

Enforce API Governance

AAM'S API GATEWAY PROVIDES A CENTRALIZED SOLUTION THAT STANDARDIZES API BEHAVIORS AND ENSURES COMPLIANCE

Govern Your APIs: Security and Consistency Without the Complexity

Most organizations struggle to enforce consistent standards across their growing API landscape, leading to security vulnerabilities and compliance risks. With 65% of companies experiencing API security incidents and 87% lacking formal governance strategies, these gaps expose businesses to data breaches, regulatory penalties, and reputation damage. With Akamai AI and API Manager (AAM), teams can move faster while maintaining the guardrails necessary for enterprise-grade security and governance.

With AAM's CI/CD integration, APIs that don't meet your security standards are automatically blocked or flagged across the pipeline—from new API code through development, staging, QA/testing, and production—preventing non-compliant deployments and raising warnings to ensure your team maintains rigorous authentication, authorization, and data protection across all environments.

> Prevent insecure APIs before they reach production

Automatically enforce security standards to block non-compliant APIs and stop vulnerabilities from entering your production environment.

> Enforce security standards automatically

Eliminate manual security reviews by defining policy-as-code that automatically enforces security requirements across all API deployments.

> Implement robust access control

Enforce the principle of least privilege with built-in Role-Based Access Control (RBAC), ensuring users access only the specific resources their role permits.

> Centralize security governance

Gain complete visibility into your expanding API ecosystem with comprehensive audit trails tracking all API changes, security policies, and access patterns.

Business Impact

> Eliminate security debt

Stop accumulating vulnerable APIs that will eventually need costly remediation.

> Continuous compliance

Automatically enforce regulatory requirements in your APIs without slowing down development velocity.

> Shift-left validation

Catch security issues early in the development lifecycle when they are easier and less expensive to fix.

> Automatic audit trails

Maintain comprehensive logs of all API access and policy changes for security analysis and compliance reporting.



The natural programmable nature of AAM makes it easy to integrate into any dev team and partner with developers to own it rather than have operations people do it.

Kevin Kuhl, Director of DevOps at SmarterX