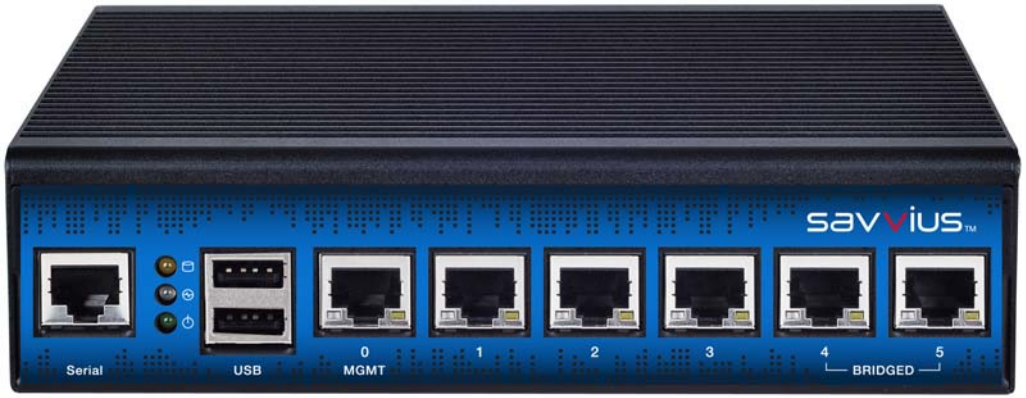
Savvius Insight FAQ

What is Savvius Insight?



Savvius Insight is a compact, quad-core, six-port mini appliance about the size of a trade paperback (177 x 44 x 146 mm). It has two 1-gigabit bridge ports (Ethernet connections, not performance; performance is in the 100 megabit-per-second range) for monitoring inline to an Internet connection, an Ethernet management port, and three additional ports for monitoring internal networks. Each Savvius Insight appliance contains Splunk Forwarder software that transmits network performance and security data to the user's Splunk Server for analysis.

Why Savvius Insight?

Networks are important to businesses of all sizes and locations from the datacenter to the network edge. Savvius network analytics, as found in Savvius's Omnipliance products, help network administrators keep high-speed networks running quickly and reliability. Savvius Insight was created to bring enterprise-class network performance management within reach of anyone responsible for the performance and security of smaller networks. This hasn't even been possible until recently.

What software is inside Savvius Insight?

Although we are just calling it Savvius Insight software, 'under the hood' Savvius Insight contains the Savvius Capture Engine version 9.0 running on Ubuntu Linux, version 12.04. This is effectively the same engine software as Omnipliances use, though it is locked to the hardware. Trying to run this engine on different hardware will not work.

What other specs?

Intel Atom C2358 ("Rangely") 1.7 Ghz processor, 128 GB SSD, 8 GB RAM, two USB 2.0 ports, and a serial port (with RJ45 physical connection). Savvius Insight uses an external power adapter and does not require a fan; without moving parts, it is perfectly suited to be connected to a small office network and hidden in a closet.

Is there a reset button?

Yes. Holding the reset button for more than three seconds causes the Savvius Insight box to go back to factory defaults.

Does Savvius Insight come with OmniPeek?

Yes, it comes with OmniPeek Insight, which has effectively the same features as OmniPeek Connect, but requires connection to a Savvius Insight appliance to function.

Where do I get the OmniPeek Insight software?

You can download the software here:

https://insight.savvius.com

Does OmniPeek Insight require activation?

No. It is designed to be used by anyone with a Savvius Insight appliance. You must register for access to future versions of OmniPeek Insight and the Savvius Insight software.

https://insight.savvius.com/omnipeek_insight.php

Does Savvius Insight support wireless capture?

Savvius Insight does not support WiFi networks. We are considering wireless capture support for a future version.

Does Savvius Insight support VoIP analysis?

Savvius Insight does not support VoIP statistics in version 1. VoIP support is under consideration for a future version.

Can Savvius Insight perform long-term Capture-to-Disk like your Enterprise-Class Omnipliance products?

Savvius Insight uses an SSD with a duty cycle that is not rated for continuous capture, though it is well-suited to occasional captures as needed.

How is Savvius Insight installed physically?

The most common way will be to remove one side of the Ethernet cable between modem and router and plug it into one of Insight's bridge ports, then complete the connection with a second Ethernet cable. A third Ethernet cable connects to the router for management functions. It is also possible to connect Savvius Insight with a single cable to a port on a router configured as a SPAN port or inline on any subnet. Multiple connections are supported.

How do the bridge ports work?

Any traffic that gets to one is copied to the other, plus a copy is sent to the analytics engine. If the power goes out, the two bridge ports are connected as if they are a wire ("fail to wire"), so Internet connectivity is not lost. On startup, the bridge ports are in "wire" (non-monitoring) mode until Insight completes the startup process.

What if I connect an Ethernet cable to just one of the two bridged ports?

No problem. Analytics on that traffic will be created. Do not connect a different network to each bridge port. That will create problems for your network.

What about the rest of the installation process?

Savvius Insight comes with a web-based setup utility. With it, you can name the Savvius Insight appliance, put in a password, set up the network connection, and, optionally, put in the address of a Splunk server (covered in more detail below). You can also set the time zone and establish which NTP (Network Time Protocol) server you wish to use.

How do I connect to Savvius Insight?

Every Savvius Insight comes preconfigured with a static IP address. You can run any browser on a PC or Mac on the same subnet and access Savvius Insight. Alternately, you can connect a monitor to the COM port and a USB keyboard to configure it in that manner using Putty or other standard terminal emulation program.

What if I'm running traffic into multiple ports?

Savvius Insight can perform four captures (the max number it is capable of) above 40 Mbit for each one, so a total of 160 Mbits.

Using fewer ports or reducing the amount of analysis speeds up each one, but the overall total goes down.

What about pure bridge mode with analytics turned off? (so I can use it later for CTD or monitoring)

We haven't fully tested this, but we know that it is way over 100 Mbits.

What is the Savvius Insight Support plan?

Support for Savvius Insight is available only at the Savvius Insight Self-Support Web Portal located at: *https://insight.savvius.com* Here you will be able to:

- Register your Savvius Insight
- View the Frequently Asked Questions
- Obtain configuration instructions for common use cases
- Share your Savvius Insight experiences and issues with other users in an interactive forum
- Learn new Tips and Tricks about Savvius Insight hardware and software

What happens in the unlikely event that my Savvius Insight appears to have a hardware failure within the 1-year warranty period?

An RMA (Return Material Authorization) number must be obtained from Savvius in order to return hardware for any reason. Your Savvius Insight must be registered to obtain warranty service or software updates. You can request hardware warranty service here:

https://insight.savvius.com/warranty.php

SPLUNK

How does Splunk on Savvius Insight work?

First, you should probably know something about Splunk, and if you don't, one way to learn is by going to the Splunk website and searching for "Education Videos". At the highest level, Splunk accepts machine data (not human created, so not Word docs or database info); logs, metadata etc., and indexes it, making it searchable and putting it into dashboards. Savvius analytics are exported as csv files that the Splunk Forwarder can send to any Splunk Server. The default interval is 10 minutes, which can be increased or decreased to fit your specific reporting needs. We have created dashboards available at SplunkBase.com so that you can view the processed data from the Splunk Enterprise server in a web browser. The data generated by Insight can also be used in other dashboards, and correlated with other data in Splunk.

I've never used Splunk before. What do I do?

It is surprisingly easy. One way is to install Splunk Enterprise on any Linux or Windows PC, even an older one. If you are indexing less than 500 MB per day, there is a free version of Splunk Enterprise. (Splunk Light is not the right choice; it doesn't support our dashboards.) The Splunk Enterprise Free license has other limitations as well, like not having alerts. To index more data and avoid limitations, Splunk licenses starting at 1 gig per day can be purchased. Customers are known to have licenses that support hundreds of gigs per day. You could also go to Splunk Cloud, but it isn't free after the trial period. In any case, follow the instructions to install Splunk Server and the Savvius for Splunk dashboards, then use the Savvius Insight web interface to point Savvius Insight at the Splunk Server and you will get long term reporting, trending, correlation, baselining, etc.

Do I need OmniPeek Insight to use Splunk?

No, when a Splunk Server IP address is provided, Savvius Insight will be configured to automatically start two captures on the bridged ports. (Using two captures increases performance.) The names of the captures both contain “Splunk”, and are configured with Statistics Output and Reset Statistics enabled. Because the statistics are reset at each statistics output interval, the Splunk capture is not useful for other types of troubleshooting. OmniPeek Insight can be used to make changes to the Splunk captures, and create and use other captures simultaneously. Please note that additional captures affect performance.

Does Savvius Insight support multiple Splunk servers?

The Splunk Forwarder software supports multiple Splunk servers, but it does require going into the Savvius Insight box rather than doing it through the Savvius Insight web interface. Adding that capability to future versions of Insight is on the list. There will be a blog post on how to do it.

Can multiple Savvius Insights be directed to one Splunk server?

Of course. Without modification, and depending on your network traffic, two Savvius Insights can be pointed to one instance of the free version of Splunk Enterprise server, which can index up to 500 MB a day. Pushing data from more Savvius Insights to the free version of Splunk Enterprise would work, but may require increasing the reporting interval to something longer than 10 minutes. Exceeding 500 MB a day will require purchasing a license or subscription from Splunk. Splunk provides many options at various data levels.

That's the low side. What about the high end?

Splunk servers and the Splunk Cloud can index terabytes of data every day, which means there is no practical limit to how many Savvius Insights can send data into a Splunk server running on appropriate hardware or in the cloud.

How much does Splunk cost?

Above the free version of Splunk Enterprise, there are a number of options. The best way to learn about them is go to Splunk.com and look at products. A few data points: A Splunk Enterprise server licensed for 1 GB/day is $150 per month or $4500 for a perpetual license. That translates to a few tens of dollars per month per Savvius Insight. Splunk Cloud indexing 20 GB/day is $2000 per month, a powerful and versatile alternative supporting 50 or more Savvius Insights.

Would Savvius consider making Splunk available to Insight customers as a service?

Not in version 1. We have looked at creating a service offering, but it didn't make sense at this point. We will continue to explore this possibility in the future.