Data Sheet

LogRhythm SysMon

LogRhythm
The Security Intelligence Company

LogRhythm SysMon enables customers to fulfill security and compliance use cases by performing data collection and generating rich host activity data. An optional component for the LogRhythm TLM platform, LogRhythm SysMon is a software agent that operates on endpoints, servers, and virtual machines running Windows, Linux, and UNIX.

LogRhythm SysMon for Data Collection

LogRhythm SysMon enables threat detection and response by consolidating and collecting log and machine data from local and remote environments and cloud infrastructure. Functioning as an agent-based data collector, it complements our agentless data collection options to facilitate the aggregation of log data, security events, and other machine data.

LogRhythm SysMon for Endpoint Monitoring & Forensics

Addressing advanced threats, compliance violations, and operational issues requires deep visibility into your environment, including the ability to correlate host activity with additional network information. Unfortunately, many categories of critical endpoint data are not available from Windows event logs and other typical sources. Even when available, many of these logs lack the level of detail necessary to achieve true visibility. Filling these gaps usually requires one or more additional agent-based solutions to perform independent monitoring.

LogRhythm SysMon's integrated endpoint monitoring and forensics capabilities perform independent logging of host activity. This telemetry enables multi-dimensional analysis of your wider environment, allowing you to:

- Detect and respond to security threats, including zero-day attacks
- Automate and enforce compliance with HIPAA, PCI, SOX, and other compliance regimes
- Monitor for operational issues, such as system and application failures

Extending the SmartResponse Automation Framework

LogRhythm SysMon extends the reach and flexibility of the LogRhythm SmartResponse™ automation framework. Together, the technologies can automatically or manually perform actions on an endpoint, such as:

- Monitoring the host to generate diagnostic and forensic data for accurate root cause analysis
- Disabling the network interface card for a compromised host
- Starting or disabling a process and collecting related information

Endpoint Monitoring Capabilities

- **File Integrity Monitoring** prevents corruption of key files by identifying when and by whom files and associated permissions are created, viewed, modified, and deleted.
- **Independent Process Monitoring** reports process and service activity, enabling detection of critical behavior, such as critical processes stopping and new/blacklisted processes (e.g., Tor) starting.
- **Windows Registry Monitoring** flags registry additions, modifications, deletions, permission (ACL) changes, and more. This provides the details necessary to detect advanced threats, compromised endpoints, and more.
- **Network Connection Monitoring** provides a detailed, independent log of all network connections opened and closed on a host, helping LogRhythm detect critical events, such as connections with unauthorized servers.
- **User Activity Monitoring** logs any user that authenticates to an endpoint, creating a forensic record to supplement and validate local auditing systems.
- **Data Loss Defender** monitors data transfers to and from removable media, such as USB drives, and can optionally block transfers on specific machines and devices.

LogRhythm SysMon Administration

LogRhythm SysMon efficiently supports large environments (>10,000 agents) through layered, policy-based configuration and central monitoring and management. Data processing is performed centrally, rather than on the endpoint, resulting in a minimal compute footprint.

SysMon transmits data to the LogRhythm data processing layer via a compressed and TLS-encrypted connection. The agent ensures data integrity during network interruptions by spooling volatile UDP traffic and tracking state for non-volatile data. Automatic failover across the data processing layer provides an additional level of resilience. SysMon Pro can be configured for unidirectional network communication paths, supporting classified environments and regulatory requirements.

LogRhythm SysMon Comparison Chart

SysMon is delivered in two versions—SysMon Lite and SysMon Pro—outlined below.

SysMon Lite	SysMon Pro
Ideal for Desktop Environments	Ideal for Server Environments
• Centralized management and updates • Guaranteed collection • TLS-encrypted communication • 10:1 data compression for transport • Remote data aggregation • Timestamp normalization • Scheduled collection • TCP forwarding	• Centralized management and updates • Guaranteed collection • TLS-encrypted communication • 10:1 data compression for transport • Remote data aggregation • Timestamp normalization • Scheduled collection • TCP forwarding
• Desktop endpoint monitoring - Windows Registry Monitoring for Desktops - Independent process monitoring - Network connection monitoring - User activity monitoring - Data Loss Defender for local storage devices • File integrity monitoring for desktops and point of sale systems - Detect reads, modifications, and deletions - Identify specific user or application - Support for policy layering	• Server endpoint monitoring - Windows Registry Monitoring for Servers - Independent process monitoring - Network connection monitoring - User activity monitoring - Data Loss Defender for local storage devices • File integrity monitoring for servers - Detect reads, modifications, and deletions - Identify specific user or application - Support for policy layering
• High-volume log collection - Syslog - UDP/TCP and secure syslog - Flat files (single-line and multi-line, compressed or uncompressed) - Windows Events, including custom event logs	• High-volume log collection - Syslog - UDP/TCP and secure syslog - Flat files (single-line and multi-line, compressed or uncompressed) - Windows Events, including custom event logs and database logs - Vendor-specific APIs (e.g., IBM iSeries, Cisco SDEE, Check Point OPSEC, Sourcefire eStreamer) - Cloud-based APIs (e.g., AWS, Azure, Box, Skyhigh, Salesforce) - Flow data (e.g., IPFIX, NetFlow, sFlow, J-Flow, SmartFlow) - SNMP - Vulnerability data (e.g., Qualys, Rapid7, Tenable Security Center) - LogRhythm Universal Database Log Adapter for system and custom logs written to database tables (e.g., Oracle, SQL Server, MySQL); ODBC & JDBC protocols • Unidirectional communications for classified environments - Integration with one-way data diodes • Support for classified/top-secret environments