Akamai Solution Brief

Akamai + Apiiro Application Security Posture Management

Security leaders are increasingly accountable for understanding which applications, APIs, and domains are exposed to the internet and whether those assets are consistently protected.

In large, distributed environments, maintaining this visibility can be challenging. Application inventories often span platforms and environments, making it difficult to maintain a clear, organization-wide view of exposure and protection coverage for multiple teams and objectives of the organization. As environments scale, security leaders need reliable insight into which applications are deployed, how they are protected, and where additional attention is required.

Akamai and Apiiro deliver application security posture management (ASPM) by combining runtime protection with application and API visibility, enabling security leaders to identify gaps, prioritize action, and demonstrate effective governance with confidence.

Key benefits

Clear understanding of application exposure and protection coverage:

- Prioritization of risk based on exposure and business impact
- Improved collaboration between security, AppSec, and infrastructure teams
- Faster response to emerging threats and security gaps
- Confidence in posture reporting to executives, auditors, and regulators

The CISO challenge: Coverage at scale

Modern enterprises operate hundreds of thousands of internet-facing applications, APIs, and domains across cloud, on-premises, and hybrid environments. While application protections are widely deployed, they are often implemented across multiple platforms, teams, and operational processes.

For CISOs, this creates a fundamental challenge: **maintaining a clear, real-time understanding of application exposure and protection coverage across the organization**.

Common challenges include:

- Incomplete or outdated inventories, or exposed applications and domains
- Fragmented ownership across application, infrastructure, and security teams
- Inconsistent visibility into where security protections are deployed
- Difficulty mapping security controls to specific applications and business services
- Heavy reliance on manual reporting and point-in-time reviews to assess posture

Without a centralized view, security leaders struggle to answer critical questions such as:

- Which applications and APIs are exposed to the internet?
- Which assets are protected by runtime security controls?
- Where should security teams focus remediation efforts?

Answering these questions requires a combination of application context and security insight.

Securing applications together

Akamai and Apiiro address this challenge by combining application posture visibility with clear insight into WAAP coverage, delivered through a unified ASPM framework.

Akamai App & API Protector delivers comprehensive runtime protection for web applications and APIs. Powered by the Adaptive Security Engine, it helps defend applications against a wide range of threats, including application-layer attacks, API abuse, automated threats, and distributed denial-of-service (DDoS) attacks.

Apiiro complements these runtime protections by providing deep visibility into applications, APIs, and their underlying code and ownership structures across the software lifecycle. By mapping applications from code to runtime, Apiiro helps organizations understand how application risks relate to the assets deployed in production.

Together, the solutions provide security leaders with the visibility needed to understand:

- Which applications, APIs, and domains exist across the organization
- Which assets are protected by WAAP security
- Where additional protections or remediation may be required

This integrated approach helps shift application security posture management from snapshot reviews to continuous visibility and governance.

What each solution provides:

Akamai provides:

- Enterprise-grade WAF, DDoS, API, and bot protection
- Protection for applications wherever they are
- Protection against DDoS, exploits, CVEs, and zero-day attacks
- Best-in-class threat intelligence and cross-estate visibility into deployed WAAP and security controls

Apiiro provides:

- Discovery and software architecture mapping from code to runtime
- Identification of applications, APIs, domains, and ownership
- Prioritization of vulnerabilities based on exposure and business impact
- Visibility into connections between risks and code owners
- Prevention of application risk by autonomously flagging potential risky commits before code is generated

How it works

Discover

Apiiro identifies applications, APIs, and domains across the organization, helping establish a comprehensive inventory of exposed assets.

Associate

Applications and domains are mapped to ownership, development teams, and deployed security controls, including runtime protections such as Akamai App & API Protector.

Assess

Apiiro evaluates application risk using exposure context, code-level insights, and business impact, helping teams prioritize remediation and security coverage.

Protect and validate

Akamai App & API Protector delivers runtime protection for applications and APIs, helping defend against exploits, API abuse, automated threats, and DDoS attacks.

Together, Akamai and Apiiro provide visibility into where protections are in place and where additional controls may be appropriate.

Customer value

Together, Akamai and Apiiro give CISOs the clarity and confidence needed to govern application security at scale. By combining runtime protection with application and API visibility, organizations gain a centralized view of exposure and WAAP coverage across their environment. This empowers security teams to identify gaps early, prioritize action based on evidence, and ensure that critical applications and APIs remain consistently protected.

The result is stronger collaboration between security and development teams, and greater assurance in the organization's ability to manage its application security posture as the landscape evolves. By surfacing this unified view of exposure and coverage, customers can also demonstrate effective oversight of security controls to stakeholders — reducing uncertainty, closing visibility gaps, and building lasting confidence that critical assets are safeguarded both today and into the future.

To learn more about application security posture management, contact your Akamai representative or email sales@akamai.com.

© 2026 Akamai Technologies | Support | | Published 03/26