ExtraHop Reveal(x) Enterprise

Detection Strategy Guide

July 2025

Product Overview

ExtraHop Reveal(x) Enterprise is a network detection and response (NDR) platform that provides complete visibility, real-time detection, and intelligent response across hybrid and multi-cloud environments. By analyzing network traffic in real-time, Reveal(x) Enterprise decrypts and analyzes all network communications to identify suspicious behaviors and potential threats that other security tools may miss. The platform uses machine learning to baseline normal network activity and automatically detect anomalies, from initial intrusion attempts to lateral movement and data exfiltration. Reveal(x) Enterprise delivers high-fidelity insights and enables security teams to investigate incidents with full context and perform guided investigations, helping to accelerate threat resolution and reduce risk across the enterprise.

Detection Strategy for Network Integrations

Detection

Network traffic monitoring is a critical element of our detection strategy, offering insight into the activity of data as it moves across an organization's systems. The network traffic data source focuses on network connection creation, content, and flow. We pull this information into our detection pipeline as events in the form of both security alerts and raw telemetry (depending on the integration). When a threat is detected, our automated response bot, Ruxie, takes action by enriching evidence fields with first- and third-party threat intelligence.

Response

Network technologies are utilized for support across many types of Expel Alerts such as endpoint and cloud. The main focus of the response strategy is on source IP, destination IP, and domain tracking to identify related connections, along with user activity summaries to give extra alert context.

What We Support for ExtraHop Reveal(x) Enterprise

To see a comprehensive list of the most up-to-date Expel detection rules, vendor detection rules, opt-in detections, and available DUETs (**d**id yo**u** **e**xpect **t**his) that we support for ExtraHop Reveal(x) Enterprise, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported versions	■ All versions
Supported event log sources	■ Alerts
ExtraHop Reveal(x) Enterprise detection rules support	Yes.
Detection rules written by Expel	Yes.
Auto remediations	No.
Investigative support through Workbench	No. We access the console directly with an "Investigator" role account.
Hunting support	No. Hunting is not currently available for this integration.

Additional Details and Common Questions

Console Access

A vendor alert does not typically include all of the contextual timeline activity surrounding the event of interest. Because this integration does not allow us to get all necessary data via the API, we will ask you for a certain level of console access during onboarding.

The level of access that we require is meant to support essential triage and research activities, and to help us determine the vector and extent of attacker activity for an identified threat. At minimum, we will ask for visibility into alert data, timeline events recorded, and live response/real time response shell (if applicable).

DUET

A DUET (**d**id yo**u** **e**xpect **t**his) rule flags certain events as needing an immediate verification or notification, and bypasses the normal internal event triage process. The events subject to DUET rules contain behaviors that are not typically indicative of true security incidents, as they are related to policy violations or *potential* risk.

There are a number of workflows that a DUET may follow. When enabled, the activity will be flagged for investigation and will be routed to you (rather than to us) to take a specified first

action. To see the specific DUET rules currently supported for this integration, visit the Detections page in Workbench.