

# Savvius works with security partners to enable network forensics in breach investigations

Savvius Vigil captures relevant network traffic minutes before and months after an alert for effective investigations.



**Cisco** is the worldwide leader in networking that transforms how people connect, communicate, and collaborate. The Savvius and Cisco joint solution makes long-term network-level data available for investigating security alerts triggered by Cisco FirePower, enabling network forensics in breach investigations. The joint solution gives visibility into network activities for alerts from months in the past, including the network traffic just before an alert was triggered.



**Cyberoam** (a Sophos Company) secures organizations with its wide range of product offerings at the network gateway. Cyberoam leverages the power of multi-core processors, offering enterprise-grade performance in its appliances. Cyberoam and Savvius have partnered to enable network forensics in breach investigations. The joint solution provides long-term network-level data to investigate security alerts generated by Cyberoam.



**Gigamon** provides active visibility into physical and virtual network traffic, enabling stronger security and superior performance. Savvius and Gigamon have partnered to bring full visibility, performance, scalability, and decryption to our enterprise customers with high-speed networks. The joint solution provides accurate time-stamping, SSL decryption, de-duplication, filtering, and load-balancing across multiple Savvius Vigil appliances.



**Hewlett Packard Enterprise** delivers high-quality, high-value products, consulting, and support services in a single package. HP has industry-leading positions in servers, storage, wired and wireless networking, converged systems, software, services, and the cloud. The Savvius and HP joint solution lets security professionals add packet intelligence into their investigation of security alerts triggered by HP ArcSight SIEM, even if the alerts happened months in the past.



**IBM** offers a deep enterprise security portfolio. Unmatched in its ability to help you disrupt new threats, deploy security innovations, and reduce the cost and complexity of IT security, IBM can safeguard your most critical data from compromise. The Savvius and IBM joint solution helps security professionals gain access to network-level data required to investigate security alerts triggered by Qradar SIEM, enabling network forensics in breach investigations. The joint solution gives visibility into network activities for alerts from months ago, including the network traffic before an alert even triggered.



**Intel Security** delivers proactive and proven security solutions and services that help protect systems, networks, customers, and business of all sizes around the world from the latest malware and emerging online threats. Savvius and Intel Security have partnered to enable network forensics in breach investigations for both immediate and delayed investigations. The joint solution adds packet intelligence to Intel McAfee ESM alerts from months earlier, and gives visibility into network activities even before an alert triggered.



**Ixia** provides application performance and security resilience solutions to validate, secure, and optimize businesses' physical and virtual networks. Savvius and Ixia have teamed up to provide accurate timestamps and load balancing across multiple Savvius Omnipliances for enterprise customers who have high speed data centers. This enables integrated and scalable network security and performance monitoring.



**Lancope, Inc.** (a Cisco company) is a leading provider of network visibility and security intelligence to protect enterprises against today's top threats. Savvius partners with Lancope to make network-level data available for investigating behavior anomalies that Lancope's StealthWatch identifies. This permits investigating an anomaly from months earlier, and even gives a view of network behavior in the minutes before the anomaly occurred.



**Napatech** provides smart data delivery to applications to ensure the quality and security of the network services we all rely on. Savvius Vigil includes Napatech high-performance network capture adapters to provide the high-speed capture and advanced hardware capabilities, such as time-stamping, slicing, and filtering, required to support today's fast networks.



**Procera Networks** engineers software that identifies applications in data traffic to drive insights, provide intelligence, and enable action in real time. Embedded in Savvius products, Procera's products bring into our joint solution the layer-7 application awareness and classification critical for managing and troubleshooting application performance.

---

Savvius and the Savvius logo are trademarks or registered trademarks of Savvius and/or its affiliates in the U.S. and other countries. All registered and unregistered trademarks are the sole property of their respective owners. The use of the word partner does not imply a partnership relationship between Savvius and any other company.