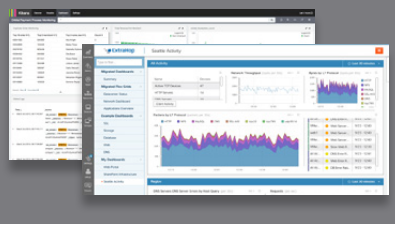
ExtraHop + elasticsearch. logstash kibana

Unleash the Potential of Your Wire Data with a Powerful Analytics Combination



ExtraHop can provide a wealth of real-time wire data for use in the Elasticsearch ELK stack—comprised of Elasticsearch, Logstash, and Kibana—enabling IT organizations to derive even deeper and more meaningful IT and business insights.

"The wire data that ExtraHop's Open Data Stream can send to the ELK stack will allow businesses to combine it with other machine and human-generated operational data, helping them gain a complete picture of their business so they can draw faster, more comprehensive insights."

– Steven Schuurman,
Elasticsearch, CEO

JOINT SOLUTION HIGHLIGHTS

- Send precise wire data events and metrics to Elasticsearch for multidimensional analysis
- Take advantage of unmatched flexibility to build a solution to meet your particular requirements
- Cost-effectively scale out your search and analytics solution with the most scalable wire data analytics platform and Elasticsearch

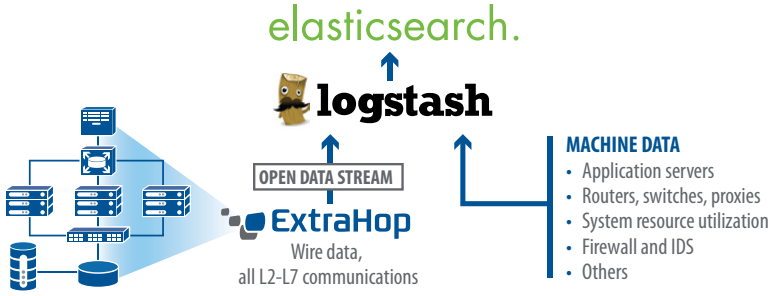
THE EXTRAHOP PLATFORM EQUIPS ALL TEAMS WITH REAL-TIME WIRE DATA

Every day, your organization produces an incredible amount of communications on the wire—every transaction and message passing over the network between devices, applications, and users. What if you could mine these communications for real-time IT and business insights?

The ExtraHop wire data analytics platform transforms raw packet data into structured wire data at an unprecedented rate of 40 Gbps. This enables you to explore and correlate a wealth of events and metrics, such as:

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

With ExtraHop's Open Data Stream capability, you can also send precise, policy-driven events and metrics to Elasticsearch for post-hoc multidimensional analysis and correlation with other data sets.



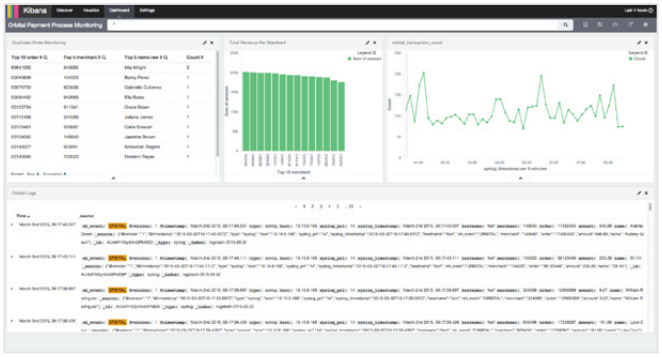
COMBINE WIRE DATA WITH OTHER DATA SETS FOR RICHER INSIGHTS

Thousands of organizations worldwide choose Elasticsearch as a scalable open-source search and analytics engine because of its flexibility and cost-effectiveness. Elasticsearch, combined with Logstash and Kibana, delivers a complete machine data analytics solution.

Wire data provides an objective, outside-looking-in view into availability, performance, and security that you cannot get with logs or other instrumentation of the host. By combining wire data, machine data, and other data sets, you can more effectively accomplish a variety of tasks, including:

- Application development and management
- Security forensics and detection
- Business analytics
- Troubleshooting and root cause analysis
- Performance benchmarking and optimization

ExtraHop UI



Wire data in ELK

WHAT IS WIRE DATA?

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

BENEFITS OF COMBINING EXTRAHOP WITH ELASTICSEARCH

- **Flexibility** – IT organizations that use ExtraHop and Elasticsearch love both platforms for the ease with which they can customize and program those solutions. If you need to solve a problem, you will be able to get it done with ExtraHop and Elasticsearch.
- **Unprecedented Scalability** – Both ExtraHop and Elasticsearch offer unparalleled scalability so that your organization can reap the full benefits of search and analytics. The ExtraHop platform offers continuous analysis of up to a sustained 40 Gbps, or the equivalent of 1.3 million HTTP transactions per second, with bulk decryption at line rate.
- **Cost-Effectiveness** – The combined solution of ExtraHop and the ELK stack frees you from worries about scaling your search and analytics deployment. Due to ExtraHop's server-based licensing model, there are no limits on the amount of wire data you can store and index besides provisioning infrastructure.
- **Data Freedom** – The data is yours; you should consume it in the manner that is most effective for your organization. Your data should not remain locked in a single data store. That's why ExtraHop offers the Open Data Stream capability, which enables you to send your real-time wire data to the data store of your choice, including industry-leading open-source solutions such as Elasticsearch.

READ MORE BY DOWNLOADING THE WHITE PAPER,
Designing and Building an Open IT Operations Analytics (ITOA) Architecture

http://www.extrahop.com/open-itoa/

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

ABOUT EXTRAHOP NETWORKS

ExtraHop is the global leader in real-time wire data analytics. The ExtraHop platform analyzes all L2-L7 communications, including full bidirectional transactional payloads. This provides the correlated, cross-tier visibility essential for today's complex and dynamic IT environments. The ExtraHop platform scales up to 40 Gbps and deploys without agents in 15 minutes.

ABOUT ELASTICSEARCH, INC

Founded in 2012 by the people behind the Elasticsearch and Apache Lucene open source projects, Elasticsearch, Inc. is on a mission to make massive amounts of data usable for businesses by delivering the world's most advanced search and analytics engine. With a laser focus on scalability and ease of use, the Elasticsearch ELK stack—comprised of Elasticsearch, Logstash, and Kibana—has been adopted by thousands of enterprises worldwide for a range of real-time search, log analysis and analytics use cases.