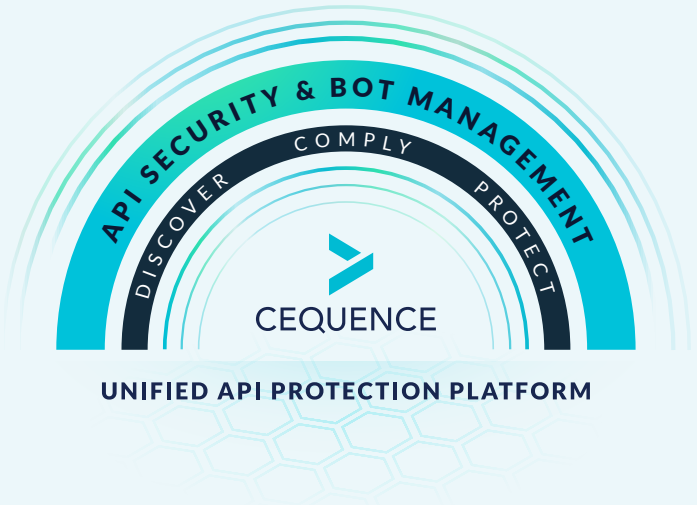
Cequence Flow Graph visualizes interactions between APIs, enabling users to see APIs communication flows. Identify internal and third-party APIs and their dependencies. Validate approved interactions, detect anomalies and gaps in security posture, and discover shadow and rogue APIs.

Protect APIs from Threats and Attack

Cequence protects web, mobile, and API applications from attacks to prevent data loss, theft, and fraud. ML-powered threat detection and analytics and integration with third-party defensive solutions such as WAF and API gateways ensures protection against even the most sophisticated attacks. Cequence Bot Management provides native mitigation including blocking, logging, rate limiting, header injection, and deception.

API Security is Part of the Cequence Unified API Protection Platform

The Cequence Unified API Protection platform unites discovery, compliance, and protection to defend an organization's applications and APIs against attacks, business logic abuse, and fraud. Demonstrating value in minutes rather than days or weeks, Cequence offers a flexible deployment model that requires no app instrumentation or modification. Cequence solutions scale to meet the needs of the largest and most demanding private and public sector organizations, protecting billions of user accounts and billions more daily API interactions.



CEQUENCE

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

© 2025 Cequence Security, Inc. All rights reserved.