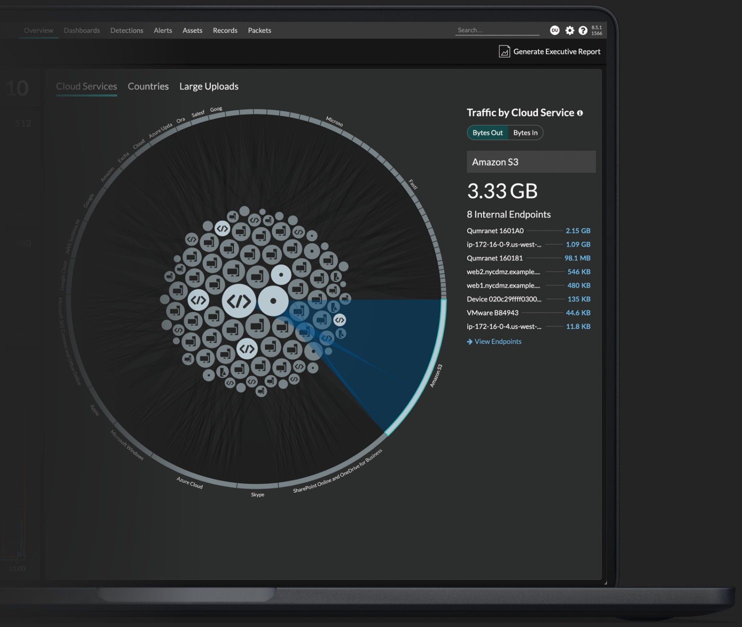
ExtraHop + Azure Sentinel

FEATURED INTEGRATION

Security Uncompromised for Azure Environments

Strengthen your Azure security by adding ExtraHop Reveal(x) 360 SaaS-based network detection and response to Azure Sentinel SIEM.



Traffic by Cloud Service

Bytes Out | Bytes In

Amazon S3

3.33 GB

8 Internal Endpoints

Qumranet 1601A0	2.15 GB
ip-172-16-0-9.us-west-...	1.09 GB
Qumranet 160181	98.1 MB
web2.nycdmz.example....	546 KB
web1.nycdmz.example....	480 KB
Device 020c29ffff0300...	135 KB
VMware B84943	44.6 KB
ip-172-16-0-4.us-west-...	11.8 KB

→ View Endpoints

Supercharge Your Azure Sentinel SIEM with NDR

The ExtraHop + Azure Sentinel integration combines what Reveal(x) 360 does best—eliminating coverage gaps, providing forensic-level investigation, and detecting advanced threats other tools miss—with Sentinel's cloud-native SIEM capabilities.

Reveal(x) 360 provides a unified, seamless security analytics and investigation environment for the cloud: a one-stop shop where SOC analysts can easily track inventory, audit configurations, and pivot from high-fidelity insights to packet-level forensic evidence in seconds.

ExtraHop sensors decrypt and process network traffic and extract metadata for behavioral analysis by cloud-scale machine learning, real-time advanced threat detection, and intelligent response. A cloud-hosted record store with 90-day lookback enables index record search, query, and drill-down investigation. Reveal(x) 360 also offers additional continuous packet capture (PCAP) for in-depth forensics.

By integrating real-time advanced threat detection with Azure Security Center, Structured Threat Information Expression (STIX) data, and automated response solutions, Reveal(x) 360 helps cloud-focused SOCs prioritize security resources and act immediately.

50%

Faster Threat Detection

84%

Faster Threat Resolution

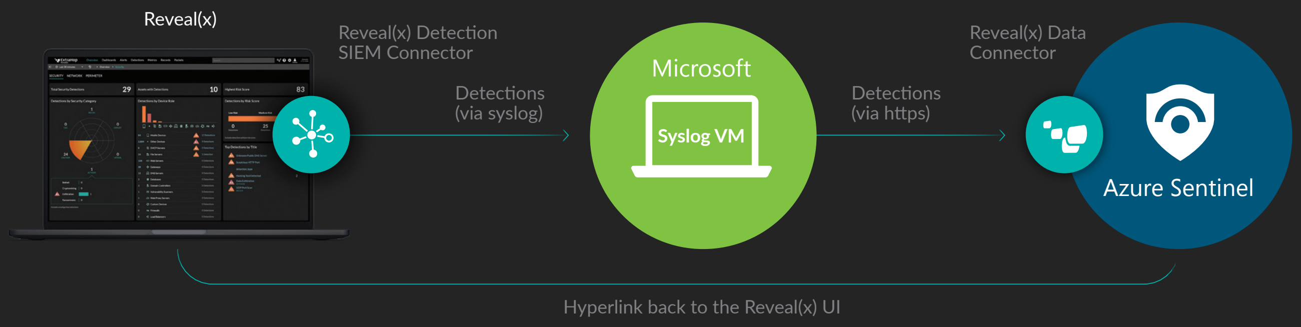
99%

Faster Troubleshooting

FEATURED INTEGRATION

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

Confidently orchestrate and automate responses via Sentinel Playbooks with high-fidelity alerts and customizable triggering from Reveal(x) 360.

WORKBOOK INTEGRATION

Gain instant access to a timeline of detections that includes category, title, top participants, most common IP addresses, and more.

JUPYTER NOTEBOOK INTEGRATION

Enhance investigation and threat hunting by combining network data from Reveal(x) 360 and other sources in customizable notebooks.

KEY FEATURES

Reveal(x) 360 fills in gaps left by log and agent-based tools to defend your Azure and hybrid environments.

Advanced Threat Detection

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

Decryption and Decoding

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

Intuitive Investigative Workflows

Go from detection to ground truth in clicks via one-click investigation to speed response.

Container Security

Gain coverage of pods/tasks and services as well as persistent and ephemeral dependencies in containerized environments.

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, uses cloud-scale AI to help enterprises detect and respond to advanced threats––before they compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised.

ExtraHop
520 Pike Street, Suite 1600
Seattle, WA 98101