Savvius and Splunk: Network Insights for Operational Intelligence

WHITE PAPER

Just as networks are critical to all kinds of operations, so 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's integration with Splunk®, a leading provider of Operational Intelligence. 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.

Savvius, Inc.
1340 Treat Blvd, Suite 500
Walnut Creek, CA 94597
925.937.3200
www.savvius.com

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: Omnipliance® network recorders and analysis appliances, and 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).

The leading data analysis platform for machine data is Splunk®. Splunk Enterprise and Splunk Cloud are the company's on-premise and cloud-based solutions, respectively.

As of OmniPeek 9.0, Savvius solutions can be integrated with Splunk, 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-Splunk 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-Splunk 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, Inc. 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

Enterprises today use powerful network analysis solutions from Savvius to visualize, troubleshoot, and analyze enterprise networks. Savvius offers two product lines: Omnipliance® network recorders and analysis appliances, and OmniPeek® network analysis software.

Savvius's family of Omnipliances enables IT organizations to record and analyze traffic from 1G, 10G, and 40G networks, supporting both real-time analysis and forensic analysis of past events. Each Omnipliance is capable of capturing terabytes of traffic with no packet loss, creating a reliable record of network activity, even on today's fastest networks. Omnipliance 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."

OmniPeek network analysis software serves a dual role as both a software console for Savvius Omnipliances 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 and Omnipliances, 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. The leading data analysis platform for this activity is Splunk®.

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

Splunk Enterprise 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. Splunk Enterprise 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.

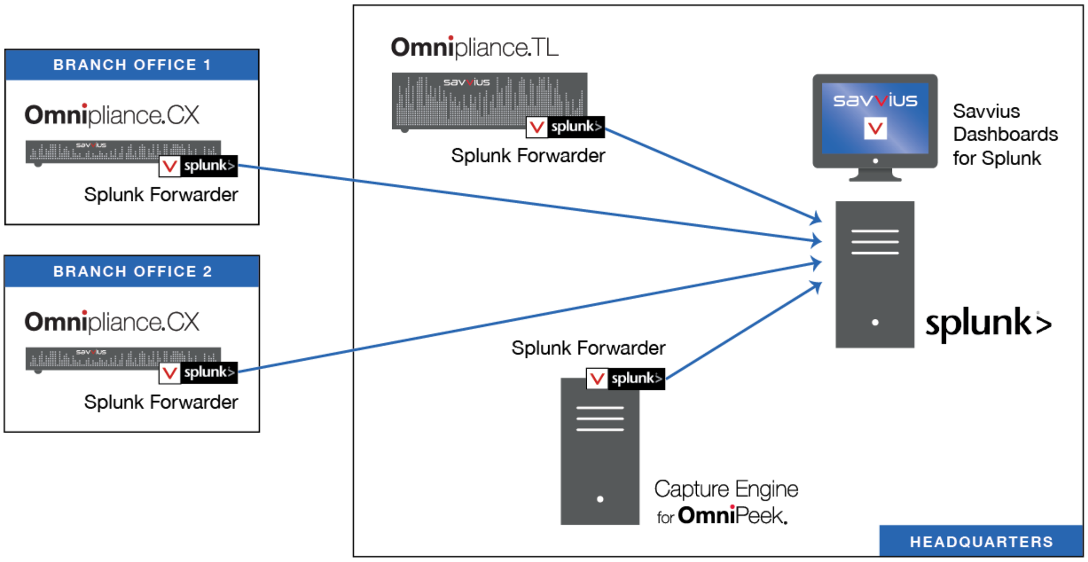
Splunk Enterprise and Splunk Cloud, the company's SaaS-based alternative, break down the data silos that have been hampering operational intelligence.

Splunk® and Savvius

Splunk's platform 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.

OmniPeek 9.0, which became available in June 2015, enables Savvius customers to integrate Savvius network analysis with Splunk Enterprise and Splunk Cloud. The result is a fast, scalable, and comprehensive data analysis platform that provides a more complete picture of IT and business activity, combining Savvius's network data and Expert analysis with other machine data collected and analyzed by Splunk.

The diagram below shows how Savvius solutions can be integrated with Splunk. Splunk Forwarders on Omnipliances and Capture Engine-enabled systems forward Savvius network analytics data to Splunk Enterprise or Splunk Cloud for analysis.



Splunk Forwarders sent Omnipliance and Capture Engine data to a central Splunk Enterprise or Splunk Cloud server, where data can be analyzed using Savvius Network Dashboards for Splunk.

A Bigger Picture: Network Analysis + Machine Data

The integration of Savvius and Splunk provides enterprises with a new opportunity for analyzing operations and security risks. The Savvius-Splunk 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 to employee training and certification. All these activities involve IT systems, and all therefore generate machine data.

Splunk 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 Splunk, 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.

Splunk 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. Splunk 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.

Predictive Analysis

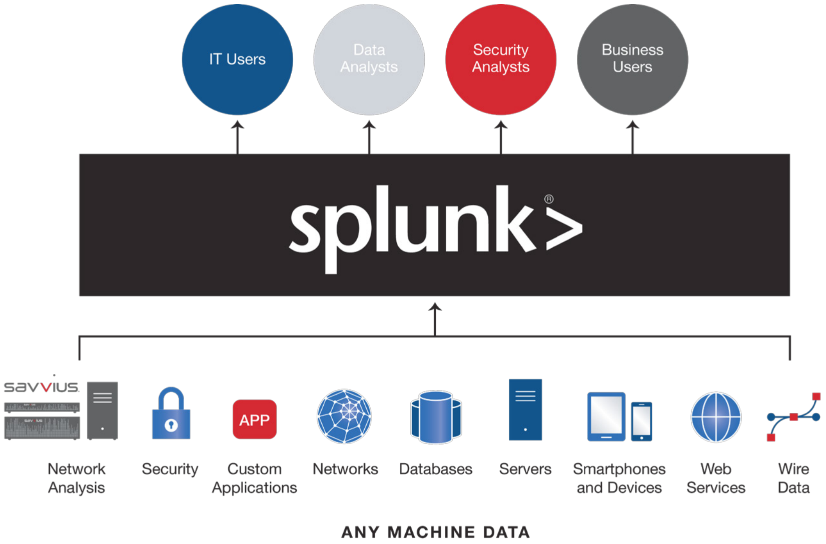
Splunk provides built-in commands and algorithms for performing various types of predictive analysis of data stored in the Splunk platform, including data collected from Omnipliances. If there are patterns and correlations to events being monitored, analysts can use them to predict future activity. Analysts can even proactively send alerts based on thresholds and perform "what-if" analyses to compare various scenarios.[1]

[1] For more information about Splunk's predictive analytics features, which include forecasting algorithms to predict future values of single and multi-valued fields, and an algorithm to remove seasonal fluctuations from trend data, see http://docs.splunk.com/Documentation/Splunk/6.2.3/Search/Aboutpredictiveanalytics.

Using the integrated Savvius-Splunk solution, enterprises can:

- Predict network performance based on historical network data.
- Predict operational performance and business metrics based on historical network data and machine data.

Predictive analysis is particularly important for capacity planning and modeling dependencies and interactions between IT resources and business activities.



Drawing on network analysis data from Savvius and other types of machine data, the Splunk platform provides a data analysis platform IT users, data analysts, security analysts, and business users.

Use Cases

The Savvius-Splunk solution supports the following use cases.

Security

Splunk as recognized as a leading vendor in the Security Information and Event Management (SIEM) market.[2] In fact, for the last two years, Splunk has been named a leader in the Gartner Magic Quadrant for Security Information and Event Management. (Gartner defines "leaders" in the Magic Quadrant as those organizations "that execute well against their current vision and are well positioned for tomorrow.") Thousands of organizations around the world use Splunk Enterprise and the Splunk App for Enterprise Security to create security intelligence platforms that leverage analytics to help detect both known and unknown advanced threats.

Splunk'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 9.0, 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 Splunk Enterprise'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

OmniPeek and Omnipliances enable engineers to graph statistics and manually generate reports to create a baseline view of network activity. Creating baselines becomes easier with Splunk as the platform aggregates statistics over long periods of time and can leverage cloud storage to amass terabytes of historical data. Users can create Splunk 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.

[2] SIEM products perform real-time analysis on security events generated by network hardware and applications. For more information, see http://en.wikipedia.org/wiki/Security_information_and_event_management

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 Splunk Enterprise or Splunk Cloud server.

With Splunk, 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 Splunk 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 Splunk 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 Splunk 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 hyperconnected world, the Savvius-Splunk integration is a data analytics solution that makes a difference.

Learn More

For information about OmniPeek trial software and Omnipliance trials, please visit www.savvius.com/product_trials. A list of Savvius Splunk add-ons is available here: www.savvius.com/splunk-apps.

Splunk trial software is available here: www.splunk.com/en_us/download.html

White papers and other resources about Savvius network analysis solutions are available here:

www.savvius.com/learn

About Savvius, Inc.

Savvius develops hardware and software solutions that drive network performance, enabling organizations of all sizes to analyze, troubleshoot, optimize, and secure their wired and wireless networks. Savvius products are sold in over 60 countries and deployed in all industrial sectors. Customers include Boeing, Chrysler, Motorola, Nationwide, and over 80 percent of the Fortune 1000. Savvius is a Cisco Solution Partner.

To learn more about Savvius solutions, please visit www.savvius.com, or contact Savvius Sales:
sales@Savvius.com or (925) 937-3200.