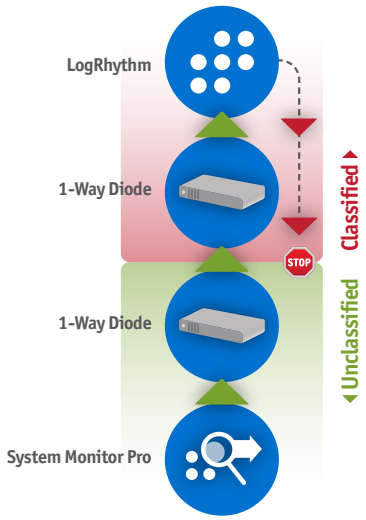
PRODUCT OVERVIEW

Collector Technology

LogRhythm

LogRhythm's collection technology facilitates the aggregation of log data, security events and other machine data using a variety of different techniques. It is architected for flexibility and can operate locally or remote for the collection of machine data. All data is transmitted via an authenticated and encrypted TLS. A Data Collector also ensures data integrity during a network connectivity interruption by spooling data while continuing to collect. They are also architected to support unidirectional networks for classified environments, including integration with one-way data diodes. All Data Collectors are centrally monitored and managed to simplify deployment, configuration and management and are configurable to failover to primary, secondary and tertiary Data Processors for high availability.



Data Collector Appliance: Provides remote, high-performance collection of all machine data including log messages, application data, security events, and network flows. A single Collector Appliance is capable of collecting and transmitting up to 10,000 messages per second from thousands of devices.

System Monitor: Local, agent-based collection is performed by the System Monitor. It serves a dual role as a locally deployed Data Collector and as an Endpoint Monitor. As a Data Collector, a single agent is capable of collecting from dozens of devices and thousands of messages per second and can be deployed on Windows, Linux and UNIX.

Universal Collection

Data Collectors are compatible with all types of devices and formats, including custom log sources, supporting the following methods:

- UDP/TCP and Secure Syslog (standard protocol)
- SNMP (standard protocol)
- Flow Data including IPFIX, NetFlow, sFlow, JFlow, and SmartFlow
- LogRhythm Universal Database Log Adapter for system and custom logs (e.g., audit, application, etc.) written to database tables (i.e. Oracle, SQL Server, MYSQL, etc.) (ODBC protocol)
- Windows Event Logs (local) (includes custom Event Logs)
- Windows Event Logs (RPC) (includes custom Event Logs)
- Vendor-specific APIs
  - Cisco SDEE
  - Checkpoint OPSEC/LEA
  - AS/400 and iSeries
  - Sourcefire eStreamer
  - Tenable Security Center
  - Cradlepoint
- Single and Multi-line Flat Files
- Compressed Single and Multi-line Flat Files
- Cloud/SaaS Solutions
  - Amazon AWS
  - Salesforce
  - Box
  - Office 365

Non-event data can also be collected via API:

- Vulnerability Scan Data: Nessus, Nexpose, Metasploit, Qualys, Retina, IP360/Tripwire
- User Directory Group Memberships or OU
- Active Directory Computer Domain Memberships
- McAfee's ePolicy Orchestrator and Remedy ticketing systems, via a two-way API
- Threat Intelligence feeds