Monitoring and Troubleshooting Remote Offices with Savvius Insight

john@bennettstrategy.com
January 6, 2016

Extending Network Visibility and Management to the Network Edge

Enterprise networks and the engineers who manage them have never been busier. Today's networks connect more devices than ever before—everything from desktop systems to tablets to wearables to IoT sensors.[1] Applications and services are scattered across data centers and third-party cloud providers. And just about every critical business function—from traditional ERP applications to video-based training—is running on the network.

Because employees depend on devices and connectivity to get work done, IT services require high availability. Because services are everywhere—on premise, in the cloud, and at remote offices—IT engineers need centralized monitoring and insight. That's true whether the IT engineers are part of an internal team such as the network operations center (NOC) staff or are field technicians working for a Managed Service Provider (MSP).

Unfortunately, for all these stakeholders, centralized monitoring and insight can be hard to come by. Consider the case of remote offices. Most remote offices don't have an IT person on staff, and few organizations can afford to have IT troubleshooters travel to a remote office every time an employee there reports a problem. Basic monitoring tools for server uptime and bandwidth usage are available for remote offices, but these tools fail to provide the packet-level analysis that IT engineers frequently need for quickly troubleshooting difficult problems. To reduce the Mean Time to Repair (MTTR) in branch offices and other remote locations, IT engineers need the same advanced network analysis and troubleshooting features they take for granted in the NOC.

The stakes for troubleshooting are high. Network outages can be costly. Gartner estimates that the typical enterprise network outage costs $5,600 per minute or over $300,000/hour.[2] Even smaller outages can be costly. If a branch office loses

[1] Gartner estimated a 30% increase in Internet-connected things between 2014 and 2015. By 2020, 25 billion "things" will be connected to networks. http://www.gartner.com/newsroom/id/2905717
[2] http://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

connectivity or access to critical applications for an afternoon, an enterprise can lose thousands of dollars, and IT engineers may get the blame.

With enterprises continuing to rely on remote offices, partners, and—increasingly in this "gig" economy—outside consultants and agencies, IT organizations need a remote monitoring and troubleshooting solution to keep IT costs down and enterprise productivity up.

IT engineers and MSP technicians also need packet-level analytics for investigating security attacks, which are increasingly subtle and sophisticated. Possible security attacks need to be promptly investigated, even if their anomalies are occurring at an obscure location. Indeed, one of the lessons of recent, headline-grabbing data breaches is that no networked device is too tangential to be irrelevant to IT security. Critical assets can be reached from partner portals, smartphones, or special-purpose internal devices, such as deli meat scales in a retail store, not presumed to be connected to valuable targets.[3]

Requirements for Remote Office Network Management

To serve the needs of internal network administrators, MSPs, and IT consultants, a network monitoring management solution for remote offices must meet the following requirements:

- Complete packet-based network analysis, including flows, conversations, apps, protocols, and performance, enables IT engineers to understand network trends, activities, and issues in detail
- Support for packet capture for rapid troubleshooting and in-depth security investigations
- Support for network recording and forensic analysis of past events to aid in troubleshooting intermittent problems
- Trend analysis, baselining, and predictive analysis for capacity planning
- Ease of deployment in locations with limited space and no technical staff
- Economical for broad deployment

Some remote network monitoring solutions available today purport to offer packet capture capabilities, but in most cases these capabilities are rudimentary capture tools without the complete suite of packet-analysis features available in best-in-class solutions—the kind of packet capture solutions available to IT engineers managing campus networks from the NOC. IT organizations should have access to best-in-class monitoring and troubleshooting solutions, regardless of whether they are managing a network segment down the hall or a branch office three time zones away. The IT teams goal should be to deliver optimal network performance and security at every location under management.

[3] http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

Savvius Insight™: Real-time Enterprise-class Network Management for Smaller Networks

Savvius Insight™ is a compact, quad-core, six-port appliance that provides real-time and forensics network monitoring and packet capture for remote offices. About the size of a trade paperback, Savvius Insight fits easily into a wiring closet and includes pass-through ports for monitoring a location's Internet connection, and three additional ports for monitoring internal 100 megabit-class networks.

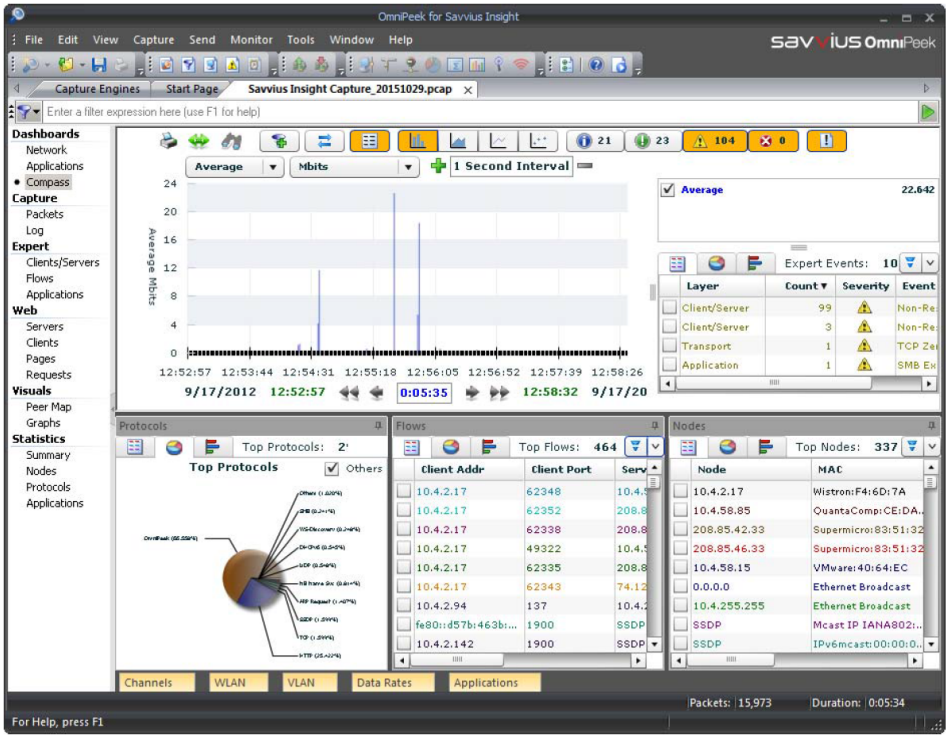
Savvius Insight (177 x 44 x 145.5 mm)

By installing Savvius Insight in every remote office, IT organizations can easily and affordably gain visibility into the network performance of all locations under management. Each Insight appliance runs Savvius Insight analytics software for capturing and analyzing local traffic. Network administrators use Savvius OmniPeek Insight network analysis software to connect to Insight appliances, monitor network activity, perform packet captures, and drill down into network activity to troubleshoot application performance issues and other network problems.

OmniPeek Insight includes high-level dashboards, along with tools for capturing packets and drilling down into traffic for troubleshooting and investing security anomalies.

OmniPeek Insight features application awareness technology that enables IT engineers to identify the applications, including Web applications, associated with communication streams and other network events. For example, engineers can use OmniPeek Insight to identify the Web traffic associated with specific applications such as SAP, Microsoft SharePoint, or YouTube. Distinguishing legitimate Web traffic from recreational Web traffic can be a critical step in resolving application performance problems and reducing security risks.

OmniPeek Insight dashboards display network utilization, alerts, Top Talkers, and other critical metrics. IT engineers can search and filter traffic to drill down for details to perform root cause analysis or other important network management tasks. IT engineers can also set triggers and alerts for specific network conditions and events. Triggering the capture of traffic for forensic analysis enables IT engineers to examine network activity after it has occurred, even if it has occurred at odd hours or intermittently over several days or weeks.



OmniPeek Insight includes enterprise-class tools for capturing packets and performing root cause analysis.

Analyzing Trends and Performing Predictive Analysis with Splunk®

Each Savvius Insight appliance also includes a Splunk Forwarder, offering IT organizations the option of using the Splunk® data analytics platform for benchmarking, monitoring, and troubleshooting remote office networks.

Splunk is a fast, scalable Big Data platform for collecting and analyzing machine data, including log data, configuration files, change events, application programming interfaces (APIs), and event streams, including event streams forwarded by Savvius Insight appliances.

Splunk offers three versions of its data analysis platform:

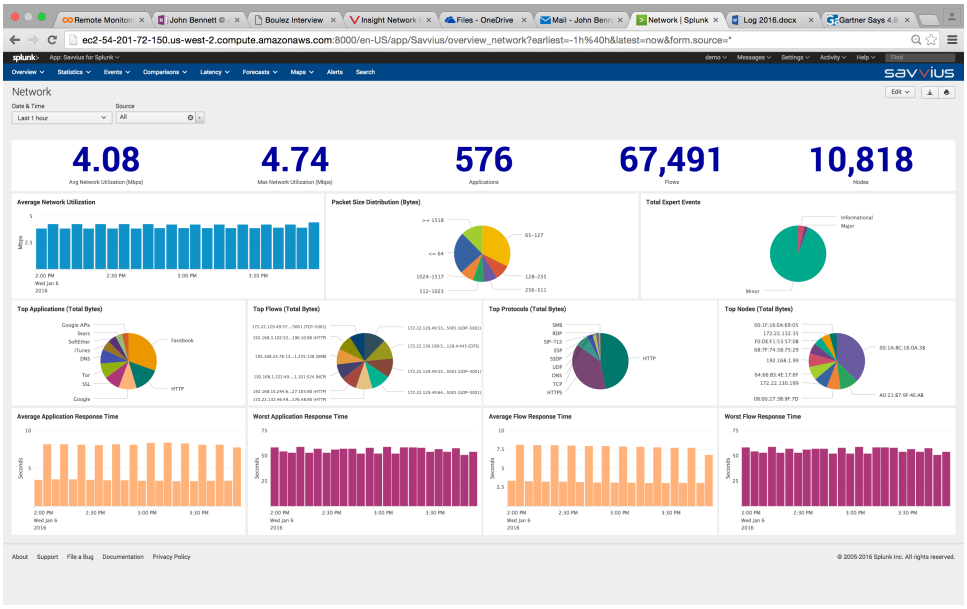
- Splunk Enterprise is the company's on-premises data analysis solution.
- Splunk Cloud is a SaaS-based alternative to Splunk Enterprise.
- Splunk Lite is a lightweight version of the platform intended for small IT teams. Splunk Lite is free for data volumes under 500 MB/day.

Featuring built-in modeling and analytics tools, Splunk provides a powerful solution for trend analysis, predictive analysis, and capacity planning.[4]

The Savvius for Splunk App is a Splunk-certified extension to the Splunk platform to optimize analysis of data from Savvius Insight appliances. The app includes high-

[4] For more information, visit www.splunk.com.

level dashboards, such as Network and Security dashboards, which report network trends and events. The app also features lower-level dashboards for reporting network activity based on nodes, flows, and protocols. All the dashboards are Web-based and available for customization.[5]



An example of a Savvius for Splunk Dashboard.

Combining Savvius analysis with Splunk analysis enables IT organizations to perform:

- **Application performance monitoring and business workflow analysis**
  OmniPeek Insight data about specific applications, including Web applications, can be incorporated into Splunk's analysis of machine data[6] (including log and event data from other business systems) for application performance monitoring. Business operations that depend on specific applications, servers, or protocols can be analyzed within the context of these IT resources.
- **Long-term trend analysis and capacity planning**
  Savvius Insight and other Savvius appliances[7] enable engineers to graph

[5] The Savvius for Splunk App is available for download on Splunkbase, the Splunk Community site, at https://splunkbase.splunk.com/app/2730/.

[6] Splunk defines machine data as "a definitive record of all the activity and behavior of your customers, users, transactions, applications, servers, networks and mobile devices. And it's more than just logs. It includes configurations, data from APIs, message queues, change events, the output of diagnostic commands, call detail records and sensor data from industrial systems and more." For more details, see http://www.splunk.com/content/splunkcom/en_us/resources/machine-data.html

[7] To learn about Savvius Omnipliance TL and other Savvius network analysis and recorder appliances for 1G and 10G+ networks, visit www.savvius.com.

statistics and manually generate reports to create a baseline view of network activity. Creating baselines becomes easier with Splunk since the platform aggregates statistics over long periods of time and can leverage cloud storage to collect many terabytes of data. Network administrators and MSP technicians can create Splunk dashboards to view custom collections of statistics and study fluctuations over time. These dashboard views can be recreated manually or automatically generated according to a predetermined schedule.

- **Security analysis**
  Gartner has named Splunk a leader in the Gartner Magic Quadrant for Security Information and Event Management (SIEM). Splunk's strengths in SIEM analysis can now be applied to analyzing network events and other data from Savvius Insight and other Savvius appliances, providing IT engineers with a strong foundation of evidence for investigating suspicious network events.
- **Centralized alerting**
  OmniPeek Insight includes support for triggers and alerts. With Splunk, searches on events from Savvius Insight and other Savvius appliances can be turned into real-time alerts and automatically trigger notifications via email or RSS, generate a ticket on a service desk or execute containment actions, coordinating Insight alerts with activities from other systems and services being managed through Splunk. By standardizing on Splunk for creating and managing alerts, IT organizations can centralize their alerting services for all sources of machine data, including Savvius Insight appliances.

Conclusion

To keep remote offices operating smoothly and securely, IT engineers need best-in-class solutions for monitoring, analyzing, and troubleshooting remote networks.

Featuring award-winning Savvius OmniPeek network analysis software and best-in-class network recording and forensics tools, Savvius Insight provides a powerful, economical network visibility and management solution for remote offices and other locations at the network edge.

Whether IT engineers need a solution for a single remote office or hundreds of remote offices, they can trust Savvius Insight to provide the network visibility and analytical insights required for keeping networks and applications performing at their best.

Learn more about Savvius Insight. Email sales@savvius.com or call +1 (925) 937-3200. Or visit us online at:

https://www.savvius.com/products/network_monitoring/savvius_insight