WIZ + CLOUDFLARE

Executive Summary

Cloudflare and Wiz integrate to bring comprehensive visibility and risk mapping across the cloud edge. By continuously scanning Cloudflare DNS zones, records, and proxy settings; the Wiz Security Graph ingests DNS zone and record data to automatically expose public entry points, unmanaged assets, and critical attack paths leading into backend infrastructure. Security teams can now spot misconfigurations, validate exposure, and trace dangling DNS records directly back to the underlying cloud resources and Infrastructure-as-Code (IaC) that created them.

Market challenge

Modern cloud security is crippled by the visibility gap between edge networks and cloud environments. As developers rapidly deploy global services and update routing rules, DNS zones frequently go unaudited by central security workflows. Misconfigured and/or dangling DNS records, and unmanaged edge resources create hidden entry points that leave internal workloads, APIs, and sensitive data exposed to internet-wide exploitation.

Benefits of the Integration

- **Eliminate Edge Blind Spots:** Automatically discover and scan all Cloudflare DNS zones and records to map your external attack surface onto the Wiz Security Graph.
- **Code-to-Cloud Edge Context:** Connect public-facing DNS endpoints back to the specific cloud infrastructure, load balancers, and Terraform / IaC code definitions that provision these resources for root-cause analysis.
- **Prioritize Exploitable Risk:** Correlate edge exposure with cloud workload findings, identity access, and sensitive data to focus on critical attack paths over low-impact noise.
- **Continuous Threat Prevention:** Continuously re-evaluate evolving DNS configurations to catch risky exposures, dangling DNS records, and misconfigurations before attackers exploit them.

The "Better Together" Story

Cloudflare powers and protects global internet traffic, while Wiz delivers deep full-stack cloud context and risk prioritization. Together, they bridge the gap between edge network routing and cloud infrastructure security. By mapping Cloudflare DNS records directly into the Wiz Security Graph, joint customers gain a single source of truth for their edge-to-cloud attack surface. Edge exposures are no longer evaluated in isolation; Wiz cross-references them against active workloads, network pathways, sensitive data, and IAM permissions to validate real-world exploitability. This allows security and DevOps teams to break down silos, eradicate shadow cloud assets, and eliminate critical risks at the source.

Use Case: Eliminating Dangling DNS Records & Preventing Subdomain Takeovers

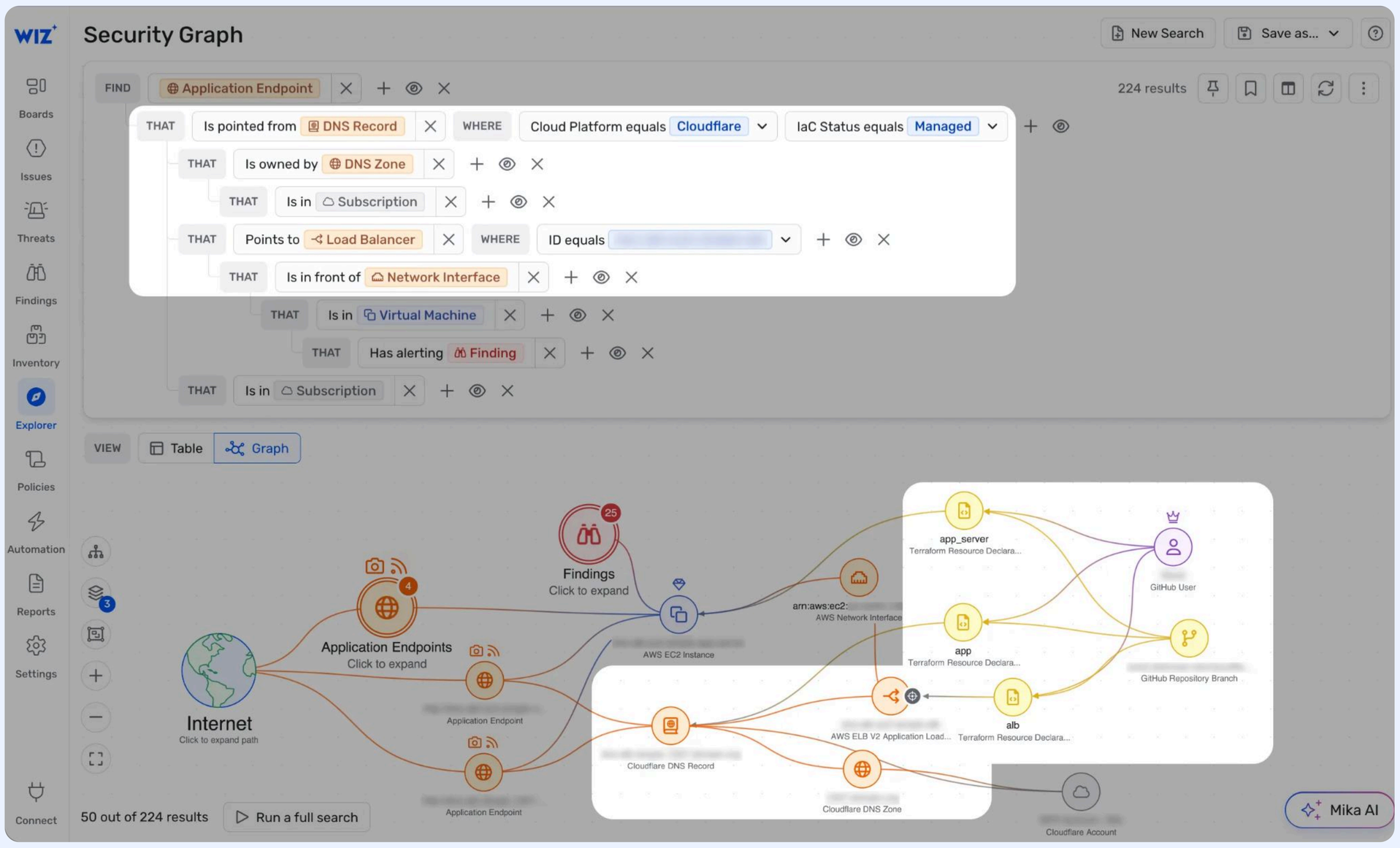
Challenge: A developer configures a public Cloudflare DNS record pointing to a temporary cloud load balancer and a backend container with database access. After sprint testing wraps up, the developer tears down the backend cloud infrastructure but forgets to remove the Cloudflare DNS record. Because the DNS record, typically a CNAME, still points to the now-deregistered cloud endpoint, an attacker can claim that endpoint on the same cloud provider and intercept any traffic that resolves through the orphaned record.

Solution: The Wiz connector continuously ingests Cloudflare DNS configurations and correlates them against active multi-cloud environments in the Wiz Security Graph. Wiz instantly flags the orphaned DNS record pointing to a non-existent cloud target, maps the dependency chain across the environment, and traces the configuration back to the originating Terraform repository and commit author, when IaC scanning and VCS integration are enabled.

Impact: Security teams immediately receive a contextual, high-priority Wiz Issue highlighting the dangling DNS record and its exposed attack path. Connecting the attack path directly back to the originating Terraform code and resource owner empowers engineering teams to fix misconfigurations at the source, reducing mean time to resolve (MTTR) and closing public attack vectors before attackers can exploit them.



** IaC trace requires Wiz IaC Scanning + VCS Integration (GitHub / GitLab / Bitbucket) separately enabled.*


Security Graph
New Search
Save as...
FIND
Application Endpoint
224 results
THAT
Is pointed from DNS Record
WHERE
Cloud Platform equals Cloudflare
IaC Status equals Managed
THAT
Is owned by DNS Zone
THAT
Is in Subscription
THAT
Points to Load Balancer
WHERE
ID equals
THAT
Is in front of Network Interface
THAT
Is in Virtual Machine
THAT
Has alerting Finding
THAT
Is in Subscription
VIEW
Table
Graph
Boards
Issues
Threats
Findings
Inventory
Explorer
Policies
Automation
Reports
Settings
Connect
25
Findings
Click to expand
4
Application Endpoints
Click to expand
Internet
Click to expand path
Application Endpoint
Application Endpoint
AWS EC2 Instance
arn:aws:ec2:
AWS Network Interface
app_server
Terraform Resource Declara...
GitHub User
app
Terraform Resource Declara...
GitHub Repository Branch
alb
Terraform Resource Declara...
AWS ELB V2 Application Load...
Cloudflare DNS Record
Cloudflare DNS Zone
Cloudflare Account
50 out of 224 results
Run a full search
Mika AI