savvius | Manufacturing

Global Pharmaceuticals Company Chooses Savvius to Ensure Continuity of Critical Manufacturing Network

"I love working with the Savvius tools. The analysis and diagnostic features in Omnipeek give me instant insight into things like Oracle or SQL queries to see what's going on. I can quickly analyze payloads and see if network switches are overloaded or if there's a speed duplex mismatch. Savvius gives me the fast access to network data I need to quickly understand and fix a multitude of network problems."

CHIEF CONSULTANT
GLOBAL PHARMACEUTICALS COMPANY

In the manufacturing sector, the last thing an organization needs is an unexpected disruption. For companies in the competitive pharmaceuticals industry, sudden equipment failures or other unscheduled events can quickly lead to delays and millions of dollars in lost revenue. With sales in excess of $20 billion each year, this U.S.-based pharmaceuticals and animal health products manufacturer today operates 35 sites throughout the U.S. and Europe, reliably providing a range of much-needed products to consumers and agricultural clients around the world.

The Challenge

Several years ago the company's Automation IT Security & Architecture team embarked on an ambitious plan to bring its manufacturing network into compliance with ANSI/ISA-95 standards, which included setting up firewalls inside the network. The primary goals of this nine-person group are to maintain the integrity and availability of the network to minimize unplanned downtime in manufacturing, and to quickly assess exposure risk.

"Our main problem in the past was that we operated with a flat network," said the Automation IT Security and Architecture team's chief consultant.

> "We have achieved our goals — and continue to achieve them — thanks to Omnipeek and Capture Engine for Omnipeek. It took three years to implement the ANSI/ISA-95 architecture across all of our sites, but only because we approached the process cautiously and methodically. We got here without any major disruptions or calamities, so I'd call that a phenomenal success."

CHIEF CONSULTANT
GLOBAL PHARMACEUTICALS COMPANY

"We could simply organize routers and switches into their proper architecture, but without a firewall in place, we wouldn't succeed in increasing security at all. So we had to learn how to deploy firewalls in the middle of our network with zero disruption. Back then, any significant changes to the network required manufacturing operations to stop, so the fewer disruptions, the better."

In order to assess the network and move toward ANSI/ISA-95 compliance, the Automation IT Security and Architecture team looked for software tools that would allow them to analyze large amounts of network data over long periods of time, providing long-term visibility into all of the network's thousands of connections.

The Solution

The company evaluated some of the leading hardware and software products from several vendors, and decided to deploy two software solutions from Savvius™: Savvius Omnipeek® and Capture Engine™ for Omnipeek. These solutions gave the company the cost-effective software platform they required, without the expense associated with introducing additional hardware into the network.

Phase One

"At first, we wanted to gather the sort of network diagnostics that we simply couldn't get from switches, routers, or firewalls," continued the chief consultant. "We considered using other tools but found that they required way too much manual intervention and couldn't automatically create the files that we needed. Capture Engine for Omnipeek gives us much more visibility and control. Once it was in place, we spent two years constantly collecting all of the flow data coming out of our 35 sites, and analyzing it with Omnipeek to help us develop strict rules for the firewalls."

Each of the company's manufacturing sites uses a pair of Cisco ASA firewalls. Sitting next to those firewalls is another PC running Capture Engine for Omnipeek. Flow data is automatically pulled for analysis every four hours from a centralized server, and used with data derived from a separate firewall simulator to diagnose network health and compliance.

"During phase one of this project, we could deploy the firewalls in passive mode, and get all the data back from the Capture Engine," stated the chief consultant. "We would then shift assets around in order to comply with our rules. For example, if there was a site in France with a server in the wrong location on the network, we'd respond with an action plan. That might involve changing the IP address, moving the server around, retiring it, replacing it, or doing something to bring it back into compliance. There's no room for flexible rules in the data center, so if you're not within that 'trusted zone' then you won't get an exemption."

Capture Engine for Savvius Omnipeek

Capture Engine for Savvius Omnipeek is a software probe built on Savvius' award-winning network analytics capabilities. Capture Engine performs real-time packet analysis on traffic captured from one or more network interfaces. It captures and analyzes network traffic in real time and records that traffic on a dedicated Windows machine or on Savvius Omnipliances for post-capture analysis. With Capture Engine, network engineers can monitor distributed networks remotely and quickly identify and remedy performance bottlenecks without leaving the office.

Savvius Omnipeek Remote Assistant

Savvius Omnipeek Remote Assistant is a small and secure program for distributed client devices. The program is extremely simple and can be operated by anyone without a network analysis background. The remote user simply double-clicks on an executable file, clicks start, then stop. The resulting encrypted files are emailed back to the network engineer for secure analysis.

Omnipeek Remote Assistant allows network engineers to:

- Quickly discover root cause of problems and reduce MTTR
- Gain access to network data anywhere, without sending staff to remote locations
- Perform single use or ongoing network analysis
- Address all types of network traffic: wired, 802.11 wireless, voice and video over IP, etc.
- Ensure full data security and privacy

Phase two

Once this first phase was complete and firewalls were deployed at every manufacturing site, the Automation IT Security and Architecture group shifted its focus to maintaining the integrity of the network. Having only a small, centrally-located team, Savvius Omnipeek's built-in Omnipeek Remote Assistant was the perfect tool to capture packets at remote sites for analysis by the team at headquarters.

"To find out what's happening on a network at a remote location, we no longer need to send an engineer onsite," continued the chief consultant. "We simply forward an executable version of Omnipeek Remote Assistant to a local staff member, who can install it on a computer to capture data for us. The resulting file is encrypted and sent back to us for analysis with Omnipeek, giving us the flexibility to securely troubleshoot common application issues like LDAP and Kerberos regardless of location."

The Benefits

Having used Capture Engine for Omnipeek together with Savvius Omnipeek and its Omnipeek Remote Assistant for several years, this pharmaceutical company has successfully achieved an ANSI/ISA 95-compliant architecture for its entire manufacturing network. This architecture enables the team to improve security while making it possible to activate a firewall at a running facility without any adverse impact to manufacturing.

Next on the team's list of goals is to use the Savvius tools to reduce the manufacturing network's exposure. At present, the firewalls trust approximately 6,000 servers, located in three primary data centers around the world. Using Capture Engine for Omnipeek, the team not only sees which servers may be misconfigured, but also unutilized servers that can be safely removed from the "trusted zone." This ongoing program is expected to reduce the number of trusted servers by more than half, further reducing the exposure risk of manufacturing assets.