USE CASE

Network and Process Monitoring

LogRhythm

In today's globally distributed enterprises, it's critical to know what's happening throughout the entire IT environment and be able to tie it all together. The challenge is finding a way to correlate event data that is consistently recorded with activities that may not be regularly logged, such as processes starting and stopping or network connections being established.

LogRhythm delivers independent awareness and unprecedented insight into what's happening on your network, from routers and switches to host systems and endpoint devices–both inside *and* outside the network. Automated data enrichment adds event-specific network context, such as Source IP and Impacted Host. LogRhythm also factors in network-aware risk-level information with event and asset-specific risk ratings, providing a comprehensive and globally aware view of the entire IT environment.

Network Connection and Process Monitoring deliver rapid insight into critical events by providing access to detailed event information at the endpoint, above and beyond what is available in standard log data.

Process Monitor	Network Connection Monitor	Secure, Reliable Communication
CUSTOMER CHALLENGE		
Enterprise IT systems have a constant flow of processes starting and stopping, but they are inconsistently logged, making them difficult to monitor without an independent record of the event. The sheer volume of activities makes identifying failing or rogue processes difficult.	Access to host-level detail surrounding network behavior is a critical component of real time monitoring and forensic analysis. This can be limited in an enterprise environment due to a lack of connection-specific log data or limited access to flow data.	Gathering accurate endpoint data from remote devices like Point-of-Sale systems is particularly challenging for IT organizations. Problems range from limited bandwidth, unencrypted and unreliable UDP transport, to managing individual collection mechanisms on each device.
LOGRHYTHM SOLUTION		
LogRhythm's Host Activity Monitoring creates an independent log of all processes and adds valuable context, including process name, user or account that owns the process, and process start time and duration.	LogRhythm's Host Activity Monitoring creates an independent log with relevant detail such as ID port, communication direction, the process that opened the connection and users that are logged in.	In addition to independent, detailed logging of network connections and processes, LogRhythm's centrally managed agents provide SSL encryption, 10:1 compression, reliable TCP transportation and spooling capabilities during dropped connections.
ADDITIONAL BENEFITS		
LogRhythm can automatically alert on non white-listed processes when they are started on controlled servers and devices. Additional visualization tools can be used to map all locations within the environment where that same process is running for rapid forensic and root cause analysis.	LogRhythm can alert on suspect behavior and blacklisted activities, such as unauthorized hosts running web servers or ftp services running on confidential file servers. Actual in-use services can also be reverse-engineered to help establish tighter access control lists.	LogRhythm's agents provide additional independent security and compliance controls at the endpoint with fully integrated File Integrity Monitoring and protection against unauthorized removable media usage via Data Loss Defender.