

# Log Retention & Compliance Reporting

## Safeguard the Infrastructure with LogVault2 Plus

### Sorting Through the Traffic

The marketplace is flooded with a variety of security products, such as network firewalls, IPS/IDS, VPNs, routers and switches. A typical enterprise deploys on average more than 75 different security products, each one—along with business-critical systems, noncritical servers, and endpoints—generating extensive logs daily. These raw logs need to be collected, archived and indexed in a readily searchable manner to comply with regulations and provide an audit trail in case of a security breach.

Keeping up with such volume is not easy. It requires dedicated infrastructure to collect and archive the many different formats of logs and alerts generated by your enterprise. Log compliance scopes are expanding every year, retention periods are growing, and individual sources are becoming more verbose as vendors add features and software. As a business grows and the volume of critical log data increases, many organizations struggle to meet the resource and store requirements necessary to maintain an efficient log management system.

### How Secureworks Helps

The Secureworks LogVault2 Plus provides clients with a scalable approach to log management, one that expands to meet clients' needs as their business expands. Our solution collects, archives and indexes logs generated by virtually any security technology and critical information asset on a 24x7 basis. LogVault2 Plus helps organizations satisfy security posture and regulatory compliance requirements for log collection, storage and reporting, without the management overhead and capital expense required for traditional log management products.

LogVault2 Plus gives support for an expandable range of sources, allowing for capture and aggregation of log traffic generated by a client's information assets. Clients are empowered with the technology, expertise and scale needed to deploy an effective log management system that meets regulatory compliance and security objectives.

### Client Benefits

- Scalable log management solution that grows with client needs
- Regulatory compliance reporting
- Integration with most security devices and critical information assets

---

### Solution Features

- Satisfies log retention requirements for NERC CIP, PCI, FFIEC, SOX, HIPAA and other regulations
- Expandable retention capabilities
- Prebuilt regulatory compliance reports
- Forensically sound log compression and cryptographic hashing

The solution enables quick access to reports needed to demonstrate compliance and measure effectiveness of log management, while maintaining the flexibility to expand capability as volume increases.

## **An Expandable, Efficient Solution**

LogVault2 Plus provides a flexible way to pull together the vast amounts of log data in a client's environment. Our log retention technology is deployed in your infrastructure and collects log data from the various products in your enterprise. Our LogVault2 Plus host base provides 4 TB of storage and can accommodate an additional 32 TB of storage. Clients can add more processing power and additional storage as retention needs change.

## **Why it Matters**

The Secureworks Log Retention & Compliance solution helps your security program:

- Deploy a scalable solution that not only meets your needs today, but can expand and grow as log retention requirements increase
- Satisfy regulatory requirements with fewer resources, removing the burden of recruiting, hiring and retaining log management personnel
- Collect logs from disparate network assets and data sources, providing a solution that can accept logs from virtually all aspects of a client's infrastructure
- Improve incident response with forensically sound log data, resulting in more efficient retrieval and investigation in the event of an incident
- Troubleshoot your security and network with readily available logs, accelerating your ability to determine what happened and your next steps
- Eliminate management overhead with a fully managed solution

### **About Secureworks**

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that keeps organizations safe in a digitally connected world. We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™



For more information, call **1-877-838-7947** to speak to a Secureworks security specialist. [secureworks.com](https://secureworks.com)