EXTRAHOP | Microsoft Entra ID

Accelerate Identity Threat Investigations with ExtraHop and Entra ID

Integrated Identity Detections and Investigations with Entra ID

PARTNER SOLUTION BRIEF

Overview

With valid users and their devices now a significant attack vector, identity context has become crucial for determining who is truly behind an activity and understanding the full scope of what occurred. Attackers are increasingly targeting users through social engineering, credential abuse, token theft, making identity context crucial for understanding who is behind the activity and what really happened.

ExtraHop now integrates identity data directly from Entra ID, enabling your SOC analysts to seamlessly search, pivot, and trace user activity across the platform for rapid context and faster insights during investigations. Identity becomes a native element and seamless part of all of your investigations, providing powerful insights, richer context, and faster response actions.

The digital identity has become a top attack vector with 91% of organizations reported an identity-related breach in the past year.*

Turning Usernames into Understanding

Enhance user profiles with contextual data from Entra ID, including titles, departments, and managers for deeper visibility into identity relationships. This integration gives you a deeper, identity-focused understanding of user actions. This critical context eliminates the need for multiple pivots to other systems, instantly clarifying for your analysts whether an action is appropriate or not. We are taking an identity-focused approach that makes users as visible and searchable as devices across ExtraHop.

IDENTITY-BASED USE CASES

- Investigating Credential Abuse
- Catching Ransomware Attacks
- Understanding “Blast Radius”
- Detecting Privilege Escalation
- Stopping Identity-Based Lateral Movement
- User Containment and Quarantine
- Preventing Data Exfiltration

*Source: IDSA’s Trends in Securing Digital Identities Report

Gain Visibility into User Activity by Ingesting IDP Logs as Records

By ingesting user activity directly from identity providers like Entra ID, you can track things like sign-ins, privilege escalations, or access changes, right alongside the network traffic you're already investigating. All of that data is brought in as records, so it's searchable, pivotable, and ready to be analyzed next to packet-level evidence. This combination of network and identity data becomes incredibly powerful for understanding not just what happened, but how and why it happened.

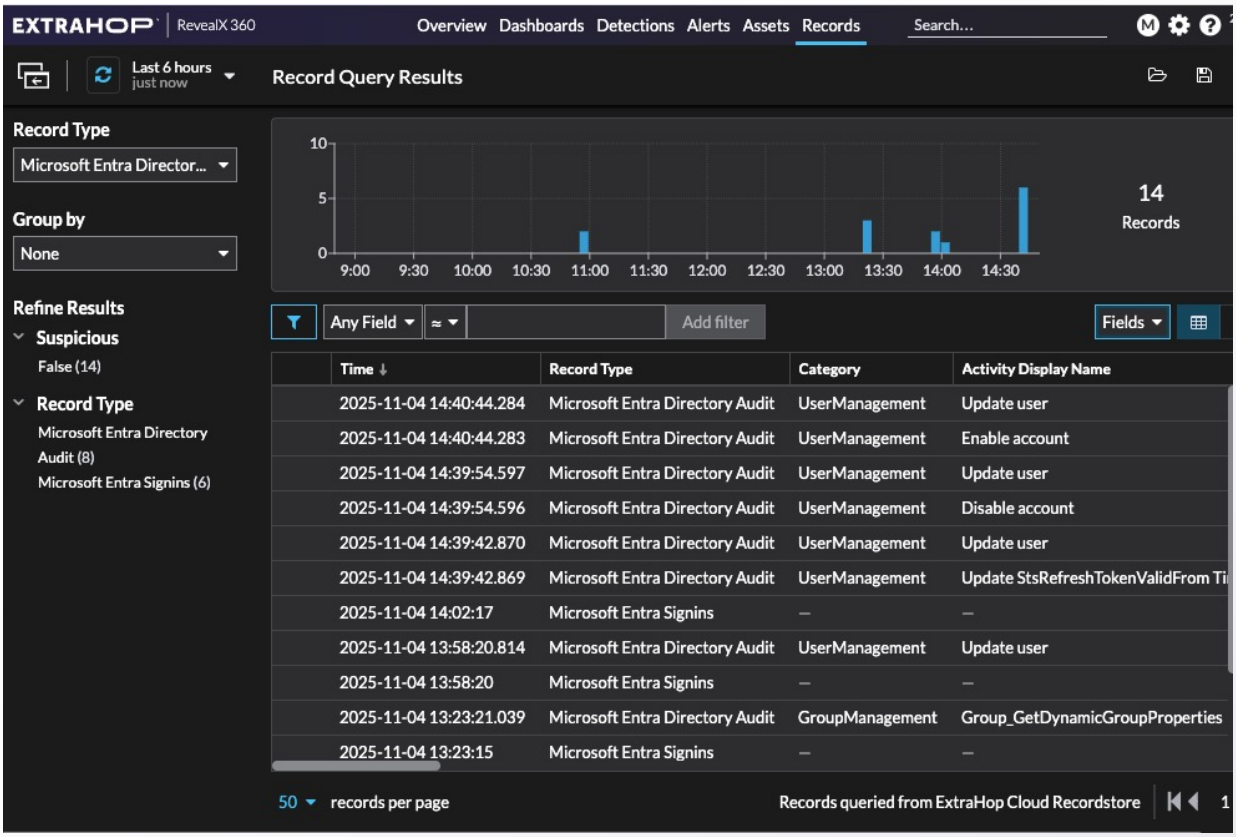

Figure 1. User activity from IDPs ingested as records in RevealX

Risky User Detections and Dashboards

We want to make identity risk easier to understand inside ExtraHop, which is why we're expanding our support for risky user detections and dashboarding. Analysts need to quickly see when an identity is behaving in a way that doesn't line up with what's normal, and they need that context presented in the same place they are already investigating their network activity. These detections surface cloud-driven identity risks in a way that fits seamlessly into an investigation workflow and pairs naturally with the AD visibility we already provide.

These Entra ID dashboards highlight unusual user activity and admin activity affecting user accounts. These new dashboards give analysts a high-level view of identity-driven risk and the ability to drill into the signals that matter. By pairing cloud-based identity signals with the deep network visibility we already provide, we're giving teams a more complete view of how users behave across their environment and where that behavior might be a risk to your organization.

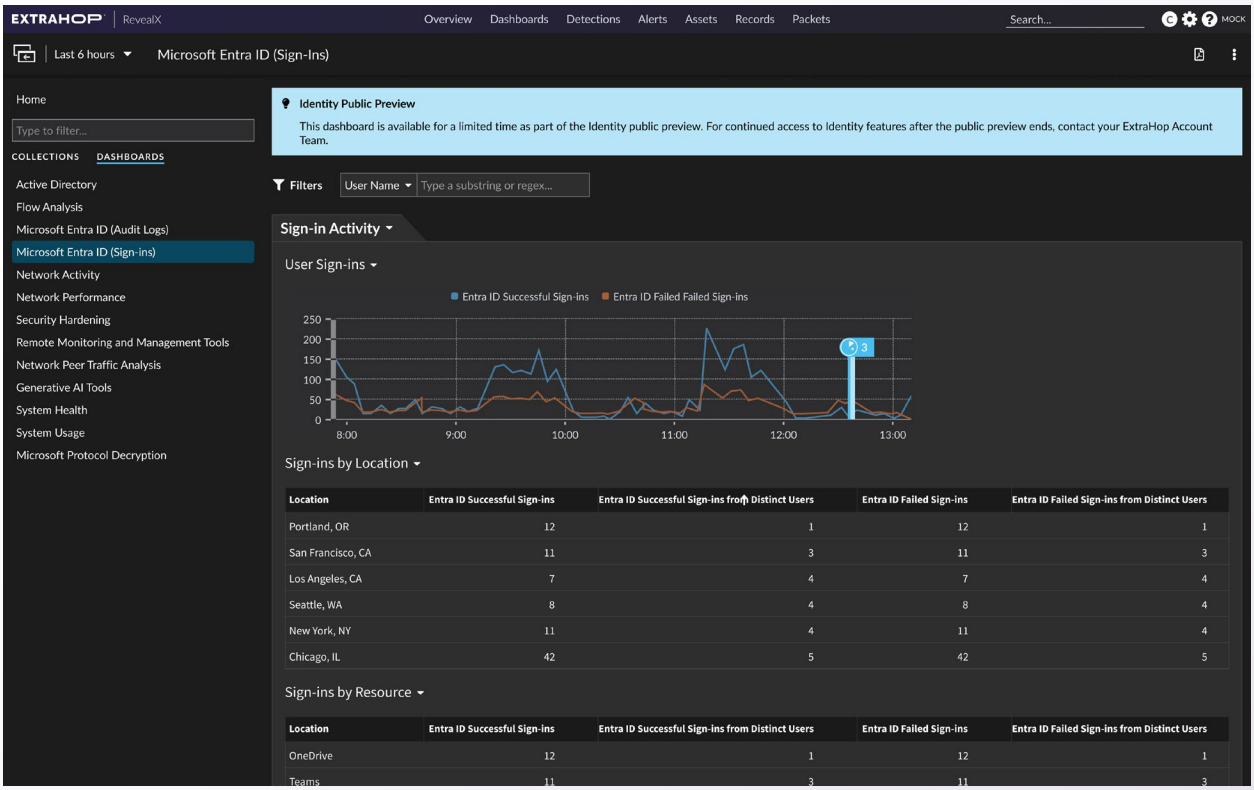

Figure 2. Entra ID Risky User Detections and Dashboards in RevealX

Identity-Powered Detections

With the Entra ID integration, we're introducing a broad set of identity-focused detections that map directly to behaviors analysts care about, such as impossible travel, password spray, anomalous token use, and suspicious file access. Each one provides a clear, actionable signal tied to the specific user involved, so you can move from alert to understanding without extra digging.

Integrated Identity Response for Faster Containment

Once an investigation confirms that a user account has been compromised, time matters. The faster you can cut off access, the smaller the blast radius, but too often that process takes analysts out of flow. You have to leave your detection, open another tool, find the user, and hope your permissions line up to take action.

We're closing that gap by bringing containment options right into the ExtraHop workflow. From the user view, analysts can take direct action through this integration. Analysts can take the following actions to stop further damage and to isolate a potential threat.

- **Revoke User Sessions:** ends active sessions and tokens to immediately disconnect the user from current access points.
- **Disable User:** suspends the account to block new authentications until reinstated.

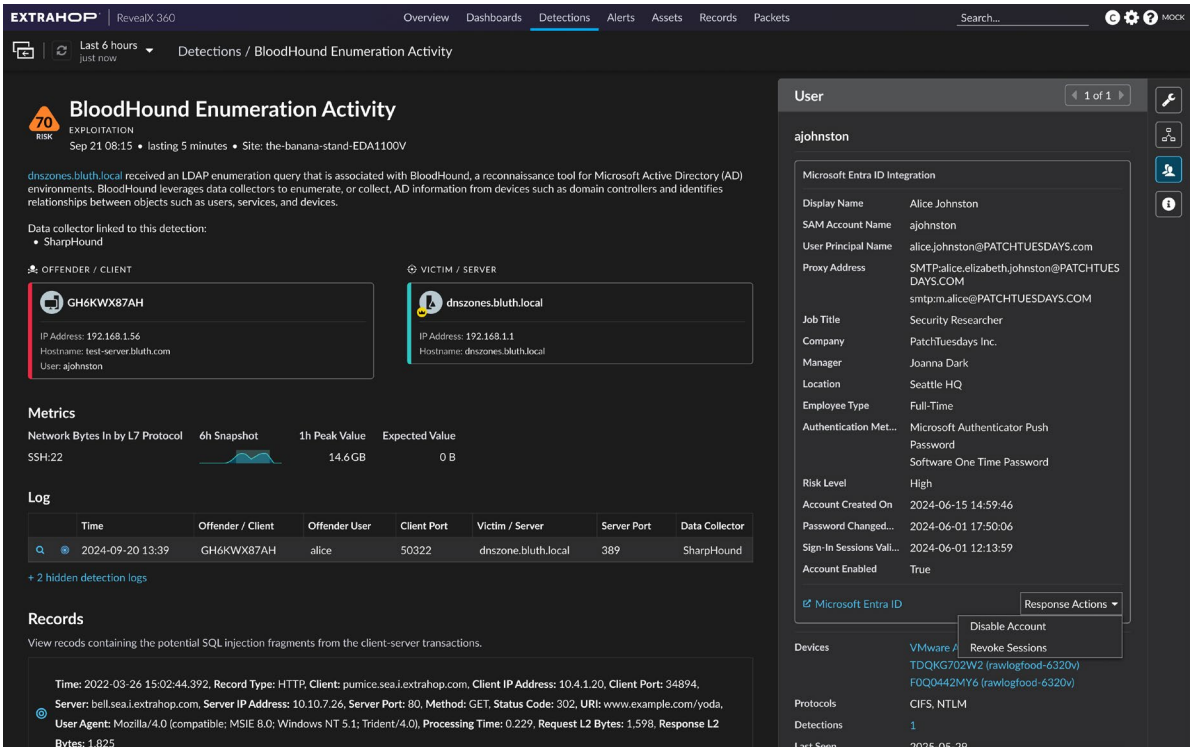

Figure 3. User Enrichment and Response Actions in RevealX

Conclusion

By integrating with Entra ID, we are strengthening ExtraHop's NDR platform to make identity a seamless and powerful part of every investigation.

TAKE THE NEXT STEP

Learn how the integration with Entra ID is designed to improve visibility into authentication activity, enrich user context, and strengthen investigations by connecting identity events across your environment. Visit extrahop.com/demo to schedule a demo.

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. Learn more at extrahop.com.

EXTRAHOP

info@extrahop.com
extrahop.com