EXTRAHOP | Microsoft Defender

Network Ground Truth for Microsoft Defender

ExtraHop RevealX™ adds decrypted network evidence to every Microsoft Defender investigation



SOLUTION BRIEF

The Attacker Is Already Inside.

Attackers exploit the protocols Windows environments rely on every day. Kerberos, NTLM, LDAP, and MSRPC carry their reconnaissance, credential theft, and remote execution. One compromised account can become a domain-wide breach before the SOC can respond.

Mandiant's M-Trends 2026 found that the median hand-off from initial access to a secondary threat group dropped to 22 seconds in 2025. ExtraHop tracks 23 known EDR evasion tools that attackers use to disable endpoint controls.

Microsoft Defender for Endpoint delivers essential host-level telemetry. Activity between devices, on unmanaged assets, and inside encrypted Microsoft protocols needs independent network evidence that a compromised host can't alter.

The Network Is the Ground Truth.

ExtraHop RevealX Network Detection and Response (NDR) analyzes network traffic continuously and out of band, beyond the reach of attackers who disable host controls. RevealX decrypts TLS 1.3 traffic, including sessions protected by perfect forward secrecy. The Active Directory integration adds decryption of LDAP, RPC, SMB, and WSMan traffic. RevealX reconstructs L2–L7 transactions across more than 90 protocols at line rate.

More than 450 machine learning and behavioral detectors, mapped to over 150 MITRE ATT&CK® techniques, surface lateral movement, credential abuse, and command-and-control as they unfold. Every finding links to the records and packets behind it.

Network Context Meets Endpoint Control.

The Microsoft Defender integration connects RevealX to Defender for Endpoint through
The Microsoft Defender integration connects RevealX to Defender for Endpoint through the Microsoft Graph security API. Defender device context and detections appear in every RevealX investigation. Integrations with Microsoft Sentinel and Microsoft Entra ID add SIEM and identity context. Analysts investigate and respond faster, with evidence behind every decision.

WHY DEFENDER CUSTOMERS NEED NETWORK DATA

Out-of-band sensors keep recording when attackers disable the endpoint agent

Unmanaged, IoT, OT, and BYOD devices run without Defender

Credential abuse hides inside encrypted Kerberos, NTLM, and MSRPC traffic

WHAT YOU GAIN

Defender device properties and detections inside every RevealX investigation

One-click pivots into Microsoft Defender

Network evidence for unmanaged devices and encrypted Microsoft protocols

The Best NDR for Microsoft Defender Customers

The Microsoft Defender integration connects ExtraHop RevealX to Microsoft Defender for Endpoint through the Microsoft Graph security API. Endpoint and network evidence meet in one investigation.

Defender Context in Every RevealX Investigation

RevealX imports Defender device properties for each device running Defender: hostname, OS platform, recent and external IP, asset group, tags, and device type. Properties appear on the Device Overview page and work as search filters. Analysts scope an incident by asset group, tag, or device type in seconds.[1]

Endpoint and Network Detections, Side by Side

Defender detections appear next to ExtraHop detections for each participant device on the Detection Details page. Analysts see host activity and network activity in one view.[1]

One Click to Microsoft Defender

Device and detection links open the matching device or alert in Microsoft Defender. Analysts move from network evidence to endpoint response in one click.[1]

Decrypt the Microsoft Protocols Attackers Abuse

The Microsoft Active Directory integration retrieves Kerberos and NTLM keys from your domain controllers. RevealX uses the keys to decrypt LDAP, RPC, SMB, and WSMan traffic. Decrypted sessions expose Kerberoasting, DCSync, pass-the-hash, and remote execution that look normal in metadata.

See Every Device, Managed or Unmanaged

RevealX discovers and classifies every device communicating on the network, including unmanaged, IoT, OT, and BYOD devices and ephemeral workloads. Devices running Defender carry Defender properties in RevealX. Devices missing those properties are the unprotected targets attackers look for.

Evidence That Survives EDR Tampering

The network record remains when an attacker disables an agent or wipes logs. Every RevealX detection links to the transaction records and packets behind it. Automated Retrospective Detection looks back through stored traffic when a new indicator of compromise is published.

Built for the Microsoft Security Stack

RevealX also sends detections to Microsoft Sentinel through a dedicated integration (see the RevealX + Microsoft Sentinel brief). The Microsoft Entra ID integration correlates user properties, sign-ins, and risk detections with network activity. Analysts can disable accounts and revoke sessions from RevealX (see the RevealX + Microsoft Entra ID brief).[2]

Context Your AI Agents Can Act On

RevealX reaches SOC agents through a REST API, an MCP server, and a CLI, published at github.com/extrahop. RevealX joins entities, resolves identity, and precomputes risk and MITRE mapping before an agent asks. Each agent receives a conclusion with the evidence attached.

1. Requires ExtraHop firmware 26.4 or later connected to ExtraHop Cloud Services; Microsoft Defender for Endpoint Plan 2 or Microsoft 365 E5; and a Microsoft Entra application with the ThreatHunting.Read.All Microsoft Graph permission.
2. Available as part of the ExtraHop Identity public preview.

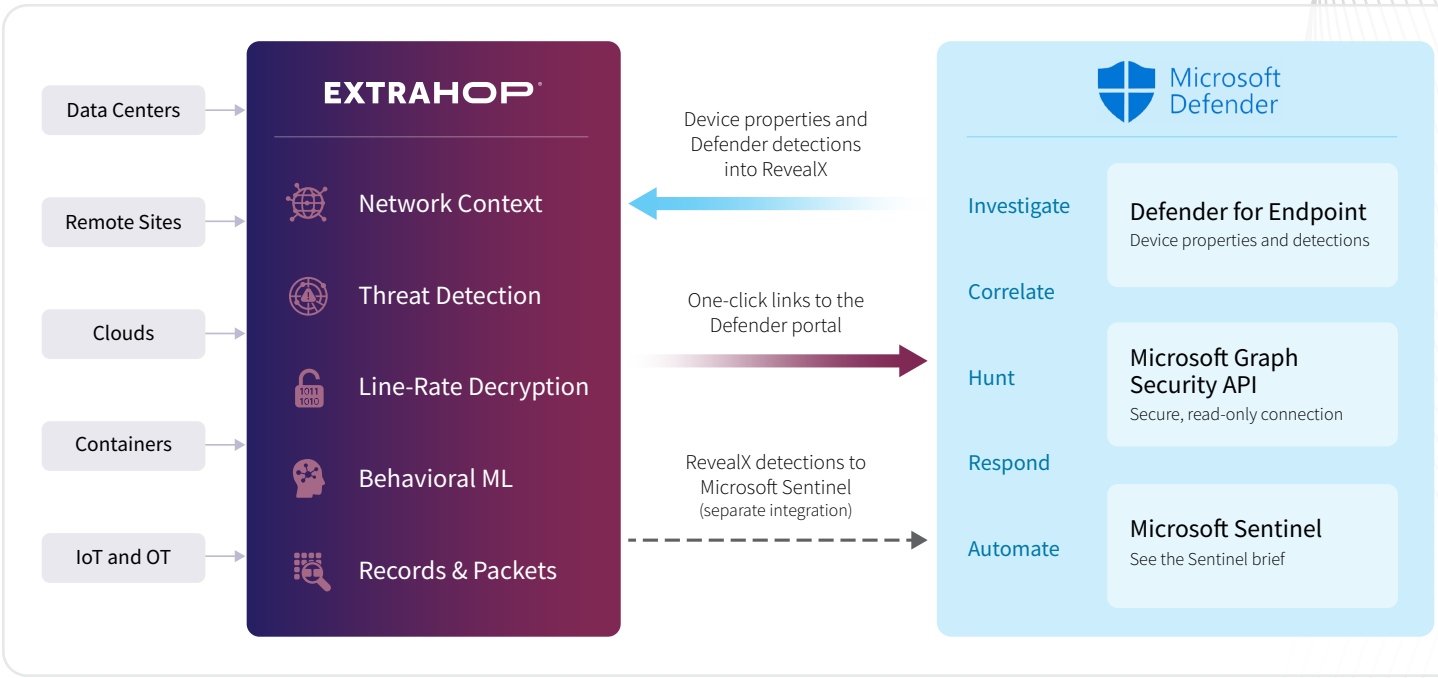


Figure 1: Defender device context and detections flow into RevealX. One click takes analysts back to Microsoft Defender.

Without the Integration	With ExtraHop + Microsoft Defender
Analysts swivel-chair between Defender and network tools to rebuild each incident	Defender device properties and detections sit beside network detections in one investigation
An attacker who disables the agent leaves that host dark	Out-of-band sensors keep recording, with records and packets behind every detection
Unmanaged, IoT, OT, and BYOD devices never appear in Defender	Every communicating device is discovered and classified, with or without an agent
Kerberos, NTLM, and MSRPC abuse looks normal in metadata	Decryption of Microsoft protocols exposes Kerberoasting, DCSync, and pass-the-hash
Endpoint, identity, and SIEM evidence sit in separate tools	Defender, Entra ID, and Sentinel integrations share one network ground truth

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. 1232A 10.30.26