securonix

DATASHEET

NXLog Management

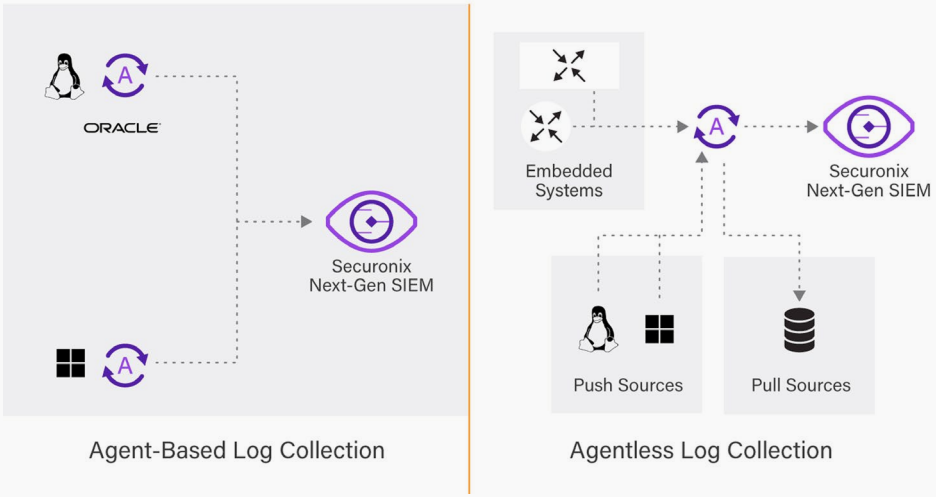
Ultimate Log Collection and Centralized Log Management

Better Threat Detection & Response With Centralized Log Collection

Organizations invest in SIEM solutions to improve security operations, manage risk, speed incident response, and provide digital forensics. However, if the SIEM is not providing proper correlation and analytics caused by insufficient log collection, the organization cannot capitalize on their SIEM investment.

Securonix with NXLog provides a highly flexible and reliable log collecting and distribution solution. NXLog is a scalable logging system that makes sure logs are collected in an efficient, secure, and reliable way. NXLog structures, formats, and filters the data. The solution supports most operating systems and can handle data sources that other tools can't handle, giving you additional visibility into your entire organization's systems.

Multi-Platform Log Management Support



Benefits of Advanced Log Collection Powered by NXLog

NXLog is a high-performance log gathering system that streamlines log management functions by ingesting your data into a central place to more easily filter, classify, convert, and digest.

Automate IT Security Operations

Simplify log collection by using a single product that reads many log sources and transmits logs to multiple destinations. Securonix offers event log parsing at the host level, which lowers the cost of distributing and managing log collection.

Reduce the Risk to Logs in Transit

Securonix with NXLog enables customers to send logs safely and reliably to Securonix Next-Gen SIEM.

Maintain Data Compliance

File integrity monitoring assists with compliance and detection by monitoring for changes to important files and folders.

Securonix Log Collection With NXLog

Securonix provides a scalable logging system by enabling data collection in multiple environments.

Centralized Log Management

Frictionless Log Acquisition

Extend and simplify data intake across a variety of sources with a single technology.

Agent-based Log Collection: NXLog runs as an agent supporting platform-specific data sources such as Windows event logs, Linux kernel logs, Android logs, local syslog, and more.

Agentless Log Collection: For embedded or legacy systems, such as routers and switches, that do not support agent installation, a server or device sends log data to an NXLog instance over the network, using its native protocols.

Log Centralization: NXLog gathers and manages log flow throughout the whole enterprise. Log centralization saves time and ensures that your log data is consistent.

Meet Compliance Mandates

Security Measures for Detection and Compliance

By providing the relevant log messages to Securonix Next-Gen SIEM, you can ensure that you are following compliance and standard requirements.

Compliance: Gain access to an integrated collection of audit logs to monitor changes to files and directories on all supported platforms, including Windows registry.

File Integrity Monitoring: NXLog's file integrity monitoring provides alerts on asset activities such as potential unauthorized changes. NXLog delivers better incident response, like the detection of malware outbreaks or malicious changes made by malware to critical assets, when used with Securonix Next-Gen SIEM.

Risk Mitigation

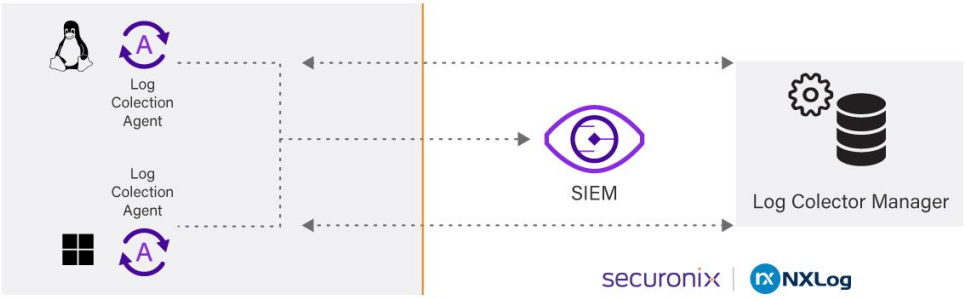
Reduce the Risk to Logs in Transit

Collecting logs from numerous devices with a single solution allows logs to move without losing their integrity. To decrease risk, the solution uses reliable transfer with compression, protocol-level acknowledgement, and batching.

SSL/TLS Data Encryption: Encryption protects log data in transit from being modified or viewed by an attacker. NXLog provides SSL/TLS data encryption; supports many input and output modules; and ensures strong authentication, message integrity, and message confidentiality.

Data Security: Secures log transfer and allows you to configure special privileges.

Securonix Log Collector Manager powered by NXLog



For more information about the Securonix Nex-Gen SIEM powered by NXLog, schedule a demo at: www.securonix.com/request-a-demo