ExtraHop

PROFESSIONAL SERVICES

Integrations

Reduce Tools Complexity, Increase Productivity and Efficiency With Integrations

The ExtraHop platform is an industry leading Network Performance Management (NPM) and Network Detection and Response (NDR) platform which can be extended through various integrations into your technology stack. The platform comes pre-packaged with several key integrations available and ExtraHop's professional services capabilities further extend the platform's reach into the network, application, and security technology stacks. ExtraHop believes integrations are key to the productivity of its users and works hard to continuously evaluate new integrations to be included both natively in the product, and from field development.

ExtraHop works with customers to scope, develop, test, deploy, and maintain integrations through Professional Services engagements. Integrations that have previously not been developed are available and will be developed on a time and materials basis.

ExtraHop's integrations capabilities are expertly developed, deployed, and maintained through professional services engagements, with support for integrations coming as part of ExtraHop's packaged support offering.

Multiple Options—Many Ways to Support Your Organization's Unique Needs

The Integration service utilizes ExtraHop Professional Services capabilities to implement integrations in one of two tiers. Tier 1 is pre-built in-product integrations that are developed into the product and need to be implemented, while Tier 2 integrations are field-developed and supported for a dynamic set of technology partners. Tier 2 integrations are subdivided into functional categories—EDR (endpoint detection and response tools), perimeter security, SIEM (Security Information and Event Management), SOAR (Security Orchestration and Automation, and Response), and ticketing. Each category contains key integrations developed by ExtraHop Solutions Architects which are developed, tested, maintained, supported, and documented for re-use in the field.

Both options are fully maintained and supported by ExtraHop's global support organization, so you have peace of mind knowing your investment in ExtraHop is supported for the long haul.

In-Product Integrations

Overview

ExtraHop provides several integrations that are natively built into the product and simply need to be customized and implemented for customers in their technical environment. In-product integrations are developed and maintained as part of the ExtraHopcore product in conjunction with our technical design partners with a complete lifecycle approach. ExtraHop continues to add in-product integrations as customers voice their praeference, technical partnerships develop, and use-cases continue to evolve over time.

Currently Available In-Product Integrations

Crowdstrike 360	ExtraHop's integration with the CrowdStrike Falcon platform allows for in-product rapid response, via endpoint isolation, in environments that have CrowdStrike deployed. The CrowdStrike integration is built-in to the ExtraHop platform, and we encourage customers who have also purchased and deployed CrowdStrike to deploy this integration to maximize their investment return and enable a SOC analyst to quickly and confidently respond to a potential incident through an ExtraHop detection.
Splunk	A SIEM integration is core to the functionality of a SOC, and an analyst's ability to triage threats in the environment. ExtraHop's Splunk integration allows analysts to rapidly pull in ExtraHop detection data and metrics to aid in the analysis and alert triage, and provides rich context and information required for decisioning and investigation determinations.
Splunk for SOAR	This integration enables you to export network threat detections from Reveal(x) 360 into Splunk SOAR. ExtraHop's Splunk SOAR integration allows analysts to rapidly pull in ExtraHop data to aid in the analysis and alert triage, and provides rich context and information required for decisioning and investigation determinations.
Office 365	With this integration, customers can import Microsoft 365 and Azure Active Directory detections and events for investigation with the ExtraHop system. Customers can also monitor Microsoft Office 365 metrics in built-in dashboards and view risk event details in records.
QRadar	The ExtraHop integration for QRadar SIEM provides automation to send ExtraHop detections into the QRadar dashboard, centralizing the storage and analysis of network threat data for customers. SOC analysts will be able to view extended detection data as events and incorporate ExtraHop into their investigation and analysis process. Analysts will be able to work seamlessly from the QRadar dashboard to the ExtraHop console when investigating a detection, streamlining process and workflow and increasing efficiency.
Cortex XSOAR	This integration supports customers of the Palo Alto Cortex XSOAR platform, bringing insight from ExtraHop's Reveal(x) 360 device understanding and mapping, as well as threat detections direction into the XSOAR platform. The net positive for the integration is providing customers' SOC analysts already familiar with Cortex XSOAR additional data needed to triage, investigate, and respond to threats in their environments.
Microsoft (Decryption)	Improve detection of security attacks within your Microsoft Windows environment. The integration between ExtraHop Reveal(x) 360 and Microsoft Active Directory enables the decryption of Microsoft protocol traffic to gain visibility to critical network information.

Packaged Integrations

Overview

To further rapidly extend the ExtraHop platform by integrating into more customer environments, ExtraHop Professional Services provides packaged integrations. Packaged integrations are field-developed integrations, created and tested as part of customer engagements by Professional Services product and domain experts. Packaged integrations are fully maintained and supported by ExtraHop as part of customer support.

Currently Available Packaged Integrations Categories

EDR (Endpoint Detection and Response)	Endpoint Detection and Response platforms are a key integration point for ExtraHop. The focus of integrations with EDR tools is to provide automated response, such as containment at the endpoint, upon detection of malicious activity. We provide a number of field-developed and maintained integrations with industry leading EDR vendors.
SIEM (Security Information and Event Management)	Security teams often work from within a unified SIEM console that provides enterprise-wide correlation, investigation, and decisioning capabilities for SOC analysts. ExtraHop integrates our detection information and context so SOC analysts can make decisions faster, and with greater confidence.
SOAR (Security Orchestration, Automation and Response)	SOAR platforms automate key tasks SOC analysts perform such as data enrichment, investigations, containment, or other capabilities. ExtraHop's ability to push detection data into SOAR platforms based on detections enables SOC analysts to scale and perform more efficiently.
Perimeter Security	ExtraHop integrates with key perimeter security vendors to perform various actions, based on detections, such as containment or other critical automation functions.
Ticketing Platforms	Ticketing platforms are a central repository for work related to events and incidents. ExtraHop integrates with various ticketing systems and platforms to push detection data for remediation and automation tasks.

ExtraHop's list of integrations is continuously growing, for an up-do-date list of available integrations contact your ExtraHop Representative.

ExtraHop

info@extrahop.com

www.extrahop.com