ExtraHop + Azure Sentinel

FEATURED INTEGRATION

Enhance Your Cloud-Native Security

Protect your Azure workloads by integrating cloud-native network detection & response (NDR) capabilities from Reveal(x) to Azure Sentinel.

Secure Workloads Across Your Hybrid Enterprise

Supplement the Microsoft Azure Sentinel log data you already have by seamlessly integrating structured wire data and real-time threat detection from ExtraHop Reveal(x).

Reveal(x) leverages the Azure vTap to passively monitor and analyze network traffic in the east-west corridor, filling in visibility gaps left by log- and agent-based tools. With automated asset discovery, classification, and dependency mapping, Reveal(x) provides a complete picture of what's happening across your hybrid environment and helps reduce risks like misconfigurations, insecure APIs, and unauthorized access.

By decoding and analyzing more than 70 protocols and 5,000 features, we keep our cloud-scale machine learning precise and up to date. Reveal(x) then leverages that ML to detect subtle changes in behavior indicative of the threats other security tools miss while eliminating false positives that lead to alert fatigue.

ExtraHop is the only vendor that converts all wire data to a fully indexed record of every element of every transaction. We deliver the largest and richest set of factual and contextualized data to answer the most important questions coming from the Security and Operational teams. No other data source provides the contextual insight you need to get to ground truth faster.

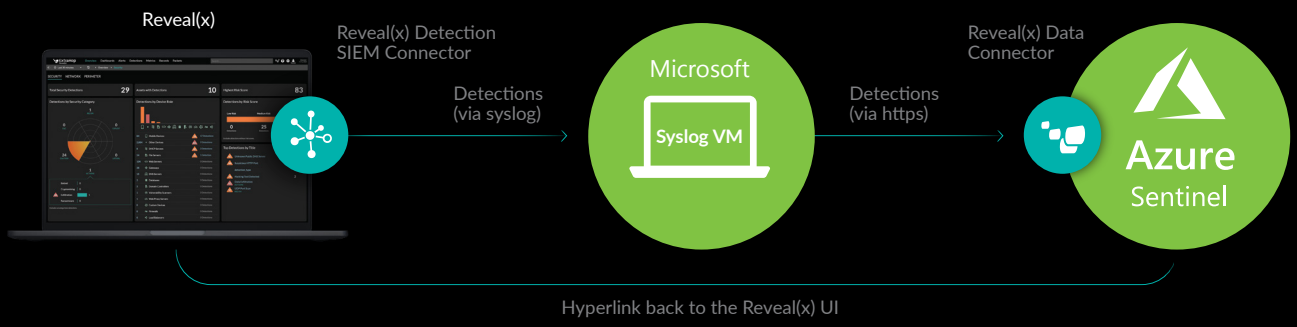
Detect threats up to
95% faster

Reduce time-to-resolve by
59%

Uphold your side of shared responsibility

HOW IT WORKS

Install the Reveal(x) data connector on the Sentinel side, and then install and configure the ExtraHop Detection SIEM Connector bundle to begin streaming data and detections directly to your Azure Sentinel UI.



PLAYBOOK INTEGRATION

High-fidelity alerts and customizable triggering from Reveal(x) enable your team to confidently orchestrate and automate responses through Sentinel Playbooks based on your unique security policies.

WORKBOOK INTEGRATION

You can see a timeline of detections that you've received, as well as a breakdown of detections by category, title, the top participants, and the most common IP addresses from the Sentinel UI.

JUPYTER NOTEBOOK INTEGRATION

SecOps and DevOps can use these highly customizable notebooks to engage in more in-depth investigation or targeted threat hunting by pooling together data from Reveal(x) and other sources.

KEY FEATURES

Reveal(x) cloud-native NDR fills in visibility gaps left by log- and agent-based data, providing a complete picture of your hybrid environment.

Threat Detection

Leverages features from protocols like Azure SQL Databases and Azure Blob Storage to find threats across cloud workloads

Automated Investigation

We automate several investigative steps before analysts even click on a detection so they can get to ground truth faster

Decryption and Decoding

Decrypt all SSL/TLS encrypted traffic and decode 70+ enterprise protocols for comprehensive risk management

ABOUT EXTRAHOP NETWORKS

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Whether you're investigating threats, ensuring the availability of critical applications, or securing your cloud investment, ExtraHop's breakthrough approach helps you rise above the noise so you can protect and accelerate your business. Learn more at www.extrahop.com.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101