PRODUCT OVERVIEW

Collection Technology

LogRhythm
The Security Intelligence Company

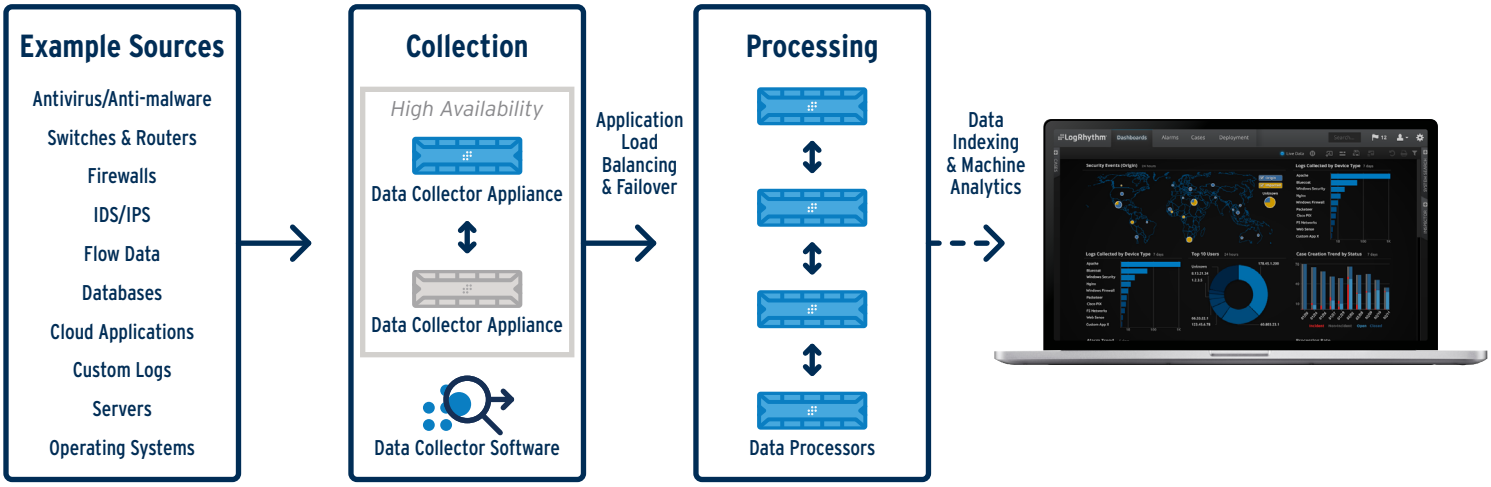
LogRhythm's collection technology facilitates the aggregation of log data, security events and other machine data. Data Collectors can operate locally or remotely and are centrally monitored and managed to simplify deployment and management. Deployment scalability is further enhanced by application load balancing between Data Processors.

Data is transmitted from Data Collectors via authenticated and encrypted TLS communications that can be compressed to minimize bandwidth utilization. Data Collectors can be configured for unidirectional network communication paths, supporting classified environments and regulatory compliance objectives.

Data Collectors ensure data integrity during network interruption by intelligently spooling volatile UDP traffic and tracking state for non-volatile data. Resilience is further buttressed through automatic failover between Data Processors.

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 can collect and transmit up to 10,000 messages per second from thousands of devices.

Data Collector Software: Local, agent-based collection is performed by System Monitor, software that also functions as an endpoint monitor. System Monitor can be installed on servers and virtual machines running Windows, Linux or UNIX. It consolidates and collects log and machine data from remote environments and cloud infrastructure. A single agent functioning as a Data Collector can collect thousands of messages per second from dozens of devices.



Universal Collection

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

- UDP/TCP and secure syslog
- SNMP
- Flow data (e.g., IPFIX, NetFlow, sFlow, J-Flow, SmartFlow)
- LogRhythm Universal Database Log Adapter for system and custom logs written to database tables (e.g., Oracle, SQL Server, MySQL) (ODBC & JDBC protocols)
- Windows Event Logs (includes custom event logs)
- Flat files (single-line and multi-line, compressed or uncompressed)
- Vendor-specific APIs (example sources):
  - AS/400 and iSeries
  - Checkpoint OPSEC/LEA
  - Cisco SDEE
  - Sourcefire eStreamer
- Vulnerability scanners (example sources):
  - Qualys
  - Rapid7
  - Tenable Security Center
- Cloud/SaaS solutions (example sources):
  - Amazon AWS
  - Box
  - Cradlepoint
  - Office 365
  - Salesforce