

# Cequence API Security

## Application, API, and AI Protection Platform

Modern applications run on APIs, and their numbers have climbed sharply as organizations move to the cloud and deepen partner integrations. Agentic AI accelerates that growth; AI agents call APIs directly and through MCP servers, multiplying the connections enterprises must secure. Visibility and control over this expanding API footprint underpin both a sound security program and regulatory compliance. Without them, organizations face security gaps that drive data loss, compliance violations, and fraud:

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

These challenges require a 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.

### 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, external, and third-party 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 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
- ✓ **Built-in AI Assistant and MCP Server** to guide practitioners and enables headless control

# Cequence API Security Features

## AI-First Architecture with Built-in AI Assistant and MCP Server

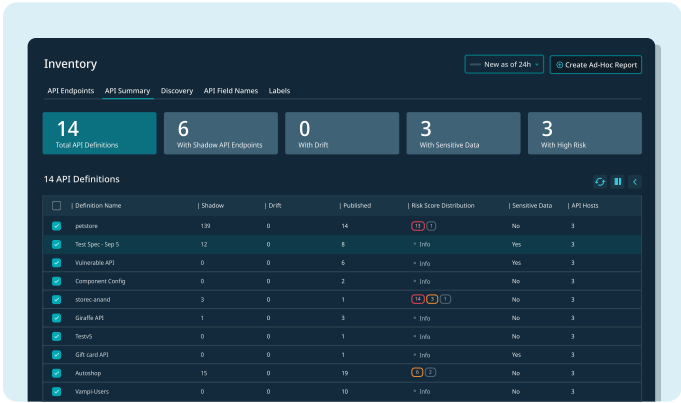
API Security exposes every product capability as MCP tools, allowing teams to drive the platform using plain language rather than through the user interface alone. The built-in AI Assistant answers questions such as “which risks are the most critical right now?” and “which public APIs are transacting sensitive data?” and returns ranked, evidence-backed findings. Practitioners act on those findings in the same conversation, enabling or disabling risk rules, adding authentication types, suppressing sensitive data patterns, changing status, and generating compliance reports without navigating the UI. Teams without dedicated API security expertise gain a knowledgeable guide, and teams running their own AI workflows gain a platform their agents can query, configure, and act through directly.

This open design sets the Assistant apart from chatbots bolted onto closed products. Any MCP-capable agent, SOAR platform, or automation workflow connects through an open API contract with no custom integration, so the assistant extends the agentic ecosystem an organization already runs. Governance is built in: read actions run freely, while every write requires human-in-the-loop approval that shows the exact change before it happens. The agent transparently exposes its reasoning and the underlying tool calls on every turn; when it lacks the tool for a request, it says so rather than guessing, and it confirms that its own changes took effect.

## 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 traffic sensors as well as integrating with your existing infrastructure such as 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.

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. API Security scales to the largest enterprise API estates, loading every view in seconds even across millions of endpoints while running on a smaller compute footprint that can reduce on-premises deployment costs.



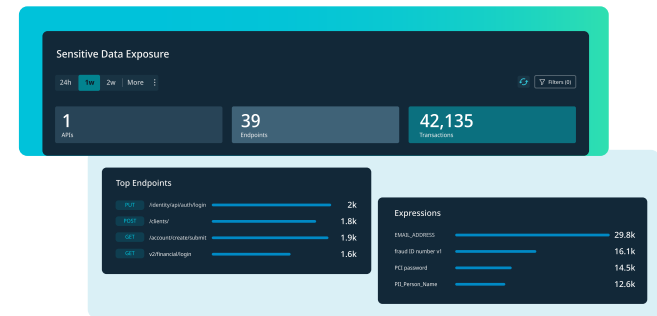
Continuous discovery, inventory tracking, and risk categorization help you reign in your API footprint

## Compliance-ready Risk Rules and Reporting

Cequence delivers audit readiness, shipping a library of more than 250 pre-built risk rules mapped to 25 global frameworks, including every version of the OWASP API Security Top 10, the OWASP Web Top 10, PCI DSS, GDPR, HIPAA, SOC 2, ISO 27001, NIST CSF, LGPD, and SAMA, with additional regional frameworks across the Americas, EMEA, and APAC. Audit-ready reports generate in a single click; each report builds from live data, maps findings to a framework's specific controls, scores risk by control area, and provides remediation guidance for every gap, with company or partner branding. An observe mode scores new rules without raising formal issues, and a test panel validates any rule against sample request and response data before activation, so teams can add and test frameworks without a flood of unreviewed findings.

## Avoiding Sensitive Data Exposure

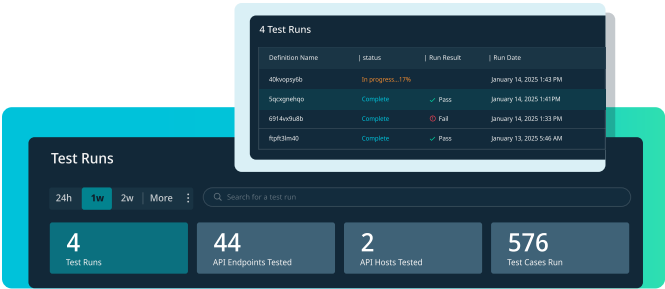
Cequence includes powerful features to prevent sensitive data exposure. Its baselining capability discovers APIs and understands their business context within hours of deployment, identifying APIs that transact sensitive information. Cequence automatically detects sensitive data based on both on predefined (e.g., credit card or social security numbers) and customizable data patterns. Sensitive data patterns are supported worldwide – Cequence



can automatically differentiate between a US driver's license number from a Saudi National ID Card ID number, for example. 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 Sensitive Data Exposure dashboard displays results graphically 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, and email. Cequence also provides sensitive data masking with format preserving encryption (FPE), 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.



### 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, rate limiting, header injection, and deception.

### 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 API specs that the AI Gateway uses to create MCP servers, eliminating significant manual effort.

## API Security is Part of the Cequence Platform

Cequence protects the applications and data that power enterprises in the agentic era. More than a decade of bot defense and API security experience has established Cequence as the leader of safe and secure agentic AI adoption. The Cequence platform delivers deep insight into user, entity, and agent behavior, enabling organizations to secure and control agentic AI workflows while protecting against bad actors and rogue agents. Cequence delivers value in minutes rather than days or weeks with a highly scalable, no-code approach. Trusted by the largest and most demanding private and public sector organizations, Cequence protects more than 10 billion daily API interactions and 4 billion user accounts.

