AKAMAI SOLUTION BRIEF

Integrated API Security and Governance for IBM API Connect and DataPower

The promise and challenge of APIs

APIs have been the driving force for digital transformation, enabling organizations across every industry to create new services and business models to accelerate growth. However, as APIs proliferate, so do their risks.

- Although business and engineering leaders have rapidly increased API usage and integration across their organizations, their ability to effectively manage APIs remains a challenge.
- In the race to quickly build and release new applications and AI-enhanced services, the underlying APIs too often contain misconfigurations, coding errors, and business logic issues.
- Every time a customer, partner, or vendor engages with an organization digitally, there's an API behind the scenes facilitating a seamless exchange of data, often sensitive — and attackers know it.

As a result, APIs have emerged as a top attack vector with high stakes. Attacks on APIs can jeopardize an enterprise's revenue, resilience, and regulatory compliance.

To address this challenge, organizations must employ a full-lifecycle approach to both governance and security — including design, development, testing, deployment, operation, and remediation. Together, Akamai API Security and IBM enable organizations to quickly develop, deploy, and manage APIs with confidence so they can predictably respond and scale with the business.

How Akamai and IBM help customers

Discover your API estate

You can't protect what you can't see. With Akamai API Security, you can automatically discover APIs, domains, and issues to build a robust API inventory that offers visibility into your entire API estate — companies typically find significantly more APIs than they thought they had or expected to find. You can also easily find exploitable intelligence, such as leaked information, to understand the attack paths available to adversaries — and enjoy seamless integration with the most common infrastructure elements adjacent to your API gateways and management platforms to ensure consistent sharing of security data across the organization.

Strengthen your security and governance posture

Scale your operations and enforce best practices when using Akamai API Security for API governance:

- Understand every API in your ecosystem with full business context and align with API management best practices
- Streamline communications between development and security teams
- Find vulnerabilities from misconfigurations to out-of-policy APIs
- Protect sensitive data and proactively monitor changes to reduce risk in your APIs

Challenges

- Maintaining an API inventory across the estate and finding unknown APIs
- Identifying noncompliant, misconfigured, or vulnerable APIs
- Detecting and stopping API abuse or misuse, including business logic attacks
- Building secure and consistent APIs without sacrificing speed or agility
- Establishing alignment and oversight of API security and governance programs

Stop API abuse and attacks with runtime protection

Detect and block API attacks from edge to core — including data leakage, data tampering, data policy violations, suspicious behavior, and more — with real-time traffic analysis, out-of-band monitoring, inline remediation options, and workflow integrations to increase security operations center (SOC) effectiveness.

Deliver secure APIs faster with Active Testing

Seamlessly integrate API security testing into every phase of API development and uncover vulnerabilities, misconfigurations, and compliance problems before APIs are promoted to production. With Active Testing, DevSecOps personnel can execute a comprehensive suite of 200+ API-focused security tests on-demand or as part of the company's CI/CD processes. Active Testing finds and tests every API based on an understanding of the application's underlying business logic, which allows developers to uncover complex vulnerabilities other testing tools could miss.

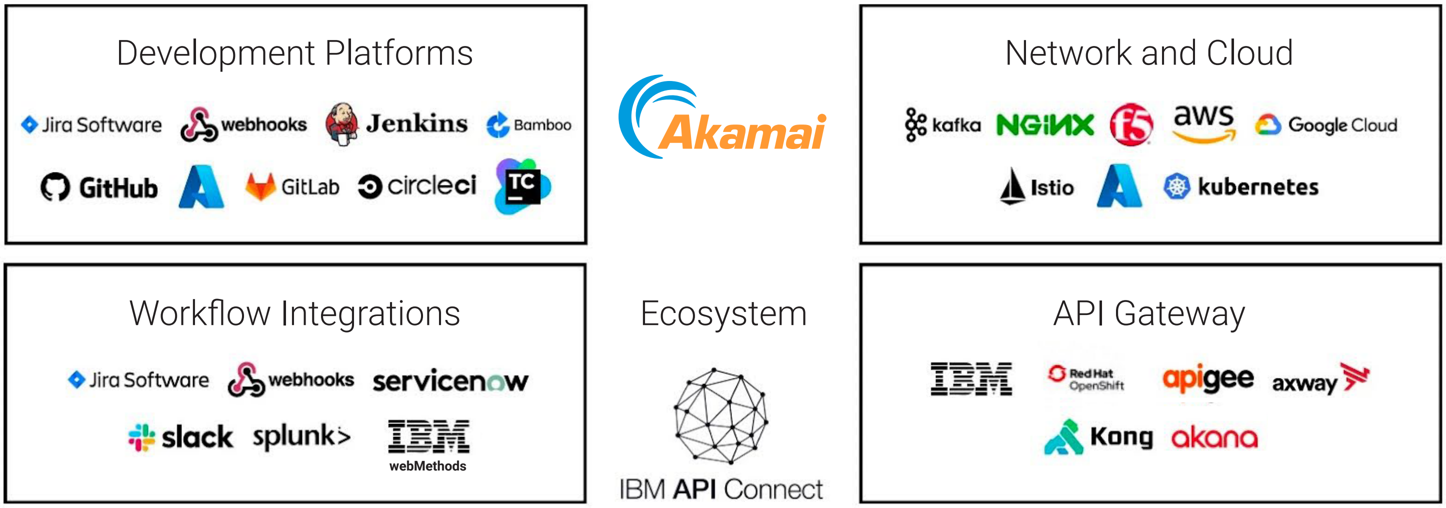
How Akamai enables IBM users to gain visibility and protection with efficiency-driving integration

Akamai API Security integrates with both API Connect and DataPower across multiple cloud platforms and deployment options. Additionally, when API Connect manages DataPower, unilateral configuration changes are made across systems, driving increased operational efficiency while reducing the risk of unauthorized and out-of-compliance development activities.

Seamless attack direction and response

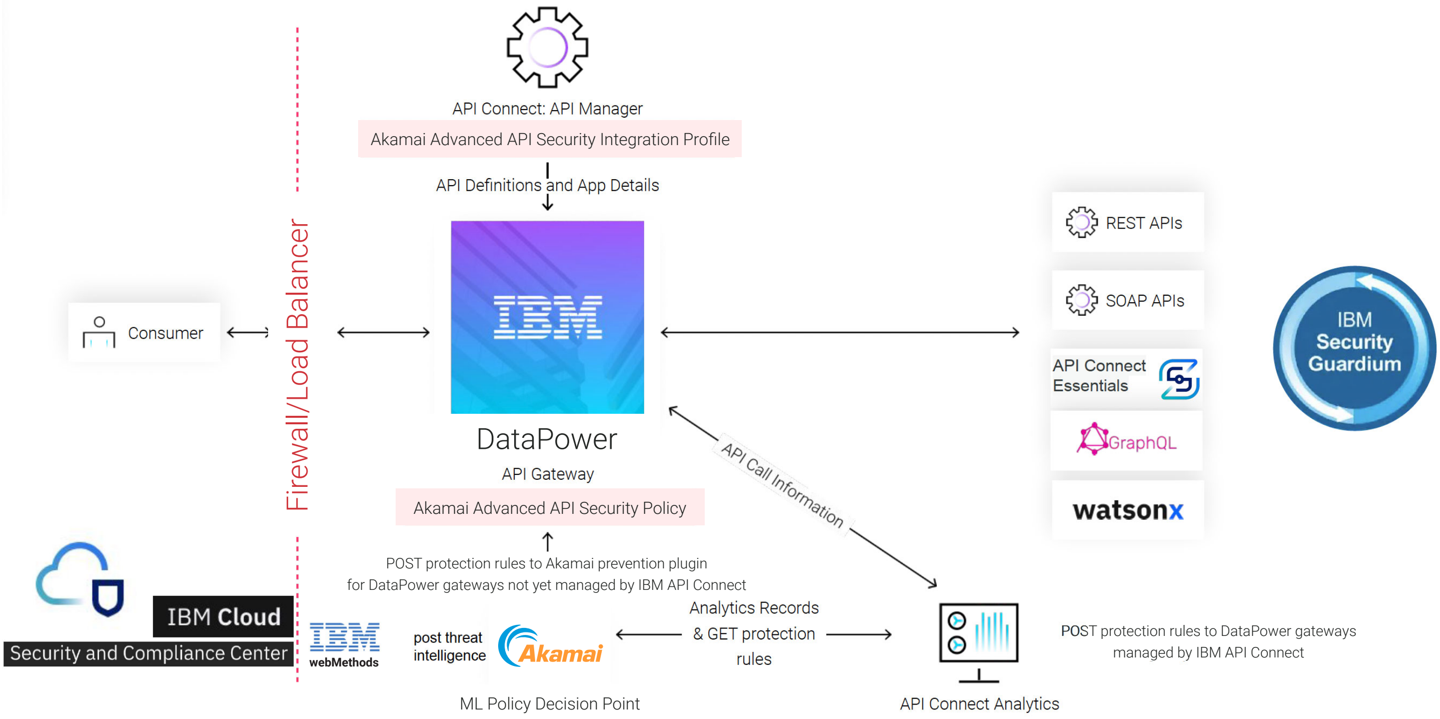
In addition, IBM DataPower customers can experience near real-time threat detection and blocking with no performance and latency impact without the need to install any additional plugins on DataPower gateways by integrating with the Akamai API Security solution.

IBM API Connect can evaluate access requests to resources against Akamai API Security authorization policies and enforce blocking rules across IBM DataPower clusters, reducing remediation times from days to minutes or seconds.



Combine the power of IBM webMethods and Akamai API Security for unparalleled API management and protection. This partnership offers a complete solution joining Akamai's advanced API discovery with IBM webMethods' robust governance and real-time data integration. Get full visibility and control over your APIs to ensure security and compliance. This integration not only strengthens defenses but also boosts efficiency, allowing your enterprise to respond quickly and securely to dynamic market demands.

Lastly, IBM DataPower customers can leverage the Akamai eBPF Red Hat OpenShift integration to discover APIs that are not yet managed by API Connect or proxied by DataPower, enabling them to find and protect APIs processing high-risk transactions and confidential data. These capabilities extend beyond on-premises to cloud and hybrid configurations, supporting Amazon Web Services (AWS), Microsoft Azure, and the Google Cloud Platform (GCP).


API Connect: API Manager
Akamai Advanced API Security Integration Profile
API Definitions and App Details
Consumer
Firewall/Load Balancer
IBM
DataPower
API Gateway
Akamai Advanced API Security Policy
POST protection rules to Akamai prevention plugin
for DataPower gateways not yet managed by IBM API Connect
API Call Information
REST APIs
SOAP APIs
API Connect Essentials
GraphQL
watsonx
IBM Security Guardium
IBM Cloud
Security and Compliance Center
IBM webMethods
post threat intelligence
Akamai
Analytics Records & GET protection rules
ML Policy Decision Point
API Connect Analytics
POST protection rules to DataPower gateways managed by IBM API Connect

Next steps

APIs are a driving force behind organizations' ability to meet customers' needs, generate revenue, and compete in a fast-moving digital economy. However, their continuous growth, proximity to data, and myriad vulnerabilities make them an appealing target for attackers. With API security incidents steadily increasing, it's essential to have capabilities in place for seeing, securing, and testing every API across your organization. The combination of IBM and Akamai can give enterprises confidence to build, maintain, and use APIs securely and at scale.

Learn how we can help you by scheduling a customized Akamai API Security demo.
You can also speak with your IBM contact to learn more.