ExtraHop + splunk>

FEATURED INTEGRATION

Close Every Visibility Gap in Your Enterprise

Get the most complete picture of your IT and Security environments by combining ExtraHop wire data with logs and other data in Splunk.

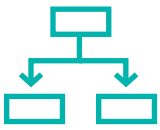
Capture Critical Security and Performance Metrics

Log and agent-based data offer insight into application code and device processes, but they still leave you blind to too many security and performance issues that can only be observed in network traffic. By passively monitoring network communications on-premises and in the cloud, ExtraHop provides complete visibility of what is happening in your hybrid environment.

Integrating ExtraHop with Splunk, Splunk Enterprise, and Splunk Phantom enables continuous capture of critical metrics that can be streamed directly into Splunk:

- Web servers (Apache, Microsoft IIS, and more)
- Network services (DNS)
- Application servers (Apache Tomcat, ASP.NET, Ruby on Rails, and more)
- Mail and collaboration servers (including Microsoft SharePoint)
- Database servers (IBM DB2, IBM Informix, MySQL, Oracle, PostgreSQL, Microsoft SQL Server, MongoDB, Redis, Riak, and Sybase ASE)
- Storage devices (SMB/CIFS, NFS)
- Authentication servers (LDAP, RADIUS, Diameter)
- Network devices (including load balancers and firewalls)

Streaming ExtraHop data into Splunk lowers costs by increasing efficiency in what you log while also providing reliable and high-fidelity insights.



Gain visibility across every application, device, and system

Decrypt all SSL/TLS 1.3 traffic at line rate and out of band

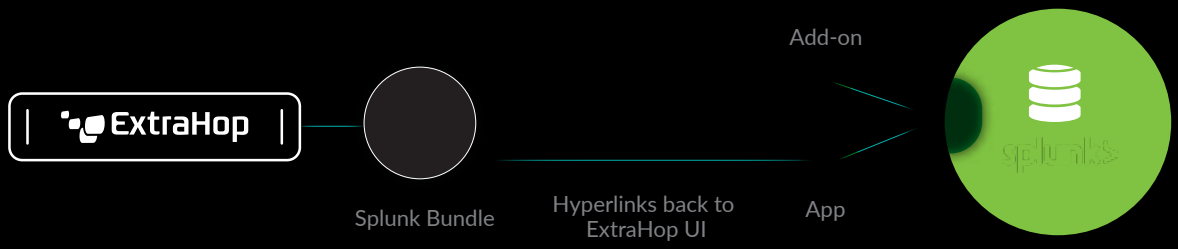
Reduce time to resolve by 59% and time to repair by 85%

ExtraHop + splunk>

FEATURED INTEGRATION

HOW IT WORKS

Install the ExtraHop add-on and app on the Splunk side to pull data via the ExtraHop REST API. You can access metrics from the ExtraHop app tab in Splunk or through the ExtraHop UI.



KEY FEATURES

ExtraHop cyber analytics provide essential security and performance capabilities you can't find anywhere else.

Complete Visibility
Immediate visibility into BYOD and IoT black boxes

Machine Learning
Cloud-scale machine learning to detect anomalous behavior

In-depth Analysis
Detailed transactional data at scale

ELIMINATE DARKSPACE

75% of what happens in your IT environment occurs in the east-west corridor. Adding ExtraHop to your security and performance monitoring stack provides visibility into that internal traffic.

85% reduction in time to **repair** issues

59% reduction in time to **resolve** threats

LINE-RATE DECRYPTION

70% of network transactions and an increasing number of security threats happen in encrypted traffic. ExtraHop decrypts SSL and TLS 1.3 encrypted traffic out of band, enabling safe, meaningful analysis.

ABOUT EXTRAHOP NETWORKS

ExtraHop is the leading provider of cloud-native network detection and response (NDR) for the hybrid enterprise. With complete visibility, real-time threat detections, and automated investigation powered by cloud-scale machine learning, ExtraHop enables security teams at leading enterprises including Credit Suisse, The Home Depot, Caesars Entertainment, and Liberty Global to rise above the noise of alerts, organizational silos, and runaway technology in order to accelerate investigations, unify policies across hybrid environments, and build their security the way they're building their business: cloud-first.

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101