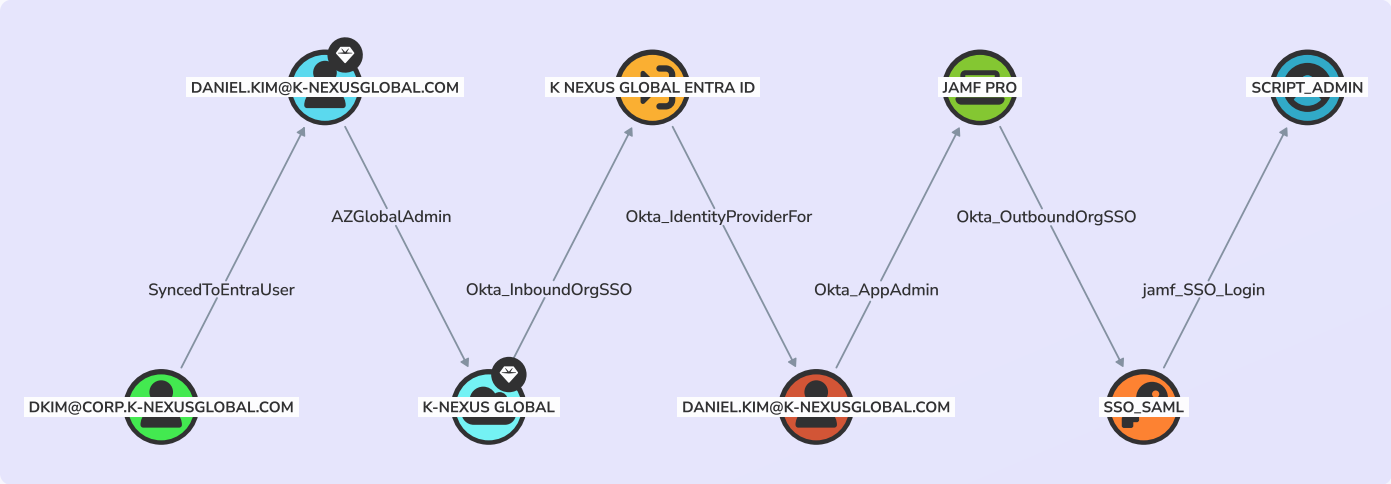
BLOODHOUND ENTERPRISE

OVERVIEW

Protecting Okta Environments with BloodHound Enterprise



The attack paths that run through Okta rarely look like attacks. A synced group membership, a federated application assignment, a misconfigured role—each appears routine in isolation. Together, they form attack paths that span platforms, cross administrative boundaries, and reach assets no single team knew were exposed.

The Problem

Okta's role in the modern enterprise extends to authentication, provisioning, and access delegation across dozens or hundreds of connected applications. Security teams responsible for Okta see their slice of that picture: role assignments, application integrations, authentication policies. The teams responsible for Active Directory, GitHub, or AWS see theirs. No single team is able to see how and where those slices connect.

Adversaries use this to their advantage and operate across the entire chain. They follow the relationships that carry identity between systems—federation links, directory sync pipelines, SSO connections—exploiting the access that accumulates. **The most consequential attack paths through Okta don't live inside Okta, they live in the gaps between it and the systems it depends on.**

The Solution

BloodHound Enterprise gives defenders a map of what adversaries see: the chained relationships that combine to create exploitable paths to critical assets. OpenGraph extends that analysis to the platforms that sit outside traditional identity infrastructure but inside real-world attack paths.

The Okta OpenGraph extension connects Okta to the broader attack path graph that covers Active Directory, Entra ID, and downstream platforms. Rather than auditing Okta separate from the other platforms it interacts with, **BloodHound Enterprise shows how Okta-mediated access combines across the environment and where those paths extend to the cloud platforms, applications, and critical assets downstream.**

Within Okta environments, BloodHound Enterprise maps the relationships adversaries rely on:

Users, Groups, and Role Assignments

Maps how permissions accumulate through group membership and role delegation to surface where excessive or misconfigured assignments create paths to administrative control.

Application Integrations and SSO

Models how Okta-mediated access translates into downstream platform access to reveal where an identity that appears low-privileged in Okta corresponds to elevated control elsewhere.

Federation and Directory Sync

Maps the upstream relationships that feed identity into Okta to show how a compromised Active Directory or Entra ID account propagates through sync pipelines into Okta and beyond.

Taken together, that coverage answers the question no configuration audit can: given everything in place across your environment, where can an adversary go from any particular point in my identity and application network?

What This Looks Like in Practice

In September 2023, Scattered Spider compromised MGM Resorts by calling the IT help desk, impersonating an employee found on LinkedIn, and requesting an account reset. The call lasted 10 minutes. The result was super administrator access to MGM's Okta environment and from there Global Administrator access to their Azure tenant. Adversaries deployed ransomware across more than 100 ESXi hypervisors, which took down reservation systems, digital room keys, and slot machines across MGM's properties. The incident cost the company $100 million in one quarter. The initial foothold was a single identity, Okta was the bridge to everything else.

BloodHound Enterprise reveals exactly this class of exposure, the routine identity relationships that individually appear unremarkable but compose into exploitable paths. Synced group memberships, federated application assignments, and excessive role delegations each represent a relationship that BloodHound Enterprise models, connects to the broader graph, and traces to wherever that access ultimately reaches.

Okta Is One Piece of a Larger Attack Surface

No single extension tells the full story. Adversaries don't limit themselves to one platform, and neither does OpenGraph. **A path that originates in Active Directory, moves through Okta, and lands in GitHub, where it assumes a privileged cloud role, is only visible when all three are in the graph.**

BloodHound Enterprise OpenGraph extensions for GitHub and Jamf extend the same attack path analysis to source code environments, CI/CD pipelines, and Jamf-managed Mac infrastructure. Together, they give defenders visibility into the cross-platform paths that form between systems, across administrative boundaries, and outside the reach of any single platform review.

Ready to See Your Okta Environment the Way Adversaries Do?

Request a demo of BloodHound Enterprise:

Visit specterops.io/get-a-demo

SPECTEROPS