

LogRhythm's Advanced Agent Technology enables customers to take advantage of several unique and powerful features that supplement traditional logging capabilities, such as encryption and File Integrity Monitoring (FIM). Benefits range from improved security and secure remote collection to compliance assurance for a variety of regulations. LogRhythm solutions can be configured to operate with or without the use of agents.

System Monitor

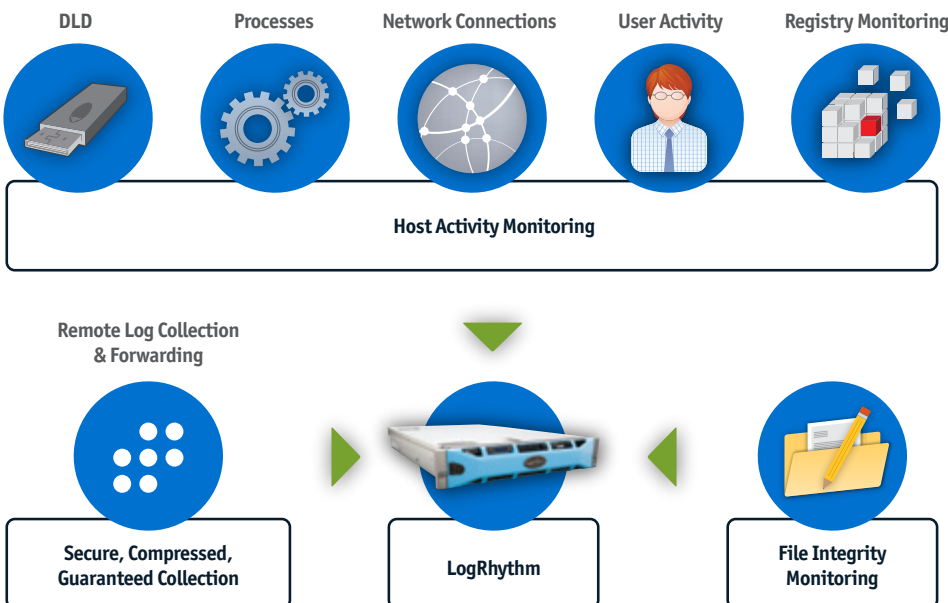
Available on Windows, Linux, Solaris, HP-UX and AIX, individual System Monitor Agents are capable of collecting from hundreds of devices and deliver:

- Centralised Management
- SSL Encrypted Communication
- Guaranteed Collection
- 10:1 Data Compression for Transportation
- Remote Data Aggregation
- Time Stamp Normalisation
- Scheduled Collection
- TCP Forwarding
- FIM for Desktops (including Point-of-Sale Systems)
 - Detect reads, modifications and deletions
 - Identify specific user or application
 - Support for multiple policies
- Host Activity Monitoring
 - Independent Process Monitor
 - Network Connection Monitor
 - User Activity Monitor
 - Data Loss Defender (DLD)
 - Windows Registry Monitoring (Desktops)

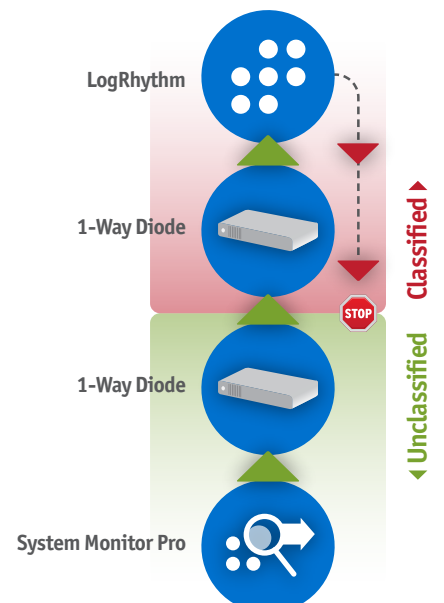
System Monitor Pro

In addition to functionality available with LogRhythm's System Monitor Agents, the following advanced features are available with the System Monitor Pro:

- High Volume Remote Collection
 - Database Logs
 - Cisco IDS - SDEE format
 - Check Point - OPSEC LEA
 - Flow Data
 - SNMP
 - Vulnerability Data
- FIM for Servers
 - Detect reads, modifications and deletions
 - Identify specific user or application
 - Support for multiple policies
- Host Activity Monitoring
 - Independent Process Monitor
 - Network Connection Monitor
 - User Activity Monitor
 - Data Loss Defender (DLD)
 - Windows Registry Monitoring (Servers)
- Unidirectional Communications for Classified Environments
 - Integration with one-way data diodes
 - Support for classified/top secret deployments



System Monitor / System Monitor Pro



System Monitor Pro - Unidirectional Communication