PRODUCT OVERVIEW

Host Activity Monitoring

Protecting your organization from advanced threats, compliance violations and operational issues is an ongoing process. It requires broad visibility, continuous monitoring, advanced analysis and pattern recognition, intelligent countermeasure capabilities, and ongoing adaptation to new and evolving issues and threats. A key component of that process is having the extended visibility to correlate what's happening at the host level to event data throughout the network. LogRhythm delivers extended visibility and protection via fully integrated Host Activity Monitoring.

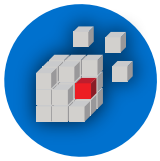
Correlating network-wide event data with activities occurring at the host level is often hindered by the fact that critical host-based activities may not be consistently logged, often requiring multiple solutions to fill the information gaps. Host Activity Monitoring provides independent awareness and insight into what's happening on a host, 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, Host Activity Monitoring includes:

- Independent logging of critical host 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 such as hosts running blacklisted processes (such as peer-to-peer clients), 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, including the addition of new startup processes, to detect advanced threats and compromised hosts.

Network Connection Monitor

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

Data Loss Defender

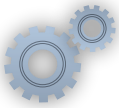
Monitors and prevents data transfers to and from removable media such as CD/DVD-RW devices and USB drives. Data Loss Defender logs, alerts on, and audits all data transfers to removable media ports and can optionally block transfers on selected machines and devices.

User Activity Monitor

Logs any user or process that authenticates to a host. 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 host.

LogRhythm's Host Activity Monitoring, 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 host 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 restart individual processes, pulling all relevant information, such as the process name and impacted host, directly from the alarm.

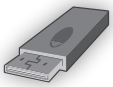
Network Connection Monitor

Problem Access to host-level detail surrounding network behavior is a critical component of real time monitoring and forensic analysis. This can be difficult in an enterprise environment 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 host, 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 host, 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 on the host, by immediately ejecting or unmounting the device, for real time protection.

User Activity Monitor

Problem Knowing who is logged in to a particular host 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 immediately remove from a network unauthorized users or those who engage in suspicious or detrimental behavior – with or without requiring authorization before taking action.

Windows Registry Monitor

Problem Changes to the Windows Registry are not natively logged, making it difficult for organizations to detect changes to the registry, including 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 Windows Registry are detected, an alarm is triggered alerting IT and security personnel to the activity. If the change is determined to be malicious, administrators can approve a Smart**Response**™ plug-in that automatically disables the startup processes to prevent the spread of malware.