akto

Solution brief

Akto for FedRAMP: RA-5 Vulnerability Scanning

API Security for FedRAMP

RA-5 FedRAMP Requirements:

FedRAMP requires CSPs to regularly conduct vulnerability scans to detect and address security issues. This is crucial for maintaining the confidentiality, integrity, and availability of federal information systems and data, and for ensuring that CSPs meet the rigorous security standards mandated by the government.

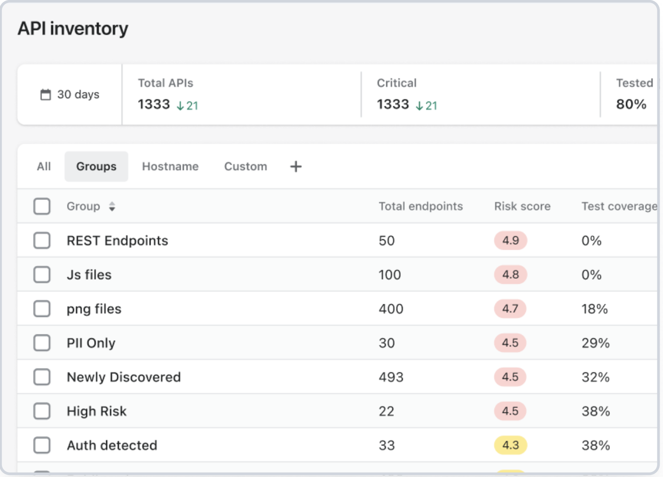
Control	Requirement	Baseline
RA-5	Scan for vulnerabilities in information systems and hosted applications; analyze & remediate vulnerabilities; share report	Moderate, High
RA-5 (1) - Update Tool Capability	Employ tools that can update vulnerabilities to be scanned as new vulnerabilities are discovered.	Moderate, High
RA-5 (2) - Update Frequency	Update vulnerabilities scanned at defined frequency, prior to a new scan, or when new vulnerabilities are reported.	Moderate, High
RA-5 (3) - Coverage	Employ scanning procedures identifying the breadth and depth of coverage.	Moderate, High
RA-5 (4) - Discoverable Information	Determines what information about the information system is discoverable by adversaries and takes correcting action.	High
RA-5 (5) - Privileged Access	Implement privileged access authorization for selected vulnerability scanning activities.	Moderate, High
RA-5 (6) - Automated Trend Analyses	Employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in results.	Moderate, High
RA-5 (8) - Review Audit Logs	Review historic audit logs to determine if a vulnerability has been previously exploited (required for high scan findings).	Moderate, High
RA-5 (10) - Correlate Information	Correlate output from scanning tools to identify multi-vulnerability/multi-hop attack vectors.	High

How Akto can help?

1. Continuous Discovery of APIs

Akto aids CSPs in complying with FedRAMP's RA-5 (5) controls by offering automated, real-time API discovery (both internal and external APIs) and monitoring. This replaces manual swagger file updates with an automatically generated, up-to-date swagger file. Akto also proactively alerts users about new or modified APIs, thus enhancing API security risk management.

Akto enhances CSP's compliance with FedRAMP standards by identifying sensitive data exposures through APIs. It identifies sensitive data such as email, SSN, credit card information assisting teams in meeting the ongoing vulnerability management requirements.



API inventory

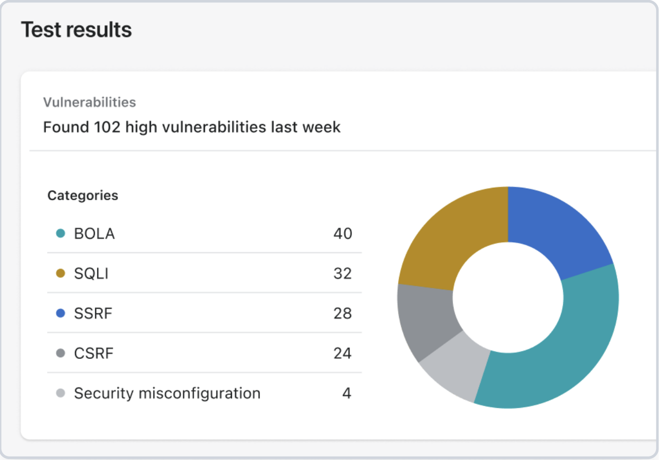
30 days	Total APIs	Critical	Tested
	1333 ↓21	1333 ↓21	80%

□	Group	Total endpoints	Risk score	Test coverage
□	REST Endpoints	50	4.9	0%
□	Js files	100	4.8	0%
□	png files	400	4.7	18%
□	PII Only	30	4.5	29%
□	Newly Discovered	493	4.5	32%
□	High Risk	22	4.5	38%
□	Auth detected	33	4.3	38%

2. API Vulnerability Scanning

Akto helps CSPs meet RA-5 requirements through its powerful API vulnerability scanning capability. Akto's vulnerability database is the most comprehensive in the industry. It covers all aspects of the latest OWASP Top 10 and HackerOne Top 10 ensuring complete coverage. We are particularly distinguished for our advanced test suites focusing on broken authentication and authorization. Akto maps each vulnerability discovered with associated CWE and related CVEs to give context of the finding to the developer.

1. Akto's dedicated security team is committed to ensuring the highest standards of API security. Our team regularly updates our extensive Test Library ensuring the most current and comprehensive coverage.
2. Akto provides the flexibility to select from these pre-existing 200+ templates or to create custom templates tailored to organization's needs



Test results

Vulnerabilities

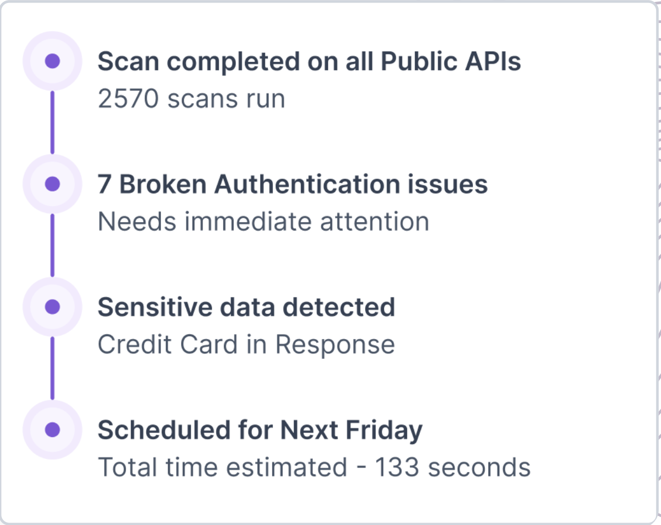
Found 102 high vulnerabilities last week

Categories

	Category	
●	BOLA	40
●	SQLI	32
●	SSRF	28
●	CSRF	24
●	Security misconfiguration	4

4. Reporting with sharing trends

Akto enhances compliance with FedRAMP's RA6 and RA2 controls through its detailed reporting and insights into historical vulnerability trends. It equips security teams with a complete overview, encompassing the discovery timeline, severity, exploit specifics, and remediation recommendations for each vulnerability



Scan completed on all Public APIs
2570 scans run

7 Broken Authentication issues
Needs immediate attention

Sensitive data detected
Credit Card in Response

Scheduled for Next Friday
Total time estimated - 133 seconds

Complete Coverage of RA-5 Controls (APIs and Web Application)

Teams can opt for a self-hosted deployment, ensuring all data remains within their VPC for enhanced security and control. Alternatively, Akto's SaaS model provides convenience by processing data on Akto's servers. Designed for shift-left API scanning, Akto integrates seamlessly into development workflows, providing detailed scan results at the Pull Request level. This empowers teams with actionable insights, thereby streamlining the developer's role in maintaining robust API security.

✓ **RA-5** Akto scan for vulnerabilities in hosted APIs; analyze & remediate vulnerabilities; share report

✓ **RA-5 (1)** Akto maintains a continuously updated database of vulnerabilities, ensuring that new discoveries are promptly incorporated into the scanning process.

✓ **RA-5 (3)** Akto covers latest OWASP Top 10 and HackerOne Top 10 ensuring depth and breadth of coverage.

✓ **RA-5 (4)** Akto maintains a dynamically updated catalog of APIs, adeptly identifying sensitive data transmitted via API responses.

✓ **RA-5 (5)** Users can input tokens for authenticated scans, available in both manual and automated modes. Akto also automates permission generation for API authorization scans.

✓ **RA-5 (6)** Akto offers comprehensive reporting, including historical trend analysis, designed for efficient sharing among teams.

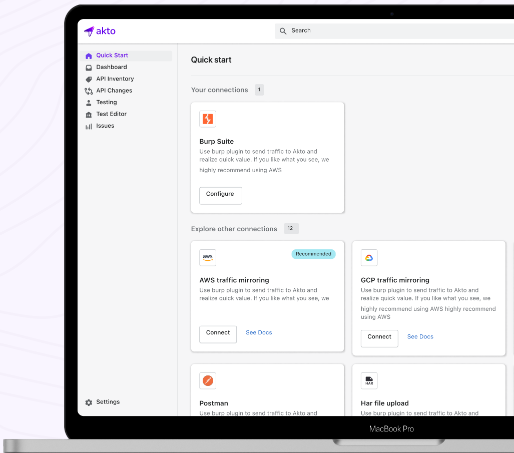
How to get Started with RA-5 using Akto?

It only takes a few minutes to deploy and get started with Akto. You can do a self hosted deployment of Akto in your environment through easy Kubernetes helm chart or find a way that works for your organization from documentation. For comprehensive onboarding assistance, reach out to support@akto.io

Protect your APIs today from attacks with Akto's proactive answer to API Security. See for yourself with a free trial. Select from the options below.

Start with Cloud version | Deploy self-hosted | Try Open Source | Schedule a demo

support@akto.io | +1 (415) 658-1353



Quick start

Your connections 1

Burp Suite
Use burp plugin to send traffic to Akto and realize quick value. If you like what you see, we highly recommend using AWS

Explore other connections 12

AWS traffic mirroring
Use burp plugin to send traffic to Akto and realize quick value. If you like what you see, we

GCP traffic mirroring
Use burp plugin to send traffic to Akto and realize quick value. If you like what you see, we highly recommend using AWS highly recommend using AWS

Postman
Use burp plugin to send traffic to Akto and

Har file upload
Use burp plugin to send traffic to Akto and