savvius™

VIGIL

Long-term packet storage for security forensics

Problem

Network packets are critical to security investigations. After all, packets are the vehicle 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 excessive investment in data storage could provide long-term access to network packets.

Solution

Savvius Vigil intelligently and automatically determines which packets might be useful in a security investigation and stores them for the weeks or months required for them to become useful. An intuitive interface provides rapid access to stored packet and event data, both directly and through sophisticated analytics.

How it works

Savvius Vigil integrates with your existing SIEM's IDS/IPS capabilities to trigger storage of network packets. Savvius Vigil integrates events from multiple sources, including network conversations with specified IP addresses. Traffic between relevant nodes is captured before and after the triggered events. Optionally, all related traffic to and from an event's IP addresses is captured as well.

Hardware

- 64TB HDD
- Optional 64TB Extended Storage
- 4 Port 1/10G Network Adapter

Software

- Savvius Vigil software for monitoring and forensics supports multiple appliances
- Monitoring dashboard with overview, storage use, and event management
- Security Forensics capability, including hierarchical search by date, event, IP address, severity, etc.

".....by automatically storing the appropriate network packets, Savvius Vigil enhances the ability of security analysts to quickly understand and respond to newly discovered threats. It allows us to go from notification of breach to completed analysis much faster."

Keatron Evans,
Principal,
Blink Digital Security

About Savvius

Savvius, Inc., a leader in packet-level network analytics and security forensics, enables network and security professionals to identify, understand, and respond to challenges in network performance and security. Savvius, formerly WildPackets, has sold products in more than 60 countries and all industrial sectors. Customers include Apple, Boeing, Cisco, Deutsche Telecom, Fidelity, Microsoft, Nationwide, and a high percentage of the Fortune 1000. Savvius is a Cisco Solution Partner. For more information, visit www.savvius.com.

More Info

Savvius offers a full line of network performance management and security forensic solutions.
For more information, visit www.savvius.com or email us at sales@savvius.com.