akana

PERFORCE

DATASHEET

Akana API Guardian – Security Audit Services

APIs drive your business, which makes it critical to secure them. From recent headlines, you know what happens to organizations without the proper safeguards in place around their APIs. A single data leak can cost millions of dollars in fines and litigation, the loss of customers, and lasting brand damage.

A recent survey by Radware, a provider of cybersecurity and application delivery solutions, underscores the challenge. API abuses are expected to become the most frequent attack vector, and API security is the most critical hole enterprises should patch. 55% of organizations responding in the survey experienced DoS attacks against their APIs at least monthly, 49% experience some form of injection attack at least monthly, and 42% experience an element/attribute manipulation at least monthly.[i]

Akana has you covered. The Akana API Platform provides all the capabilities, tools, and security policies you need for authorization, privacy, non-repudiation, and attack prevention. Akana secures your API products and helps you:

- Reduce risks with automated application of security policies.
- Comply with industry regulations (Open Banking/PSD2, PCI).
- Protect against the latest security threats and attacks.

Akana includes the following out-of-the-box, no-code security policies:

- OpenID Connect Provider/Relying Party
- OAuth2.0 (all grant-types)
- App Key Authentication and Authorization
- CORS Management
- HTTP Basic-Auth, Digest Auth
- Mutual TLS-based Authentication
- JOSE Security (JWS, JWE)
- SAML 1.1 and 2.0 (STS included)
- WS-Trust 1.2 and 1.3
- WS-Security Transport Binding
- WS-Security Username Token
- WS-Security Message Encryption /Signature
- Integration with AD, SiteMinder, OAM, RSA
- Cookie-based Authentication
- Denial of Service Attack Prevention
- SQL Injection Prevention
- Virus Scanning
- JSON Schema Validation
- XML Schema Validation
- Malicious Pattern Detection
- SLA/Throttling by a Developer/Partner
- Certificate (PKI) Management (CA Included)

[i] Security Magazine. "API abuse is a leading threat." Jan. 20, 2021.

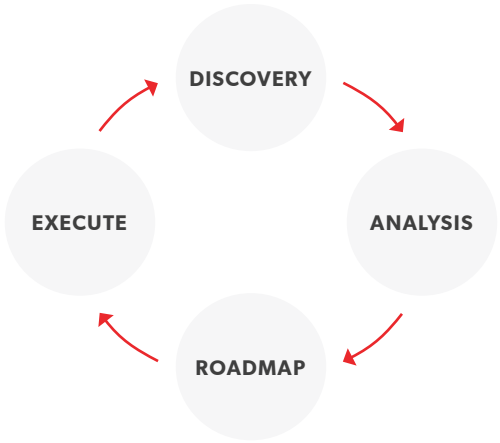
Through our ***API Guardian*** service, our expert consultants are available to evaluate and audit your API Platform for vulnerabilities, ensuring you're protected with a security-first approach.

API Guardian

We work with your team to audit and evaluate multiple domains, including:

- Secure platform architecture and deployment pattern.
- Platform credential storage.
- Platform audit logging and anomaly detection practices.
- Security policy implementation on APIs.
- API definition auditing.
- OWASP top 10 risks.
- Usage of OAuth, tokens, SAML, SSO & JWT.
- Integration into corporate identity and access management providers.
- API security testing best practices.
- API security for open banking.

API Guardian follows our ARAI (Akana Rapid API Improvement) Methodology, which consists of a phased approach:



DELIVERABLE

You'll receive your security audit results in a report that clearly highlights risk areas to address along with recommendations on how to mitigate any vulnerabilities we discovered during the engagement.

We typically complete our audit process within 10 business days depending on the number of APIs we review for you.

Work with an Expert Consultant to Review Your API Security

Talk with your Account Executive to schedule a free consultation with one of our experts.
Or, visit our website to request more information today!

REQUEST SERVICES

akana.com/services/request-services