EXTRAHOP | Microsoft

Network Ground Truth for the Microsoft Security Stack

ExtraHop RevealX™ adds decrypted network evidence across the Microsoft security stack



SOLUTION BRIEF

Attackers Move Between Your Microsoft Tools.

Defender protects endpoints. Entra ID governs identity. Sentinel correlates signals. Attackers move through the territory between those tools: encrypted Kerberos, NTLM, and MSRPC traffic, unmanaged devices, and east-west paths in Azure and the data center. Credential abuse appears in 39% of breaches, according to the Verizon 2026 Data Breach Investigations Report. Mandiant's M-Trends 2026 found that the median hand-off from initial access to a secondary threat group fell to 22 seconds in 2025.

Analysts and AI agents working from endpoint and log data alone reason over half the story. Attackers can disable agents and erase logs.

The Network Is the Ground Truth.

Every attack crosses the network. ExtraHop RevealX Network Detection and Response (NDR) runs agentless and out of band, leaving an attacker on the host with no sensor to switch off. RevealX decrypts TLS 1.3 traffic, including sessions protected by perfect forward secrecy. RevealX reconstructs full L2–L7 transactions across more than 90 protocols at line rate.

More than 450 machine learning and behavioral detectors, mapped to more than 150 MITRE ATT&CK® techniques, surface lateral movement, credential abuse, command-and-control, and living-off-the-land activity as it happens. Every detection carries the records and packets behind it. Automated Retrospective Detection rechecks stored traffic when a new indicator emerges.

One Platform Across the Microsoft Stack.

RevealX shares context with Microsoft Defender, Microsoft Sentinel, Microsoft Entra ID, and Active Directory. RevealX also runs in Azure. RevealX correlates once, upstream, and every Microsoft tool and every agent works from the same decision-grade intelligence.

WHY MICROSOFT SECURITY TEAMS NEED NETWORK DATA

- Out-of-band sensors keep recording when attackers disable endpoint agents
- Unmanaged devices and Azure workloads sit outside endpoint coverage
- Credential abuse hides inside encrypted Microsoft protocols

WHAT YOU GAIN

- Defender and Entra ID context inside every RevealX investigation
- Decision-grade network detections in Microsoft Sentinel
- Decrypted Kerberos, NTLM, LDAP, RPC, SMB, and WSMan traffic

How RevealX Works With Microsoft

Five integration points connect RevealX to the Microsoft stack. Every integration point has its own solution brief.

Microsoft Defender

Defender device properties and detections appear beside network detections in every RevealX investigation. One-click links open Microsoft Defender.[1] **Read the brief**

Microsoft Sentinel

Risk-scored, MITRE-mapped RevealX detections flow into Sentinel with a ready-made workbook and a triage analytics rule. Every detection links back to the records and packets. **Read the brief**

Microsoft Entra ID

Entra ID user, sign-in, and risk context, including Microsoft 365 sign-ins, appears on every RevealX user. Analysts disable accounts and revoke sessions from the detection. **Read the brief**

Active Directory

Kerberos and NTLM keys from your domain controllers let RevealX decrypt LDAP, RPC, SMB, and WSMan traffic. Decrypted sessions expose Kerberoasting, DCSync, and pass-the-hash. **Read the brief**

Azure and Hyper-V

RevealX virtual sensors, packetstores, recordstores, and consoles deploy in Azure for agentless visibility into Azure workloads. Virtual sensors also run on Hyper-V in the data center. ExtraHop is a Microsoft partner in the Azure virtual network TAP preview.[2] **Read the blog**

Context Your AI Agents Can Act On

RevealX reaches SOC agents through a REST API, an MCP server, and a CLI. Entities arrive joined, with identity resolved and risk and MITRE mapping precomputed.

1. Defender integration requires ExtraHop firmware 26.4 or later.
2. Self-managed Azure sensors connect to RevealX Enterprise or RevealX 360.

Without ExtraHop	With ExtraHop + Microsoft
Defender sees the host, and traffic between hosts stays dark	RevealX shows what moved between devices, with Defender context on each one
Credential abuse in Kerberos, NTLM, and MSRPC looks normal in metadata	Active Directory decryption exposes Kerberoasting, DCSync, and pass-the-hash
Entra ID records the sign-in, and the account's next moves go unseen	RevealX ties every device, protocol, and detection to the user and disables the account on demand
Sentinel receives raw logs that still need correlation	Sentinel receives pre-correlated, risk-scored detections linked to packets

ABOUT EXTRAHOP

ExtraHop is a leader in real-time network intelligence, giving organizations the high-fidelity context to power security and IT AI automation, detect risks faster, and respond with confidence. AI agents rely on ExtraHop's real-time, ground-truth data to operate reliably in the SOC and NOC. For security teams, that means surfacing threats and definitive evidence to investigate them at machine speed. For IT operations, it means resolving performance issues in seconds. Engineered for unmatched scale, the ExtraHop RevealX platform delivers a unified view of the network across data centers, campus, branch, cloud, and AI environments. To learn more, visit **extrahop.com** or follow us on **LinkedIn**.

EXTRAHOP®

info@extrahop.com
extrahop.com

© 2026 ExtraHop Networks, Inc., RevealX and ExtraHop are registered trademarks or trademarks of ExtraHop Networks, Inc. in the United States and/or other countries. All other products are the trademarks of their respective owners. 1235A 10.28.26