



Executive Summary

The Wiz and Akamai integration extends continuous, graph-based visibility from the cloud runtime all the way to the internet edge. Akamai DNS Posture Management provides dedicated visibility, observability, and actionability across the DNS estate, while the Wiz Security Graph delivers context across underlying cloud workloads, identities, and sensitive data. Connecting these layers eliminates edge blind spots, correlates edge exposure with backend cloud risk, and pinpoints critical attack paths across the entire application delivery lifecycle.



Market challenge

Modern architectures rely on distributed edge networks for traffic delivery, performance, and DNS routing, often managed outside core cloud security workflows. When edge routing rules or DNS records are modified in silos, they can inadvertently undermine backend cloud hardening. A single misconfigured edge rule can expose unprotected internal workloads, sensitive data, or internal APIs directly to the public internet, creating a critical blind spot and a prime attack vector.



Benefits of the Integration

- ✓ **Unified Edge-to-Cloud Visibility:** Connect Akamai's DNS posture insights, including Edge DNS zones and account metadata, with the Wiz Security Graph to visualize risk across all layers.
- ✓ **Contextual Risk Prioritization:** Correlate edge exposure findings from Akamai with backend cloud workloads, identities, and sensitive data in Wiz to prioritize truly exploitable attack paths.
- ✓ **Proactive Exposure Detection:** Akamai DNS Posture Management to maintain continuous observability and actionability over DNS record changes. Wiz then evaluates these edge shifts against cloud access controls and security posture in real time to flag unintended exposure.
- ✓ **Streamlined DevSecOps & Accelerated Remediation:** Bridge the gap between network, edge, and cloud security teams. By connecting Akamai's DNS posture insights directly to Wiz's mapped backend resources and owners, teams receive step-by-step guidance to resolve root causes rapidly.



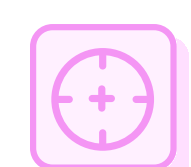
The "Better Together" Story

Securing modern web applications requires bridging the gap between global traffic delivery and backend cloud infrastructure. Akamai DNS Posture Management delivers visibility, observability, and actionability across DNS resolution, property rules, and traffic routing at the edge. Wiz provides agentless context into cloud workloads, identities, and sensitive data.

Together, Wiz and Akamai connect edge DNS posture with core cloud context. When Akamai surfaces DNS and routing configurations, Wiz maps them against the Security Graph so joint customers gain a single view of their attack surface. Overly permissive edge rules are no longer analyzed in isolation, they are evaluated against the specific cloud assets, sensitive data, and identities they expose. This enables security and engineering teams to move fast, eliminate edge blind spots, and burn down critical risks across the entire stack.



Use Case: Preventing Accidental Exposure from Edge DNS & Routing Changes



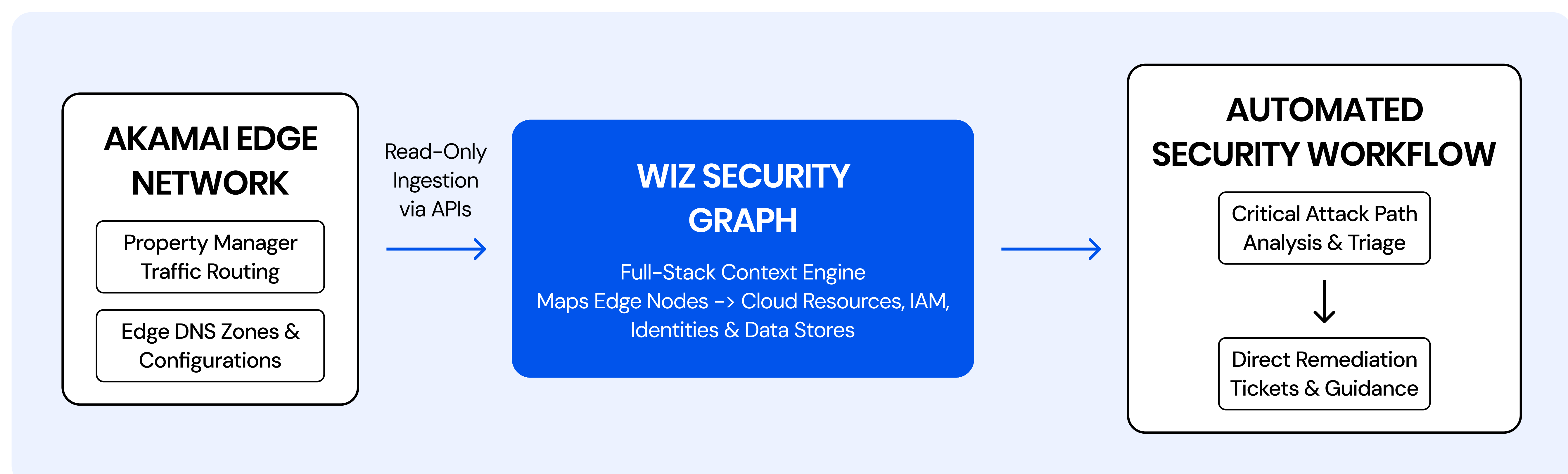
Challenge: Developers and platform engineers routinely update Akamai Edge DNS records and traffic routing rules to deploy new features and scale services. Without connected edge-to-cloud context, security teams have no automated way to know when an edge update accidentally exposes a private API, staging environment, or sensitive database directly to the internet.

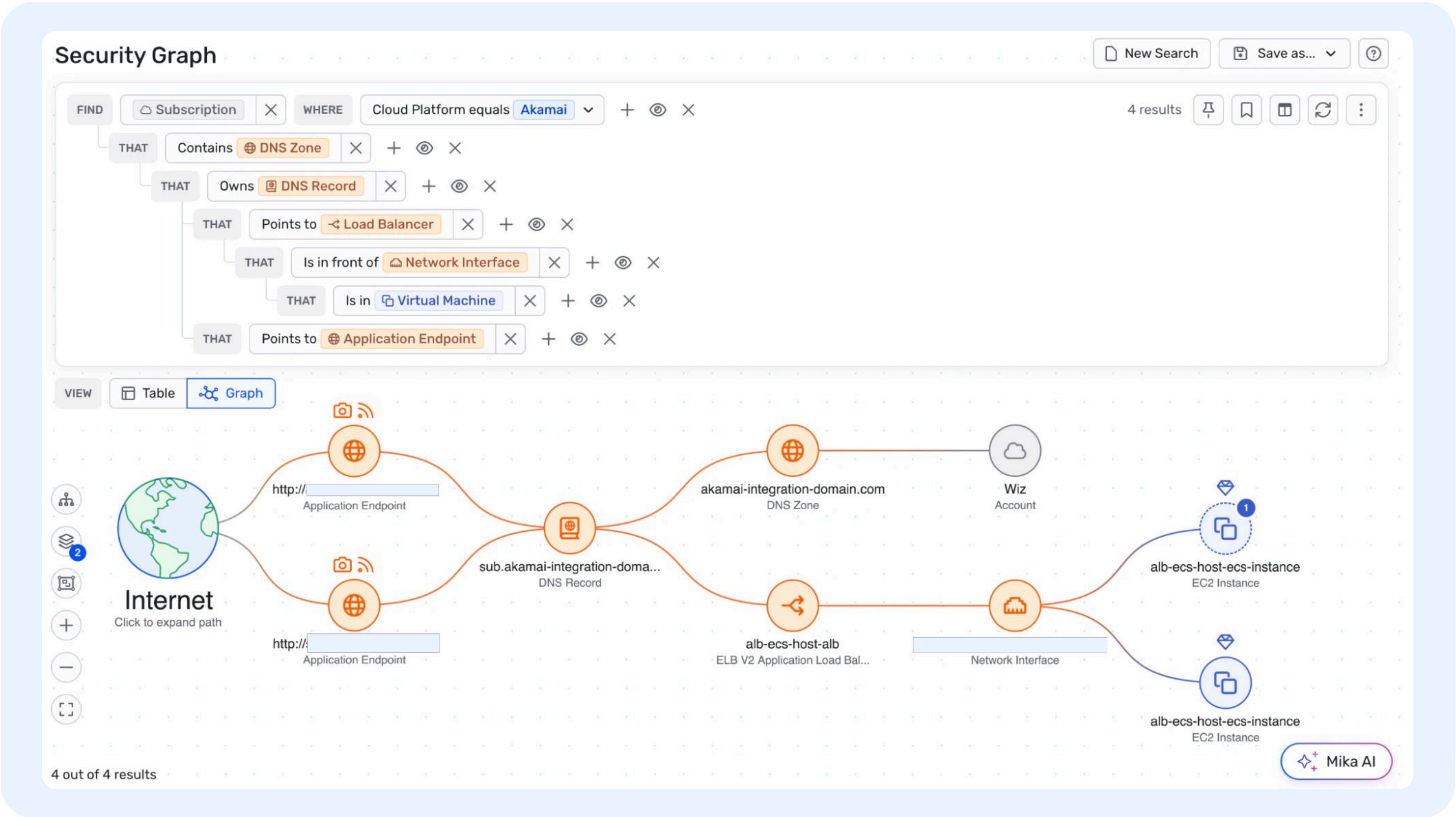


Solution: Akamai DNS Posture Management continuously monitors Edge DNS zones, configurations, and routing changes, surfacing posture insights through lightweight, read-only APIs. Wiz connects those insights to the Security Graph, mapping them against backend workload vulnerabilities, network architectures, and sensitive data stores. When an edge change creates a toxic combination, such as exposing an unauthenticated internal microservice holding sensitive data, Wiz surfaces the attack path, prioritizes the risk, and routes remediation guidance directly to the resource owner.



Impact: Teams eliminate edge blind spots and automatically surface real attack paths. Security and development teams can immediately distinguish between benign edge configurations and critical exposures—such as an exposed backend API containing sensitive data—reducing mean time to respond (MTTR) and preventing edge-based security incidents.





Security Graph

NEW SEARCH SAVE AS... ?

FIND WHERE Cloud Platform equals Akamai + X

6 results

VIEW Table Graph

DNS Record	Cloud Platform	Status	External ID	Native Type	Type
akamai-integration-domain.com Akamai DNS Record	Akamai	Inactive	a4e3	DNS Record	SOA
akamai-integration-domain.com Akamai DNS Record	Akamai	Inactive	a4e3	DNS Record	NS
sub.akamai-integration-domain.com Akamai DNS Record	Akamai	Inactive	a4e3	DNS Record	CNAME
application.akamai-integration-domain.com Akamai DNS Record	Akamai	Inactive	a4e3	DNS Record	CNAME
aws-record.akamai-integration-domain.com Akamai DNS Record	Akamai	Inactive	a4e3	DNS Record	CNAME
apigateway.akamai-integration-domain.com Akamai DNS Record	Akamai	Inactive	a4e3	DNS Record	CNAME