# savvius Vigil™

## Network Forensics Appliance for Incident Response

### Highlights

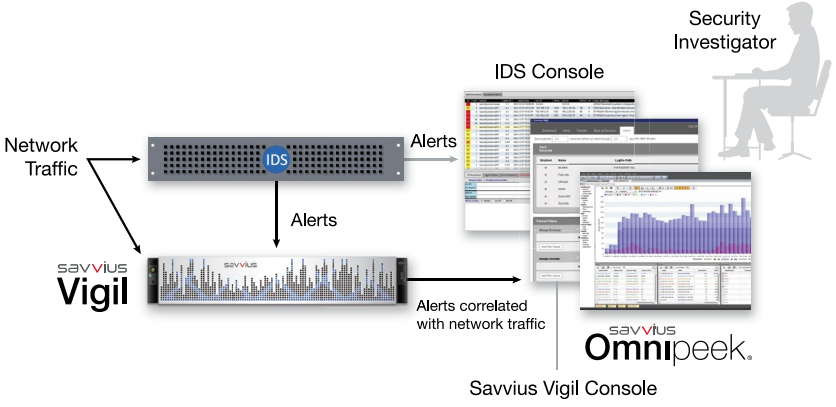
- Investigate security incidents either as they happen, or months later
- Intelligent capture of network traffic based on IDS/IPS alerts dramatically reduces required storage
- Capture all network data from sensitive assets or suspicious protocols, all the time, to provide insight into attacks that IDS/IPS solutions miss
- Retains the critical pre-alert packets that show how a breach occurred
- Initiate full packet capture with the push of a button
- Integrates with existing IDS/IPS solutions
- Instantly investigate packets related to suspicious activity
- Stores relevant network packets for months
- PCAP output for use in your current investigation workflow or with Omnipeek Connect (license included)

### Problem

Network packets are critical to security investigations, since packets are the vehicles for the attack. Yet the typical delays between breach and discovery mean most security investigations must proceed without access to network packets. Before Savvius Vigil, only expensive investments in data storage could provide the long-term access to network packets an investigation needs.

### Solution

Savvius Vigil automates the collection of network traffic needed for security investigations, both reducing the likelihood of a breach, and minimizing the impact should one occur. Even breaches not discovered for months can be effectively investigated using Savvius Vigil. Savvius Vigil lets your organization conduct powerful forensic investigations by extending breach visibility and integrating with key security systems. You can intelligently capture critical packet data before and after an attack occurs so your organization can gain a clear and accurate picture of the damage, and react quickly.



## Specs

2U appliance with
1G and 10G interfaces

96TB of storage

## Integration

Savvius Vigil integrates with major IDS/IPS solutions, including:

- Cisco
- Sophos Cyberoam
- Gigamon
- HP Enterprise
- IBM
- IXIA
- Lancope
- Palo Alto Networks
- Snort
- Suricata

## How it works

Savvius Vigil integrates with your existing SIEM/IDS/IPS capabilities to intelligently determine what network traffic is relevant for breach investigations. Savvius Vigil continuously collects all network packets and only stores traffic associated with security alerts, discarding unassociated packets. The device also supports feeds from multiple sources simultaneously. Savvius Vigil captures the critical packets that led up to the alert being triggered, from up to 5 minutes before the alert, showing the original cause of a potential breach. You can also configure Savvius Vigil to store all packets based on specified IPs, ports or protocols, all the time, to provide insight into attacks that IDS/IPS solutions miss. And if you suspect an attack is ongoing, you can initiate a full packet capture with a single click, including up to 5 minutes of packet history.

## About Savvius

Savvius offers a range of powerful software and appliance products that automate the collection of critical network data for network forensics in security investigations and for network and application performance diagnostics. Savvius products are trusted by network and security professionals at over 6,000 companies in 60 countries around the world. Visit www.savvius.com for information about Savvius Omnipliance®, Savvius Omnipeek®, Savvius Vigil™, and Savvius Insight™, and to learn about Savvius technology and channel partners.

## Learn more about Savvius Vigil

Email sales@savvius.com or call +1 (925) 937-3200.
Or visit us online at: https://www.savvius.com/products/network_forensics_for_security_investigations/savvius_vigil