

ExtraHop + sumologic

Gain New Insights Through the Combined Power of Wire and Machine Data



ExtraHop's wire data analytics platform provides a rich source of data for Sumo Logic, the next-generation cloud-based log management and analytics service. The integration enables you to derive deeper and richer IT and business insights from your data. The flexibility, scalability, and ease of deployment of both ExtraHop and Sumo Logic make these best-of-breed solutions a perfect match.

"Bringing ExtraHop data into the Sumo Logic service for proactive analysis and correlating it with other machine data sources enables IT teams to gain unprecedented performance, security and business insights."

— Mark Musselman, Vice President of Strategic Alliances, Sumo Logic

JOINT SOLUTION HIGHLIGHTS

- Augment Sumo Logic's proactive machine data analytics with observed wire data
- Detect anomalies through Sumo Logic and then explore the contextual communications in ExtraHop
- Simplify IT operations with best-in-class analytics solutions that are easy to deploy and maintain

WHAT IS WIRE DATA?

Wire data is all L2-L7 communications between systems, including full bi-directional transactional payloads. It represents a rich but untapped source of visibility for most IT organizations.

RAW PACKETS TO STRUCTURED WIRE DATA

ExtraHop enables your IT organization to tap into the wealth of wire data flowing through its environment, transforming raw packet data into structured wire data at unprecedented rate of 20Gbps. This wire data includes metrics and events such as:

- Transaction and payload analysis
- Database and storage transaction details, such as process time for individual stored procedures
- Web services (APIs)
- Cross-tier correlation metrics
- Network performance and correlation

DEEPER ANALYSIS OF YOUR WIRE DATA

With the ExtraHop Open Data Stream, you can send precise, policy-driven events and metrics to Sumo Logic in real time for multidimensional analysis and correlation with other machine data sources. Streaming wire data from ExtraHop to Sumo Logic will enable you to quickly answer questions such as "What are the slowest stored procedures for my applications?" "Which DNS servers are misconfigured and returning errors?" or "Which Citrix XenApp server is responsible for slow application launch times?"

EXTRAHOP AND SUMO LOGIC: BETTER TOGETHER

The observed data off the wire is deep and rich, but is made much more powerful when paired with Sumo Logic's Anomaly Detection capabilities. IT teams responsible for performance or security can use Sumo Logic to detect unknown issues that would have otherwise gone unnoticed, then switch over to ExtraHop to explore the L2-L7 communications of the devices involved.

TRY EXTRAHOP FREE

Download the ExtraHop Discovery Edition, a free-forever virtual appliance that lets you start exploring what is possible with wire data analytics.

www.extrahop.com/discovery

