PRODUCT OVERVIEW

Endpoint Monitoring and Forensics

LogRhythm
The Security Intelligence Company

Protecting your organization from advanced threats, compliance violations and operational issues is an ongoing process. It requires broad visibility, continuous monitoring, automated behavioral analytics, advanced threat detection, intelligent countermeasure capabilities, and ongoing adaptation to new and evolving issues and threats. A key component of that process is having the ability to correlate what's happening at the endpoint level to event data throughout the network. LogRhythm delivers extended visibility and protection via fully integrated Endpoint Monitoring and Forensics.

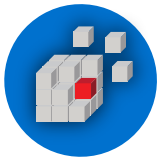
Correlating network-wide event data with activities occurring on the endpoint is often hindered by the fact that critical endpoint-based activities may not be consistently logged, often requiring multiple solutions to fill the information gaps. Endpoint Monitoring and Forensics provides independent awareness and insight into what's happening on an endpoint, providing a critical layer of protection from a broad spectrum of problems, ranging from important operational events such as system and application failures to security and compliance violations tied to unauthorized or malicious activity.

Centrally monitored and managed as a fully integrated component of LogRhythm, Endpoint Monitoring and Forensics includes:

- Independent logging of critical endpoint activity
- Detection of changes made to the Windows startup registry
- Comprehensive event detail
- Protection from zero-day attacks and critical failures
- Prevention of unauthorized data transfers
- Full integration with all event data for true correlation and event context

Independent Process Monitor

Detects and records process and service activity that may not otherwise be reported. This can identify and alert on important behavior like endpoints running blacklisted processes (peer-to-peer clients, etc.), critical processes stopping or any non-approved process starting up.



Windows Registry Monitor

Monitors the Windows Registry for additions, modifications, deletions, permission (ACL) changes, and ownership changes. This visibility provides greater insight into changes or manipulations of Windows operating systems, like the addition of new startup processes, to detect advanced threats and compromised endpoints.

Network Connection Monitor

Independently records network connection activity to and from the endpoint, providing a detailed, independent log of all network connections opened and closed on a endpoint. It detects and alarms on critical events on the endpoint like activity from unauthorized web or FTP servers.

Data Loss Defender

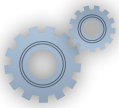
Monitors and prevents data transfers to and from removable media like CD/DVD-RW devices and USB drives. Data Loss Defender logs, alerts on, and audits all data transfers to removable media ports and can optionally block transfers on selected machines and devices.

User Activity Monitor

Logs any user or process that authenticates to an endpoint. This independently records an audit trial that can be used to either supplement local auditing systems or to validate that system logs have not been modified on the endpoint.

LogRhythm's Endpoint Monitoring and Forensics, combined with LogRhythm's comprehensive Security Intelligence Platform, provides tremendous visibility into what's going throughout the IT Environment. By harnessing the power of Smart**Response**™, LogRhythm provides extensive, active protection at the endpoint level from advanced threats, compliance violations, and operational issues.

Independent Process Monitor



Problem Enterprise IT systems have a constant flow of processes starting and stopping, but they are inconsistently logged. This makes it challenging to detect individual events, such as critical processes restarting properly after routine maintenance, without an independent record of the event.

Detection LogRhythm can independently detect and alert whenever a blacklisted process starts or when a critical process stops or fails to restart following a specific event, such as a reboot.

Response Smart**Response**™ can stop and/or start individual processes, pulling all relevant information, such as the process name and impacted endpoint, directly from the alarm.

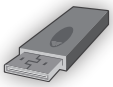
Network Connection Monitor

Problem Endpoint-level detail surrounding network behavior is a critical component of real time monitoring and forensic analysis. This can be difficult due to a lack of connection-specific log data or limited access to flow data.

Detection LogRhythm creates an independent log of every network connection on a monitored endpoint, including relevant detail such as ID port, communication direction and the process that opened the connection.

Response Smart**Response**™ can be configured to automatically close an unauthorized port or shut down a suspicious network connection in response to any alarm.

Data Loss Defender



Problem Many advanced threats that result in data breaches employ physical means of transferring information, using removable media sources such as UDB thumb dives and CD/DVD-RW devices to remove sensitive data from the network.

Detection LogRhythm can independently detect the use of removable media directly on the endpoint, generating an alarm before data can be transferred to or from a removable media device.

Response Data Loss Defender can automatically prevent data from being transferred to or from removable media directly, by immediately ejecting or unmounting the device.

User Activity Monitor

Problem Knowing who is logged in to a particular endpoint when malicious activity or a critical operations failure happens is a key component to comprehensive understanding of a specific event.

Detection LogRhythm can independently log who is logged in and for how long, correlating user audit activity with other log and event data, creating a comprehensive audit of user behavior throughout the IT environment.

Response Smart**Response**™ can disable suspiciously behaving user accounts automatically or following an optional approval process.

Windows Registry Monitor

Problem Changes to the Windows Registry are not natively logged, making it difficult to detect modifications, like the addition of malicious software. Once embedded in the registry, malware can easily propagate by controlling processes, downloading payloads, and infecting additional systems.

Detection LogRhythm can independently monitor the Windows Registry to detect changes, including the introduction of malicious software and new startup processes.

Response When changes to the Registry are detected, LogRhythm alerts IT and security personnel. If a change is found to be malicious, administrators can approve a Smart**Response**™ plug-in that disables the startup processes to prevent the spread of malware.

Endpoint Lockdown

Problem Devices continue to operate on a network even after a compromise is detected. This allows malicious software to infiltrate the organization, spread to other systems and gain increasing access to network resources.

Detection Smart**Response**™ can automatically run a series of scans directly on the host to generate extensive diagnostic and forensic data for accurate root cause analysis.

Response Smart**Response**™ can prevent a compromised host from affecting other devices on the network by automatically disabling device and user access to other resources