Solution Showcase

Savvius Spotlight: Shedding Light on Enterprise Networks

Date: October 2017 **Author:** Dan Conde, Analyst

Abstract: Savvius Spotlight provides organizations with insights into their network operations and delivers multiple advantages compared to traditional solutions:

- It allows networking professionals to avoid having to make tradeoffs between real-time and detailed network data, due to limitations stemming from when those were designed.
- It provides organizations that have modern data centers with required insights into the network using data from the past and present, and the ability to move easily from problem identification to investigation.
- It performs analytics on the actual network traffic, providing detailed, real-time visibility into the user experience.

Overview

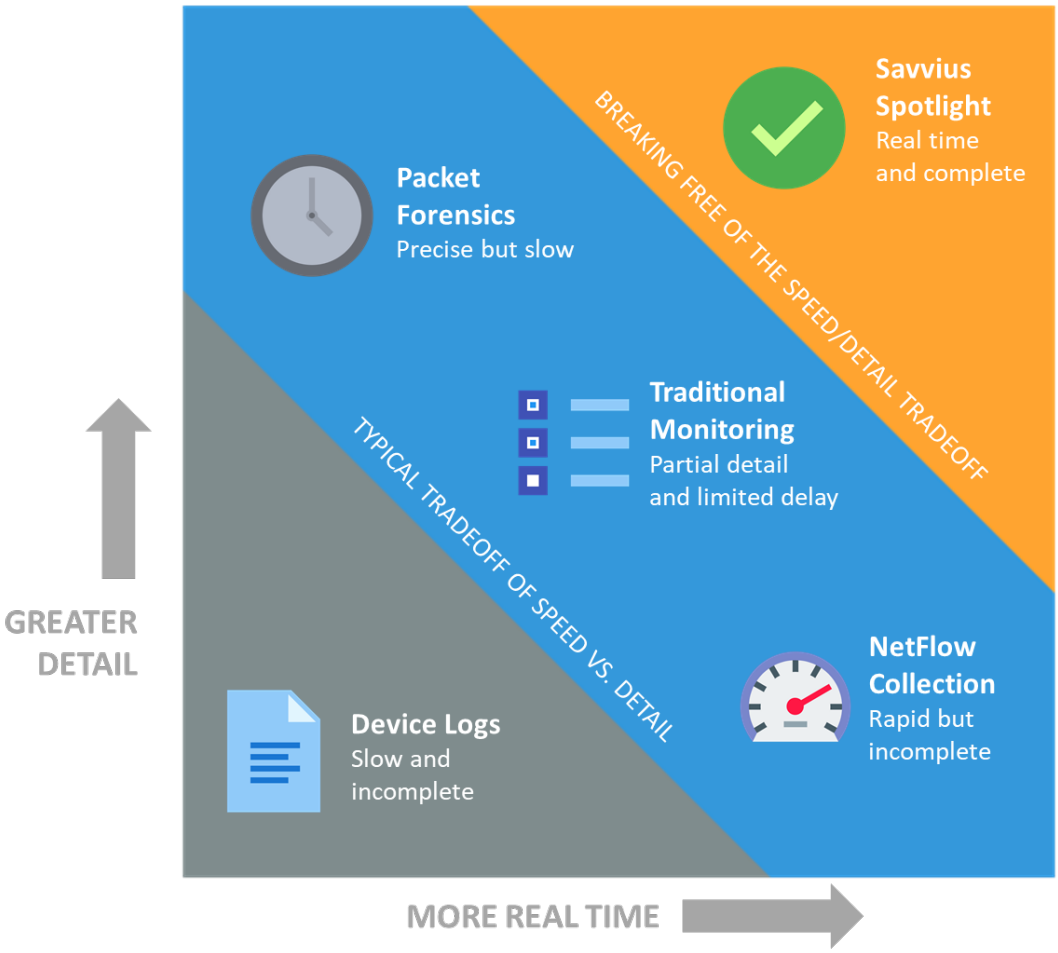
Why do IT organizations need visibility into their networks? Rather than simply being alerted to problems, organizations need to anticipate, get details about, quantify, and gain insights into resolving those problems. Visibility aids in anticipating network issues to help to avoid problems altogether where possible, and, when unavoidable problems do occur, to assist in resolving them and reducing the organization's Mean Time to Resolution (MTTR).

Solutions that have worked in the past may not be adequate for modern production networks. For example, NetFlow is a popular protocol for collecting IP network traffic information for analysis. Although it has achieved popularity due to its inclusion in Cisco network devices, its inability to measure latency or quality limits its utility, and other similar protocols rely on sampling to achieve necessary performance. Limiting performance measures or aggregating network traffic across a sampling rate or across nodes may lead to blind spots in the network. Such loss of visibility results in the reduced ability to act. To put it another way, IT organizations cannot act on what they don't know, and cannot act within an appropriate timeframe if they are not able to access information about network behavior in a timely manner.

Savvius's Approach

Savvius Spotlight has an approach that addresses these challenges and is not limited by the constraints imposed upon traditional tools (see Figure 1).

Figure 1. Tradeoffs between Detailed and Real-time Information in Network Monitoring



Source: Enterprise Strategy Group, 2017

View Current and Past Network Activity

It's important for organizations to view both current and past network activity to benefit from context. An organization may discover a problem that, by the time an investigation is underway, may have disappeared, only to reappear later. By investigating historical activities, organizations can identify problem sources before they resurrect themselves. Of course, it is critical that organizations have information about current activity to identify problems as they occur. It's not an either-or issue, and IT professionals need access to information about both past and current activity.

Gain Visibility with Both Detailed and Real-time Information

Traditionally, organizations had to choose between getting up-to-the-moment, or real-time, network visibility data and getting details. Real-time visibility tools require speed, which often meant that they were unable to gather detailed information such as an analysis of which flows have high network latency and which packets are associated with that flow. Savvius's method for gathering network data allows organizations to avoid this compromise by providing detailed information while still collecting data in real time.

Accuracy is important. Organizations cannot rely on incomplete analytics, estimations, and sampling, which may lead to guesswork or speculation.

Low-level Actionable Details Enable IT Professionals to be More Effective

It's one thing for a company to create flashy demos or provide appealing looking graphs, but the actual utility of a product is uncovered when it is placed into use. IT professionals need access to the details to properly diagnose and troubleshoot their networks. This is a critical issue that is often overlooked. It is possible to create charts and graphics that claim to represent network traffic, problems, or errors, but they generally are aggregations or summaries that don't provide sufficient information to resolve network issues without further investigation. IT professionals need investigations based on detailed, readily-available information if they are to achieve rapid problem resolution.

Detailed Data from the Past Is Important

When past data is aggregated, it loses a view of the details. In turn, organizations cannot remediate and analyze issues at the desired level. As long as storage is available, it is best if organizations can go back in time and view all the data required. The least helpful thing network administrators can hear from end-users is that "something wrong occurred" in the past. They need to understand precisely what happened. If, instead, they can only see averages, they might miss the spikes that indicate the real problems. Furthermore, if IT professionals can only access past data without details and are required to initiate a packet capture to troubleshoot in the future, then they have missed the opportunity to understand precisely the issues that caused the problem.

Product Capabilities and Workflow

A product that simply offers these capabilities does not necessarily make for a useful solution in production. Organizations need a full solution that allows the IT professional to move from identifying problem spots to immediately diving into investigation.

The ideal solution would allow IT professionals to follow these best practice steps:

1. Determine the problem at hand. Some problems, such as Voice over IP (VoIP), may not even be related to the network, such as problems related to a phone handset, but the process of elimination may require investigation of the network. A quick dashboard that shows the global state of the network will help IT professionals choose the problem to focus on.

2. Use proactive alerts to identify problems before end-users report them. Application-specific alerts, such as MOS scores for VoIP, and application latency, will help IT staff get ahead of errors before they turn into business-critical failures. IT professionals are accustomed to performing investigations after a problem is reported, but that results in a process that is reactive and interrupt-driven. By the time a problem is reported, end-user satisfaction has started to decline and, regardless of how quickly it is resolved, the memory of a problem may linger in an end-user's mind.

3. Understand the traffic patterns that are suspected of causing errors. Are particular traffic flows experiencing high latency? Are network segments experiencing high traffic? There may be no easy or set method for examining all of the indicator signals that indicate problems. A glance at many signals, or suspected culprits, is necessary to gain an understanding of the network status. Graphs are a useful way to visualize the suspected flows with high application or network latency.

4. Visualize the network, since network segments are interconnected and deployed in a hierarchical manner. It is not helpful for an IT professional to focus on a particular port or a switch. While these small items are important, service-level problems require a global view of the entire network, and it is also critical to understand the inter-relationships.

5. Use filters to narrow the focus to specific information such as affected IP addresses. Graphics are useful, but they cannot be the sole method for identifying the potential culprits. Using filters to identify specific flows enables sifting through a high volume of network visibility data.

The Bigger Truth

Can Savvius Spotlight provide a solution that meets enterprise visibility needs without compromise?

Organizations require visibility into their networks not just for the sake of the network operations team, but to drive better business outcomes. Modern data centers are built upon components that arguably derive more of their value from communicating over networks than from their monolithic, standalone capabilities. Probes can be placed at a variety of places in the infrastructure, such as in the programs running on a server or on storage systems, but they only offer a view into a particular facet of the workload, such as CPU or disk use, and may not correspond to the actual user experience.

The network, however, acts as the central nervous system for the entire infrastructure since it carries key critical communications. Therefore, it tells the truth: All communication between components must travel across the network, so analyzing that communication offers insights into the applications as well as the network. However, this analysis of network traffic data must go beyond basic access to gain deep insights.

Sampling data occasionally is like listening to a conversation in which you only hear every other word. You may miss critical and relevant information. Accessing the right amount of detail, in real time as well as historically, is the key approach to achieving complete network visibility.

What are the benefits of accurate, detailed visibility?

1. Reduced Mean Time to Resolution. Timely access to the data necessary to investigate problems when they occur leads to increased opportunities for successful remediation.

2. Proactive operations. Visibility allows organizations to move away from being reactive and to better understand the signals that affect the quality of the user experience, compliance levels, and capacity needs so that they can be addressed before problems occur.

3. Global visibility into the enterprise. Rather than focusing on a small facet of IT infrastructure, organizations are able to view the overall status of the network that ties many aspects of the enterprise together.

Savvius' approach with Spotlight provides actionable insights via a modern approach that is not encumbered by the limitations of the past, and that enables modern infrastructure management teams to be effective and efficient.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.