EXTRAHOP | Microsoft Sentinel

Decision-Grade Context for Microsoft Sentinel

ExtraHop RevealX™ sends Microsoft Sentinel risk-scored detections linked to packet-level evidence



SOLUTION BRIEF

Logs Record Events. The Network Records Evidence.

Microsoft Sentinel gives the SOC one place to correlate signals across the enterprise. Logs record observations, and analysts still have to reach the verdict. Logs arrive late, get tampered with, or never exist for unmanaged devices and encrypted east-west traffic. Mandiant's M-Trends 2026 documented the BRICKSTORM backdoor reaching dwell times of nearly 400 days, far beyond a typical 90-day log retention window.

Analysts and their AI agents need trusted conclusions and defensible evidence. Re-correlating raw network data on every query adds cost and delay.

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 re-checks stored traffic when a new indicator emerges.

ExtraHop Correlates Once. Sentinel Acts Everywhere.

RevealX correlates upstream, joining entities, resolving identity, and scoring risk before a detection leaves the platform. Microsoft Sentinel receives a compact, high-fidelity detection. Sentinel then applies its own analytics, automation, and retention across the rest of your security data.

WHY SENTINEL NEEDS NETWORK DATA

- Logs miss unmanaged devices and encrypted east-west traffic
- Attackers wipe logs and outlast short retention windows
- Raw network telemetry adds ingest cost without adding verdicts

WHAT YOU GAIN

- RevealX detections recommended for triage, raised as Sentinel alerts
- A ready-made ExtraHop Detections Overview workbook
- One click from any alert to the records and packets behind it

The Best NDR for Microsoft Sentinel Customers

The ExtraHop RevealX for Microsoft Sentinel app in the Azure Marketplace deploys an Azure Function to receive RevealX detections. The app also installs ready-made Sentinel content.*

Network Detections in Your Sentinel Workspace

Detection notification rules in RevealX 360 or RevealX Enterprise send detections to your Sentinel workspace as webhooks over HTTPS (TCP 443). Rules send directly or through a connected ExtraHop sensor acting as a proxy.

Send What Matters and Filter the Rest

Filters choose which detections reach Sentinel: recommendation for triage, minimum risk score, detection type or category, MITRE technique, offender, victim, device role, participant, or site. Teams use the default payload or define a custom JSON payload.

Detections With Context Attached

Each detection arrives with its title, description, risk score, categories, MITRE techniques, and RevealX triage recommendation. Each detection also lists the hostname, IP address, MAC address, role, and username of every offender and victim.

Alerts Prioritized for Triage

The included analytics rule, “Generate alerts based on ExtraHop detections recommended for triage,” raises Sentinel alerts with severity mapped from the RevealX risk score: Low (1–30), Medium (31–79), and High (80–99).

ExtraHop Detections Overview Workbook

A ready-made workbook shows recommended and total detections, maximum risk score, top detection categories and MITRE techniques, top sources and destinations, and recent detections. Analysts see network risk at a glance.

One Click From Alert to Evidence

Every detection carries a link back to RevealX. Analysts move from the detection to the transaction records and then to the packets. Sentinel holds the alert, and RevealX holds the proof.

Correlate and Automate With Microsoft Signals

RevealX detections land in your Sentinel workspace, ready to join with Microsoft Defender, Microsoft Entra ID, and other data sources in KQL. Network findings can trigger Sentinel automation rules and Logic Apps playbooks.

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.

*Requires ExtraHop firmware 9.9.2 or later and the ExtraHop RevealX for Microsoft Sentinel app.

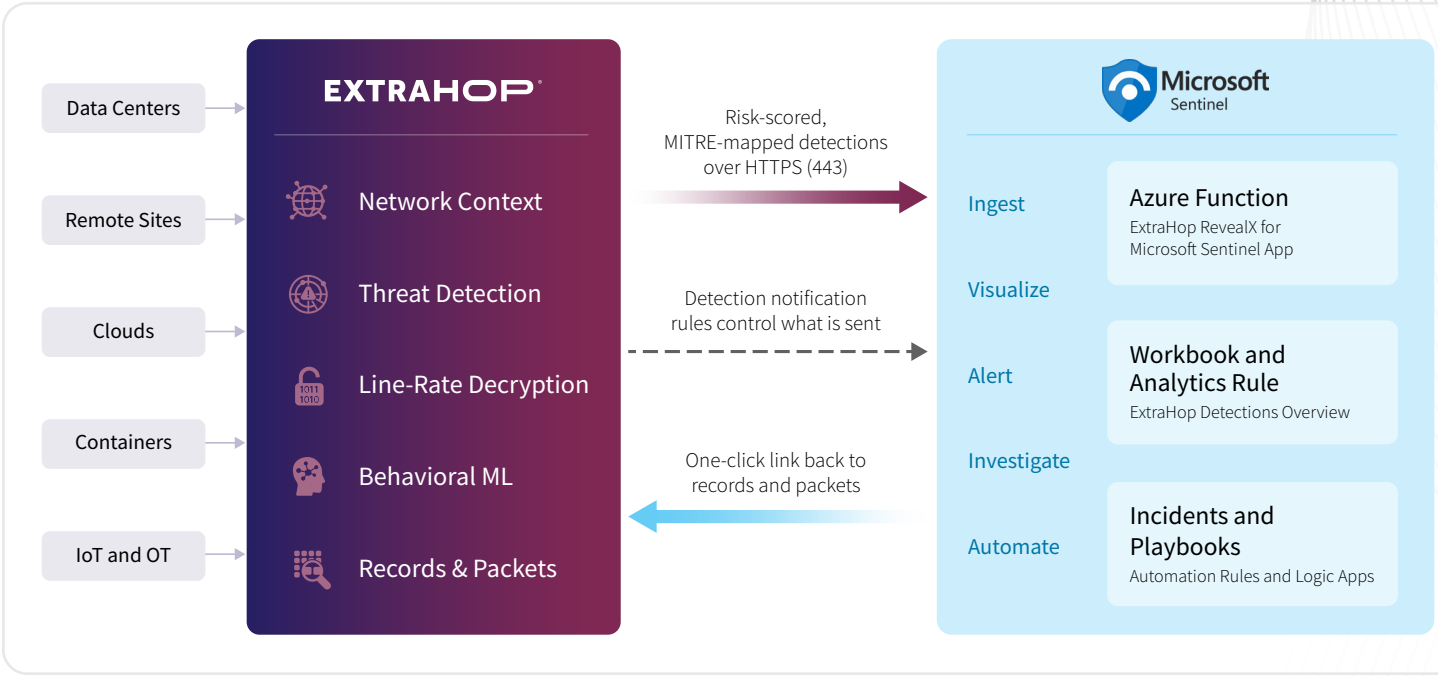

Figure 1: RevealX correlates once, upstream. Microsoft Sentinel receives decision-grade detections linked to the evidence.

Without the Integration	With ExtraHop + Microsoft Sentinel
Encrypted east-west traffic and unmanaged devices never appear in logs	RevealX decrypts east-west traffic and sends its findings to Sentinel
Raw network telemetry inflates ingest and still needs correlation	Compact, pre-correlated, risk-scored detections keep ingest lean
Network alerts arrive without priority	Detections recommended for triage become Sentinel alerts with mapped severity
Alerts lack the evidence to confirm scope	One click from any alert to the records and packets behind it
Logs age out before a long-dwell intrusion is found	Automated Retrospective Detection rechecks stored traffic for new indicators

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. 1092B 11.13.26