

Accelerate Investigations and Reduce MTTR with User Context from Okta

Enrich User Context, Unmask Suspicious Behavior, and Accelerate Threat Containment

PARTNER SOLUTION BRIEF

As AI-powered threats grow more powerful and multiply rapidly, organizations face unprecedented challenges in detecting and investigating threats that compromise identity at the perimeter. Rather than breaking into systems, modern attackers simply log in with valid credentials, leveraging AI to accelerate attack velocity and navigate network environments with greater speed. Detecting credential misuse, privilege escalation, and lateral movement requires security teams to understand not only what activity is occurring across the network, but precisely who is behind it.

The ExtraHop RevealX integration with Okta addresses these identity challenges by connecting authoritative Okta identity metadata with real-time network detection and response (NDR). By correlating user identities with network behavior, security analysts gain critical identity context, eliminate silos during investigations, and accelerate threat containment directly within your NDR platform.

Turning Usernames into Understanding

Enhance user profiles with contextual data from Okta, including titles, managers, and departments for deeper visibility into identity relationships. This integration gives you a stronger, identity-focused understanding of user actions. Without identity context, a username on an alert is just a static label. ExtraHop RevealX™ imports rich user properties from Okta and associates them directly with user entities within the ExtraHop system. This critical context eliminates the need for multiple pivots to other systems, clarifying for your analysts whether an action is appropriate or not.

- **Enriched User Profiles:** Displays Okta user attributes directly in RevealX, including Display Name, UPN, Job Title, Company, Location, Employee Type, Group Memberships, Account Created On, Password Changed On, and Account Status.
- **Identity-Driven Triage:** Surface privileged and influential users directly within detection views to prioritize high-risk investigations.
- **User Search & Filtering:** Find users and activity based on identity properties (e.g., Object ID or UPN).



Detect and Stop Lateral Movement

Attackers rarely rely on malware once they have footholds; they weaponize legitimate credentials to move laterally across hybrid environments. ExtraHop correlates network behavior with Okta identifiers, pinpointing exactly which devices or internal domain services a compromised user has touched to establish blast radius. By providing visibility across layers, this defense directly combats lateral movement, which can occur within minutes of initial access. Integrating ExtraHop network visibility and analytics with Okta user context makes detecting anomalous post-authentication actions immediate, such as a finance user executing administrative PowerShell commands over RDP.

Integrated Response for Rapid Containment

When an account compromise is confirmed, stopping the adversary's progress requires swift execution. RevealX provides built-in response actions for Okta accounts, allowing security operations center (SOC) analysts to act immediately within their active investigation workflow:

- **Revoke User Sessions:** Immediately invalidates active Okta sessions, forcing the user to reauthenticate across connected devices and applications.
- **Suspend Account:** Suspends the Okta user account to prevent further authentication while the account remains suspended.

Flexibility and Workflow Continuity

The integration is built on a flexible, opt-in framework. Organizations can selectively enable capabilities that match their operational controls and security policies, ensuring flexible deployment without requiring structural changes to identity governance.

User Context is Critical for the Agentic SOC

Identity context serves as a foundational element within ExtraHop's Agentic SOC framework. By correlating user accounts and authorization levels directly with live network telemetry, it equips autonomous security agents to efficiently analyze credential exploitation and lateral movement.

The screenshot displays the ExtraHop RevealX interface. On the left, the 'BloodHound Enumeration Activity' panel shows a detection for 'dmszones.bluth.local' receiving an LDAP enumeration query. It identifies an offender (GH6KW87AH) and a victim (dmszones.bluth.local). Below this, a 'Metrics' section shows network bytes in by L7 protocol, and a 'Log' table lists the event details. On the right, the 'User' panel for 'alice.johnston@PATCHTUESDAYS.com' displays Okta integration details, including display name, principal name, job title, company, location, employee type, group memberships, account creation and password change dates, and account status. A 'Response Actions' dropdown menu is visible, showing options like 'Revoke Sessions' and 'Suspend Account'.

Correlating Okta user metadata with Bloodhound enumeration activity within the detection view.

Getting Started with ExtraHop and Okta

The integration between ExtraHop RevealX and Okta delivers immediate, identity-aware visibility and rapid containment capabilities to secure modern hybrid environments against credential abuse and lateral movement. By connecting real-time network telemetry with rich user context, security operations teams can streamline triage, reduce MTTR, and neutralize threats with confidence.

Ready to accelerate your threat detection and investigations?

[Request a demo](#) or contact your ExtraHop representative today to get started with the Okta integration.

ExtraHop is a leader in real-time network intelligence, empowering organizations with high-fidelity context to power security and IT automation, detect risks faster, and respond with confidence. The ExtraHop RevealX platform delivers a complete, unified view of the network to help the largest enterprises in the world uncover what others miss. To learn more, visit extrahop.com or follow us on [LinkedIn](#).

EXTRAHOP

info@extrahop.com
extrahop.com