ExtraHop and Splunk

Combining Wire Data from ExtraHop and Machine Data from Splunk for an IT Operations Architecture

Both Splunk and ExtraHop offer new and better ways of gaining visibility for IT operations. Together, these complementary solutions provide complete IT operational intelligence, with ExtraHop transforming wire data into machine data for Splunk.

In enterprise IT, each significant technology is designed and operated according to a deliberate architecture: network and security architecture, SOA and application architecture, and even database and storage architecture. Remarkably, the one place where all these technologies meet, IT operations, typically lacks a planned framework, resulting in massive collections of niche tools, significant gaps in visibility, high coordination costs, and inefficiencies in incident escalation.

Together, ExtraHop and Splunk provide the framework for a rationalized and strategic IT Operations architecture. ExtraHop analyzes and transforms wire data into machine data in real time, including event-driven metrics and payload information that is otherwise impractical or impossible to log. ExtraHop captures metrics for network performance, transaction timing, database internals, file-based storage, and locked-down environments like mainframes. With the flexibility to mine both wire and machine data, IT teams have the complete operational intelligence they need to answer IT and business questions.

> "ExtraHop is a critical source of data. Concur uses ExtraHop to extract the precise information we're looking for and immediately export it to Splunk, where we can perform deep analytics. This combination of wire data and machine data enables us to quickly answer questions that would not be able to answer otherwise."
>
> —John Tharp, Lead Software Configuration Engineer, Concur Technologies
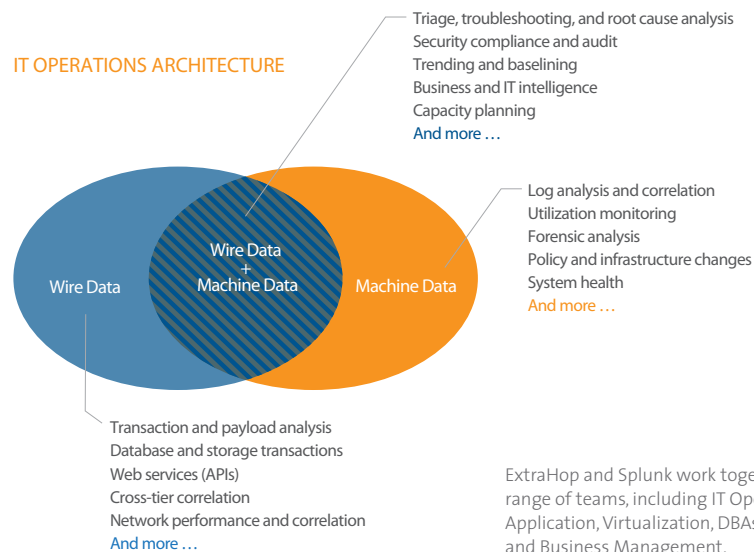
ExtraHop provides correlated, cross-tier visibility for the entire application environment:

- **Web servers (Apache, Microsoft IIS, and more)**
- **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, and Sybase ASE)**
- **Storage devices**
- **Authentication servers (LDAP, RADIUS, and Diameter)**
- **Network services (DNS)**
- **Network devices (including load balancers and firewalls)**

IT OPERATIONS ARCHITECTURE

Triage, troubleshooting, and root cause analysis
Security compliance and audit
Trending and baselining
Business and IT intelligence
Capacity planning
And more …

Log analysis and correlation
Utilization monitoring
Forensic analysis
Policy and infrastructure changes
System health
And more …

Wire Data
Wire Data + Machine Data
Machine Data

Transaction and payload analysis
Database and storage transactions
Web services (APIs)
Cross-tier correlation
Network performance and correlation
And more …

ExtraHop and Splunk work together to empower a range of teams, including IT Operations, Network, Application, Virtualization, DBAs, Storage, Security, and Business Management.

Splunk App for ExtraHop

The Splunk app for ExtraHop enables users to forward transaction-level details from ExtraHop to Splunk through rsyslog. The result is a mechanism for precisely logging the wealth of previously untapped wire data in your environment.

In addition to the precision-logging capability, the extensible Splunk app for ExtraHop collects the following metrics:

- **Web metrics –** Responses over time, average transaction response times, JSON, AJAX, and SOAP/XML payload, status codes with detail, and web traffic throughput

- **Web services metrics –** External and internal API calls, events over time, top active account numbers, top active users, and other customizable metrics such as duplicate order IDs

- **Database metrics –** All methods, queries, response times, transaction response times, errors, top methods, and top users

- **Storage metrics –** Responses over time, average transaction response times, errors, top methods, and top users

- **Memcache metrics –** Transactions over time, average access time, errors, message sizes, top response codes, top methods

You can also add other elements, including the following, to your Splunk app for ExtraHop:

- **Transaction metrics –** Anything in the payload can be measured in real-time for IT operations analytics and business intelligence

- **Mainframe –** MQ and CICS methods, status, and transactions

- **FIX and SMPP –** Transactions, response times, and payload information

Get The Whole Picture

Capture and convert real-time wire data into machine data, and combine it with other machine data from throughout the datacenter in Splunk.

- Log consistent metrics across all tiers, including the network, web, middleware, application, database, memcache, and storage.
- Capture holistic metrics such as end-to-end response time.
- Monitor locked-down environments such as mainframe deployments, including DB2 environments.
- Log payload data, including transaction details such as order ID, merchant ID, and account number.
- Correlate network performance and application performance.

Answer IT and Business Questions

Quickly the find the answers to questions that would be nearly impossible to find otherwise.

- Identify missed business opportunities by analyzing transactional data by account and user.
- Parse data by top methods and top users.
- Define new metrics not available through the logging options available on web, database, and storage servers.
- Gain real-time insight into database performance without having to run profilers.

Simple Deployment

Gain immediate value and minimize total cost of ownership with an elegant network-based deployment.

- Start collecting meaningful events off the wire in as little as 15 minutes with no configuration required and no system overhead.
- Automatically discover and classify applications and devices.
- Avoid brittle agents which can lock you into a specific vendor or version and cost valuable resources to deploy and maintain.

About ExtraHop Networks

ExtraHop provides the real-time operational intelligence required to make IT more agile and proactive. The world's best-run IT organizations use ExtraHop to manage more than half a million devices and monitor over a trillion transactions daily, including Adobe, Alaska Airlines, Concur, Expedia, and Microsoft.

Try ExtraHop for free at www.extrahop.com/discovery.