SilverSky

SilverSky Log Management

Effective log management is time-consuming, resource-intensive, and expensive

For many, log management is no longer just an industry best practice, it's an organizational requirement. In the past, a network administrator or security analyst could handle this requirement by collecting log data from a few select systems in the event that the data might be needed later. That is no longer an option today, as the number, variety, and volume of log data and network infrastructures have created a massive challenge. The expansion of IT infrastructure into hosted and cloud deployments means that there is not only more data to manage, but that it resides in a variety of environments. Effective log management requires comprehensive functionality that extends beyond data collection to encompass normalization, analysis, reporting, and disaster-proof archival.

For those in highly regulated industries, PCI, HIPAA, SOX, and GLBA mandate that log data must be collected, regularly reviewed and archived. In addition, regular analysis and forensics should be performed on the same log data to enhance overall security and availability.

SilverSky's Log Management solution helps organizations reduce the costs and complexity of log management and reduce the compliance burden. Our cloud-based software automates log collection, aggregation, normalization and parsing of your data. We offer flexible data collection options, which include physical appliances or remote collectors with agent-based or agentless methodology. Our web portal provides a unified view into all of your data, with tools to rapidly uncover the insight you need to remain secure and compliant. Log data often contains sensitive data (such as customer data), and breach of log data is a serious problem. SilverSky encrypts your log data both in transit to the log collection solution and when stored at rest. We also provide various archival options to meet all of your compliance needs.

SilverSky MDR Solution

PCI DSS Requirement 10

PCI DSS Requirement 10 is explicit about the requirements for auditing and logging. It states that logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

HIPAA Section 164

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) outlines relevant security standards for health information. Several HIPAA requirements are applicable to logging, log review and security monitoring. Subsections of Section 164 calls for monitoring the systems relating to patient information for login and access which also applies to "login attempts," including both failed and successful logins. Section 164 also requires Audit Controls, which covers audit logging and other audit trails on systems that deal with sensitive health information.

SilverSky's Log Management

- Real-time 24x7x365 monitoring of virtually all log types
- Detailed event escalation process
- Event correlation and forensics
- Comprehensive reporting for compliance
- PCI compliant service satisfying Requirement 10
- One year log retention and archival
- Trouble ticket integration via email
- Available as a physical or virtual appliance

Management

Provides log collection from the customer environment, which is then encrypted, compressed and sent to our cloud for processing and storage. Through our portal you have full access to reporting and can install the software onto other devices and configure your settings. Our extensive team of certified security experts provides 24x7 device management via our AICPA SOC 2 Type 2 Security Operations Centers (SOCs).

Monitoring

Using our proprietary SSA device this SaaS service provides clients with on demand log collection, storage, reporting, correlation, and monitoring services across their entire environment. Our extensive team of certified security experts provides the 24x7 monitoring, alerting and reporting via our AICPA SOC 2 Type 2 SOCs. Moreover, SilverSky is the only major cloud messaging provider examined by the FFIEC.

Retention

Using Log Retention service allows you to offload the management and maintenance burden while retaining full access to your appliances. The service helps you satisfy security and compliance requirements for log collection, storage and reporting. Our cloud-powered service captures and aggregates millions of logs generated every day from your data sources with full reporting available via our portal.

Trusted Cybersecurity for an Uncertain World

SilverSky offers a comprehensive suite of technology and services that brings simplicity to your compliance and cybersecurity program.

SilverSky has been serving regulated industries for decades so we understand your business and regulatory challenges.

By tirelessly safeguarding your most important data, SilverSky enables growth-minded organizations to pursue their business ambitions without security worry.

SilverSky

www.silversky.com

Contact Details: US: 1-800-234-2175 | E: learn@silversky.com
SilverSky, 4813 Emperor Boulevard, Suite 200
Durham, North Carolina 27703
linkedin.com/company/silversky | twitter.com/SilverSky