EXTRAHOP

# Arming Your SOC to Defeat Advanced Identity Attacks

SOLUTION BRIEF

The security landscape has fundamentally shifted, and the perimeter, once defined by firewalls and network boundaries, has become vulnerable. Today, identity stands as the new perimeter, yet visibility into this critical domain often lags behind.

The harsh reality is that identity-based attacks, once limited to advanced threat groups, are now common practice. These attacks exploit compromised credentials and Identity Access Management (IAM) systems to escalate privileges and move laterally, often evading detection and gaining access to your organization's most sensitive data, and posing a significant risk to your organization.

## The Evolving Threat Landscape: Why Identity Is Your Toughest Challenge

Despite identity being at the center of modern attacks, security teams consistently report struggling to investigate identity-based threats. This isn't surprising when you consider that over 80% of breaches involve compromised identities.*

Threat actors understand this shift better than anyone. They exploit compromised credentials, conceal their actions by encrypting them within legitimate tools, leverage lateral movement techniques to evade detection, and escalate privileges to achieve their objectives. If you can't see into your encrypted east-west traffic and trace these patterns back to a specific user or account, it becomes exponentially harder to understand the full scope of an incident and what actions to take next.

Your current tools, often siloed and lacking deep identity context, force your analysts into a "swivel chair" investigation process, constantly switching between multiple security tools to piece together a complete picture of events. This inefficiency slows down investigations and can lead to missed threats.

## Bringing Identity Into Focus for Faster Investigations

ExtraHop is designed to bring identity context directly into every step of your investigation workflows, providing you with a clear, real-time picture of account activity across your network without relying on endpoint agents.

Identity-aware NDR enables precise investigation of suspicious user behavior by providing you with a holistic view of associated devices, protocols, and detections, eliminating the need for multiple tools.

## CUSTOMER BENEFITS

**Faster Investigations and Response**
ExtraHop brings identity context directly into investigation workflows, providing a clear, real-time picture of account activity and automatically connecting users with devices, allowing you to trace the "blast radius" of a compromised account.

**Confident Lateral Movement Detection**
SOC teams can confidently confirm lateral movement by identifying users accessing multiple hosts via common encrypted east-west protocols.

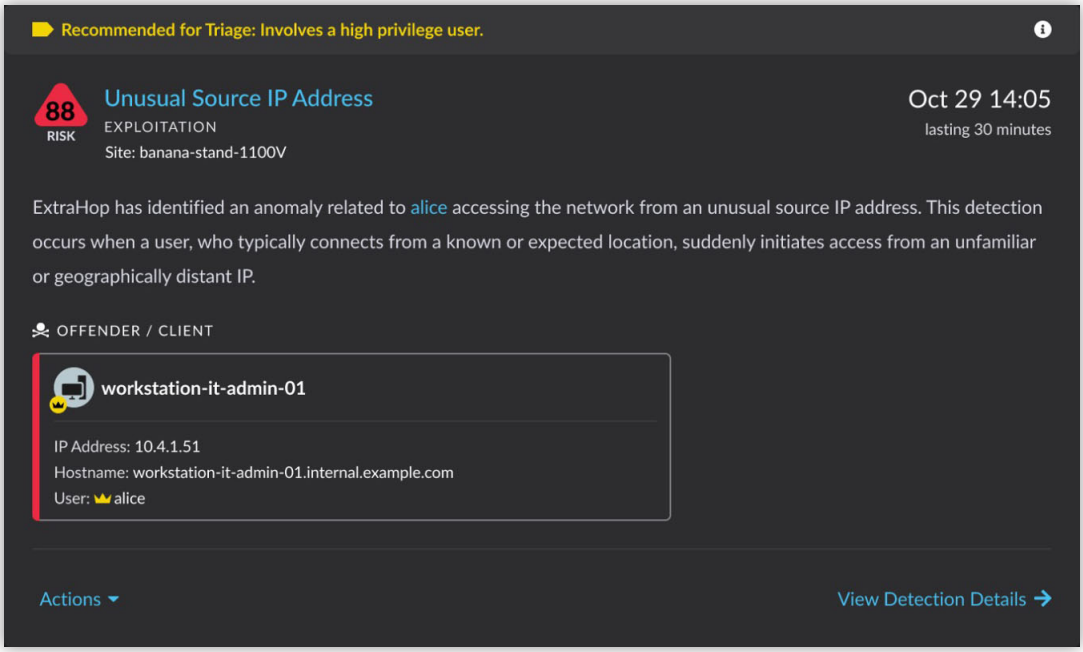
**Prioritize Privileged and High-Risk Users**
Detections can be filtered and tuned based on specific usernames, allowing security teams to prioritize high-risk accounts and reduce noise from less critical service accounts. This ensures critical identity-driven threats involving privileged users are triaged and investigated promptly.

**Centralized Visibility and Threat Hunting**
Users and their metadata are visible and searchable in one place, enabling identity-based threat hunting and a deeper understanding of user activity across the network.

*Verizon 2024 Data Breach Investigations Report

The ExtraHop RevealX™ platform empowers you to confidently confirm lateral movement by identifying users accessing multiple hosts via common encrypted east-west protocols. In the event of a compromise, you can quickly understand the blast radius by identifying all devices accessed by a user during an attack, allowing for accurate scoping of potential system impact.

You can easily prioritize investigations and reduce noise by filtering detections for strategic users and allowlist known noisy accounts. This includes automating detections involving privileged users by surfacing them at a higher priority, ensuring critical identity-driven threats are triaged and investigated promptly.




Designate privileged and influential users within ExtraHop RevealX to prioritize identity-based detections for triage.

## Deepening Your Defenses: ExtraHop's Expansive Detection Coverage

ExtraHop's strength in identity-based attack detection is rooted in its robust understanding and coverage of Active Directory tools and techniques. Attackers employ a range of sophisticated tools and techniques to compromise identity systems. They utilize legitimate tools such as BloodHound, SharpHound, and Mimikatz to evade detection and identify vulnerabilities within these systems.

Attackers use methods like Kerberoasting or AS-REP Roasting to acquire user credentials. They also engage in ticket forgery, including Golden, Silver, and Diamond Tickets, to establish persistence and escalate privileges. These actions facilitate their objectives, which include credential theft, privilege escalation, evasion of defenses, lateral movement across networks, data exfiltration, and maintaining persistent access. Ultimately, their goal is to achieve complete control over the identity infrastructure.

### IDENTITY-BASED USE CASES

- Defending Privileged Users
- Catching Ransomware Attacks
- Understanding "Blast Radius"
- Investigating Phishing-Driven Compromises
- Monitoring Watchlists
- User Containment and Quarantine
- Investigating Credential Abuse
- Detecting Privilege Escalation
- Stopping Identity-Based Lateral Movement
- Preventing Data Exfiltration

## KEY CAPABILITIES

**Real-Time Identity Insights**
ExtraHop automatically discovers and attributes user identities to network activities by analyzing traffic from sources like Active Directory.

**Cloud-Scale Machine Learning**
Leverage advanced ML to continuously monitor petabytes of telemetry and identify suspicious behavior related to identity-based attacks that can bypass traditional security tools.

**High-Fidelity Detections**
ExtraHop uses a combination of anomaly, behavioral, statistical, and rules-based logic to trigger high-fidelity detections around the most pervasive AD tools and techniques like Impacket, Mimikatz, and BloodHound, as well as advanced techniques like Kerberoasting, remote command execution, SMB named pipe abuse, golden and silver ticket forging, DCSync attacks, and more.

**Suspicious Behavior Tracking**
Track user behavior across the network, viewing device interactions and encrypted protocol usage (SMB, RDP, NTLM, Kerberos, etc.) within a single interface to spot anomalies.

**Automated Recommended Triage**
Detections are automatically prioritized involving privileged or influential users to a higher priority level, so SOC analysts can quickly triage the most critical identity-driven threats.

**Enhanced Alert Efficacy**
Detections can be filtered and tuned based on specific usernames or tags, including watchlists, allowing your security teams to prioritize high-risk accounts and reduce noise from less critical service accounts.

**Visibility Into ZScaler Connections**
Integrates with ZScaler ZPA to provide continuous visibility on suspicious identities and device behavior across the SSE environment.

**MITRE ATT&CK Mapping**
Detected activities are mapped to the MITRE ATT&CK framework, providing context on how a user's behavior fits into known attack patterns and kill chain stages.

## Your Command Center for Identity Investigation

ExtraHop makes identity a seamless and powerful part of every investigation, giving analysts richer context, sharper pivots, and faster insights. We provide your security teams with easy-to-understand, structured information about user activity derived directly from network traffic in a simple-to-use table format that you can pivot from to investigate suspicious activity. From this central location, you can:

- **Gain Top-Level Insights:** Quickly gather insights into user activity, including the number of detections associated with a user, their last seen time, and a list of devices and their associated users.
- **Identify Suspicious Patterns:** This information helps you correlate how users are active on the network and understand their behavior patterns, enabling you to identify suspicious activity, whether it's a single event or a broader trend.

## Customizing Your Defenses

ExtraHop understands that while its platform provides objective insights into network activity, your analysts possess the subjective understanding to determine what truly constitutes suspicious behavior. This is why the platform makes it easy to tune detections based on username. This functionality allows you to:

- **Refine Your Detection List:** Streamline your detection list by adjusting for low-value detections.
- **Cut Through Noise:** Reduce the noise created by usernames tied to frequently triggered detections and notifications.
- **Quickly Manage Tuning Rules:** Easily add or edit usernames for tuning rules or detection notifications, and hide specific username participants in detections without hiding the entire detection.

## Evolving Identity Visibility: A Future-Forward Approach

ExtraHop is continuously investing in expanding its identity coverage to include more environments and context. This includes comprehensive support for hybrid identity environments, integrating user information from both on-premise identity providers like Active Directory and cloud-based systems like Entra ID and Okta. These integrations enable seamless tracking of user activity across various domains and enriched context for investigations, offering a clearer picture of behavior throughout your environment.

Future enhancements will focus on detecting anomalies in user and service account behavior to flag potential compromises or insider risks. Additionally, ExtraHop will continue to research the misuse of session tokens by analyzing decrypted network traffic, helping analysts uncover credential theft even when other identity tools fail. The platform also offers the ability to take action, including isolating users and quarantining threats to provide SOC analysts the ability to investigate without having to impact the business.

## Stop Credential Abuse in Its Tracks. Lead with Confidence.

By connecting users to threats, devices, and impact, ExtraHop provides you with the visibility you need to investigate faster, hunt smarter, and ultimately stop credential abuse in its tracks. Our goal is to help you facilitate identity-aware investigations, allowing users to start with a specific user or account and trace their activities, behavioral shifts, and presence across the network. In a world where identity is the new perimeter, ExtraHop empowers you to lead with confidence.

To see ExtraHop RevealX in action, schedule a demo at extrahop.com/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**