Using ELK for Operational Intelligence

Just as networks are critical to all kinds of operations, network data is critical to all kinds of operational analysis. Savvius provides industry-leading solutions for network analysis. Now that analysis can be used along with other types of machine data through Savvius’ integration with ELK, an open source software stack for big data search and analysis. The result is powerful, scalable analytics solutions for understanding how networks and operations interact, and how both can be optimized for the benefit of the enterprise overall.
Contents

Executive Summary .................................................................................................................. 3
Overcoming the Barrier to Insight .......................................................................................... 3
  The Importance of Network Data .................................................................................... 3
  Savvius Network Analysis Solutions ........................................................................... 3
  Broadening the Scope of Analysis: Machine Data ......................................................... 4
  Savvius and ELK .............................................................................................................. 4

A Bigger Picture: Network Analysis + Machine Data .......................................................... 5
  Operational Intelligence .................................................................................................. 5
  Business Analytics ......................................................................................................... 6

Use Cases ................................................................................................................................. 7
  Security ............................................................................................................................ 7
  Application Performance Monitoring (APM) .............................................................. 7
  Baselining and Monitoring ........................................................................................... 7
  Centralized Alerting ....................................................................................................... 7

Conclusion ............................................................................................................................... 8
  Learn More ....................................................................................................................... 8
  About Savvius ................................................................................................................ 8
Executive Summary

Networking is the fundamental technology at the core of any business, and network data has become indispensable for any type of comprehensive operational analysis.

Enterprises today use powerful network analysis solutions from Savvius to visualize, troubleshoot, and analyze enterprise networks. Savvius offers two product lines: Savvius Omnipliance® network recorders and analysis appliances (including the Savvius Insight mini-appliance) and Savvius Omnipeek® network analysis software.

Analyzing and improving the efficiency and security of business operations requires insight into non-network data, as well. The data generated by non-human activities, often referred to as machine data, includes log data, configuration files, change events, event streams, and Application Programming Interfaces (APIs).

A popular open source data analysis platform for machine data is ELK, which stands for Elasticsearch, Logstash, and Kibana. Elastic, the company behind ELK, provides an ELK cloud service and support.

With Omnipeek, Savvius solutions can be integrated with ELK, enabling Savvius network analysis to be applied to:

- **Operational Intelligence** — The analysis of machine data to gain insights about an organization’s operations
- **Business Analytics** — Operational intelligence applied to business goals and outcomes
- **Predictive Analysis** — Applying predictive algorithms to machine data to understand trends and future results

Use cases for the Savvius-ELK solution include:

- **Security** — Analyzing data to detect and characterize attacks
- **Application Performance Monitoring** — Understanding service degradations and outages
- **Baselining and Monitoring** — Gaining a long-term understanding of IT performance
- **Centralized Alerting** — Managing network-based alerts with other types of IT alerts

The Savvius-ELK solution offers new data and new insights to enterprises, enabling them to optimize efficiency, security, service, and the networks that make their operations possible at all.

Overcoming the Barrier to Insight

The Importance of Network Data

Data makes a difference.

Not just any data — network data. Networking is the core technology of business today. Every transaction, communication, analysis, and production process touches — and is typically dependent upon — a well-functioning network.

Today’s networks are incredibly complex and impressively intertwined with applications, data storage, hypervisors, websites, firewalls, and a mobile ecosystem that grows daily.

Extracting insight from these environments requires expertise, ideally embedded in analysis tools and presented in a way made useful through contextual awareness, a focus on desired outcomes, and an awareness of the entire hierarchy from low-level network packet data to user actions.

That’s what Savvius does: Create hardware and software solutions that incorporate decades of network experience so that organizations can quickly and easily gain useful insight into their network.

Savvius Network Analysis Solutions

Savvius’ family of Omnipiances enables organizations to record and analyze traffic from 1G, 10G, and 40G networks, supporting both real-time analysis and forensic analysis of past events. Each Omnipiance is capable of capturing terabytes of traffic with no packet loss, creating a reliable record of network activity, even on today’s fastest networks.
Omnippliance analytics include Expert Analysis for monitoring and troubleshooting, voice and video over IP metrics, and popular network metrics such as “Top Talkers” and “Top Protocols.”

Savvius Insight provides packet intelligence in a compact and economical all-in-one appliance perfect for monitoring the performance and security of small business and remote office networks with external data rates up to 100 Mbps.

Savvius Omnipeek network analysis software serves a dual role as both a software console for Savvius Omnipiances and a stand-alone solution for local packet capture and analysis. The software offers an intuitive, easy-to-use graphical interface that engineers can use to rapidly analyze and troubleshoot enterprise networks.

Using Omnipeek’s intuitive dashboards and “top-down” approach to visualizing network conditions, network engineers can quickly analyze faults from multiple network segments, drill down through multiple layers of analysis, and pinpoint problems that need correction. Omnipeek provides centralized Expert Analysis for all networks under management.

With Omnipeek, Omnippliance, and Insight, enterprises have a powerful solution for maintaining the reliability and performance of LANs, WANs, and WLANs.

Broadening the Scope of Analysis: Machine Data

Analyzing and improving the efficiency of business operations requires insight into many kinds of data. The data generated by non-human activities, often referred to as machine data, includes log data, configuration files, change events, event streams, and Application Programming Interfaces (APIs).

Much of the value of machine data comes from the simultaneous analysis and correlation of multiple data sources. One particular data analysis platform for this activity is ELK.

Elastic, the company behind ELK, is a software and cloud-services company that offers a fast, scalable Big Data platform for collecting, analyzing, and acting upon machine data. Elastic is a leading on-premise platform for operational intelligence — actionable insights gained by analyzing the IT and business information available from machine data.

ELK collects machine data from wherever it’s generated, including physical, virtual, and cloud environments. The platform enables users to search, monitor, and analyze data from a central repository in real time. ELK helps enterprises to:

- Troubleshoot problems and investigate security incidents in minutes, not hours or days
- Monitor end-to-end infrastructure to avoid service degradation or outages
- Gain operational intelligence with real-time visibility and critical insights into customer experience, transactions and other key business metrics

ELK, Elastic’s Software as a Service (SaaS)-based alternative, breaks down the data silos that have been hampering operational intelligence.

Savvius and ELK

The ELK stack can only be as effective as the data available to it. When it comes to networks, there is no substitute for analytics derived directly from the network traffic. That’s where Savvius comes in.

Savvius Omnipeek enables Savvius customers to integrate Savvius network analysis with ELK. The result is a fast, scalable, and comprehensive data analysis platform that provides a more complete picture of IT and business activity, combining Savvius’ network data and Expert analysis with other machine data collected and analyzed by ELK.
A Bigger Picture: Network Analysis + Machine Data

The integration of Savvius and ELK provides enterprises with a new opportunity for analyzing operations and security risks. The Savvius-ELK solution supports various types of analysis, including operational intelligence, business analytics, and predictive analytics.

Operational Intelligence

Operational intelligence refers to the insight gained through the analysis of a variety of operational data elements including metrics from adherence to SLAs, workflows, bottlenecks, and process productivity. Operational intelligence can be applied to any area of enterprise operations, from sales and customer onboarding, to support, to shipping and logistics, and to employee training and certification. All these activities involve IT systems, and all therefore generate machine data.

ELK helps organizations get an unprecedented, real-time view of their operations — enabling them to take action, to respond to opportunities and threats, and to optimize results for profits and service.

Savvius network analytics, when uploaded to ELK, bring an added dimension to operational intelligence by providing precise, fine-grained information on network utilization, application responsiveness, end-to-end latency, threat vectors, and other factors that are critical for tuning and improving operations.
Business Analytics

Business analytics is operational intelligence applied to business operations and outcomes.

ELK software complements existing business intelligence (BI) technologies and traditional web analytics tools by combining machine data with structured data to deliver real-time insights into an enterprise’s business. ELK enables organizations to monitor sales, inventory, customer activities, and other metrics in real time.

Through integration with Savvius network analytics, network activity can be correlated with these other business-centric metrics to provide data on meeting SLAs, on session and transaction metrics at a more granular level than platform reporting, on threat activity correlations, and more. Only with network analytics can application responsiveness be definitively assessed.

**ANY MACHINE DATA**

**DRAWING ON NETWORK ANALYSIS DATA FROM SAVVIUS AND OTHER TYPES OF MACHINE DATA, THE ELK STACK PROVIDES A COMPLETE VIEW FOR IT USERS, NETWORK ANALYSTS, SECURITY ANALYSTS, AND BUSINESS USERS.**
Use Cases

The Savvius-ELK solution supports the following use cases.

Security

Organizations around the world use ELK to create security intelligence platforms that leverage analytics to help detect both known and unknown advanced threats.

ELK’s strengths in the area of SIEM analysis can now leverage network events and analysis from Omnipliances, providing a strong foundation of evidence to examining and characterizing suspicious network events.

(For more information about Savvius security solutions, including the Savvius Vigil appliance for providing long-term storage of network data correlated with SIEM events, visit www.savvius.com.)

Application Performance Monitoring (APM)

Savvius Omnipeek features application awareness technology from Procera Networks, enabling engineers and others to identify the applications — including specific web applications — associated with communication streams and other network events. Using Omnipeek, network engineers can easily identify not just generic web traffic, but the web traffic associated with specific applications, such as SAP, Microsoft SharePoint, or YouTube.

This application data can now be incorporated into the ELK’s analysis of machine data for application performance monitoring. Business operations that depend on specific applications, servers, or protocols can be analyzed within the context of these IT resources.

Baselining and Monitoring

Savvius Omnipeek and Omnipliances enable network engineers to graph statistics and manually generate reports to create a baseline view of network activity. Creating baselines becomes easier with ELK as the platform aggregates statistics over long periods of time and can leverage cloud storage to amass terabytes of historical data. Users can create ELK dashboards to view custom collections of statistics and study fluctuations in these statistics over time. These dashboard views can be recreated manually or automatically generated on a pre-ordained schedule.

Centralized Alerting

In any organization where networks have become mission-critical, network degradations and outages must be fixed as quickly as possible. To fix a problem, it must first be identified and understood.

Savvius Omnipliances and Capture Engines perform real-time analysis on network traffic and automatically identify many different types of network, application, and security issues. When these issues are identified, events are generated, which are sent as syslog events to a central ELK server.

With ELK, searches on events from Omnipliances and Capture Engines can be turned into real-time alerts, which can automatically trigger notifications via email or RSS, generate tickets on a service desk, or execute containment actions. Alerts can be triggered based on a variety of thresholds, trend-based conditions, and complex searches.

By using ELK to create and manage alerts, IT organizations can centralize their alerting services and manage them in a consistent language that is already familiar to IT organizations that rely on ELK for analysis and reporting.
Conclusion

The volume of data available to enterprises can be an unmanageable blizzard of bits and bytes, or it can be collected, analyzed, and graphed to provide actionable insights, meeting the needs of internal users ranging from line-of-business managers to IT managers to security experts.

The integration of Savvius and ELK gives enterprises a powerful new solution for correlating network activity with other IT and business activity. It’s a solution that offers new data and insights to enterprises, enabling them to optimize efficiency, security, service, and the networks that their operations depend on. In a hyper connected world, the Savvius-ELK integration is a data analytics solution that makes a difference.

Learn More

To get a Savvius Omnipeek trial, please visit https://www.savvius.com/product_trials

Watch this OnDemand webinar featuring Long-Term Reporting with ELK
https://www.savvius.com/resources/ondemand_webinars/ow/long_term_reporting_with_elk

White papers and other resources about Savvius network analysis solutions are available here:
https://www.savvius.com/resources

About Savvius

Savvius offers a range of powerful software and appliance products that automate the collection of critical network data for network forensics in security investigations and for network and application performance diagnostics. Savvius products are trusted by network and security professionals at over 6,000 companies in 60 countries around the world. Visit www.savvius.com for information about Savvius Omnipliance®, Savvius Omnipeek®, Savvius Vigil™, and Savvius Insight™, and to learn about Savvius technology and channel partners.

Savvius and the Savvius logo are trademarks or registered trademarks of Savvius and/or its affiliates in the U.S. and other countries. All registered and unregistered trademarks are the sole property of their respective owners. The use of the word partner does not imply a partnership relationship between Savvius and any other company.