PRODUCT OVERVIEW

LogRhythm and Symantec: Symantec Security Information Manager (SSIM) Migration Program

Following Symantec's end-of-sale announcement for Symantec Security Information Manager (SSIM), customers are looking for alternative solutions to meet their SIEM needs. For customers that want or require an on-premise solution, LogRhythm has developed a simple and efficient migration path from SSIM to LogRhythm's best-in-class Security Intelligence Platform.

To protect themselves in today's rapidly evolving cyber threat landscape, organizations require deep visibility and intelligence across the breadth of their IT environments. LogRhythm's Security Intelligence Platform uniquely combines next-generation Security Information & Event Management (SIEM), Log Management, Endpoint Forensics and Network Forensics in a highly scalable, unified platform that empowers organizations to comply with regulatory requirements and detect today's most sophisticated cyber threats and breaches faster and with greater accuracy than previously possible.

LogRhythm for Enterprise Security Intelligence

☑ Real-time Threat Detection & Response

☑ Compliance Automation & Assurance

☑ Robust support for Symantec products

☑ Easy to deploy, manage and use

☑ Global 24x7 support

A Higher Standard for SIEM & Security Intelligence

LogRhythm delivers a new generation of capabilities for detecting, defending against and responding to cyber threats and associated risks. LogRhythm's Security Intelligence Platform delivers:

- Next-Generation SIEM and Log Management
- Independent Endpoint Forensics and File Integrity Monitoring
- Network Forensics, with application ID, metadata extraction, search and Full Packet Capture
- Highly scalable, state-of-the art machine analytics
  - Advanced Correlation and Pattern Recognition that is flexible and powerful yet easy to use
  - Multi-dimensional User/Network/Endpoint Behavior Profiling & Anomaly Detection
- Rapid, intelligent search across 100% of data collected
- Large data set analysis via visual analytics, pivot and drill down
- Workflow-enabled automatic response via LogRhythm's Smart**Response**™
- Integrated case management

Collecting 100% of the log, flow, event and other machine data generated in an environment and combining it with LogRhythm's independently generated host and network forensic data, delivers deep visibility to customers. LogRhythm's patented Advanced Intelligence Engine (AIE) machine analytics technology leverages this data to provide automated, continuous analysis of all activity and behavior observed across the environment, delivering global visibility and actionable intelligence.

Broad Forensic Data Collection

LogRhythm provides device and application intelligence with extensive and ever-expanding support for well over 700 unique systems and devices, including security devices, networking equipment, applications, databases, operating systems, virtual environments and industry-specific devices (e.g. POS, SCADA, etc.). LogRhythm's collection support includes the vast majority of systems and devices currently supported by Symantec Security Information Manager, including key Symantec technologies such as:

- Symantec Enterprise Security Manager
- Symantec Endpoint Protection
- Symantec Data Loss Prevention
- Symantec Sygate Enterprise Protection
- and others

Rapid Time to Value

LogRhythm's integrated architecture, next-generation analytics and robust out-of-the-box capabilities ensure a solution that is highly flexible and yet very easy to deploy, manage and use, delivering rapid time to value. LogRhythm provides a robust and regularly updated Knowledge Base that includes:

- An extensive and ever-expanding collection of log parsing rules
- A growing library of advanced analytics and correlation rules, layouts, dashboards and saved investigations
- Compliance Automation Suites for PCI, SOX, HIPAA, FISMA, GLBA, ISO27001, DODI 8500.1, NERC-CIP, and others
- Security Analytics Modules such as:
  - Privileged User Monitoring
  - Advanced Persistent Threats (APT) Detection
  - Web Application Defense
  - User/Endpoint/Network Behavior Anomaly Detection
  - and others

Flexible Deployment Options

High Performance Appliances

	ALL-IN-ONE (XM) (Includes PM, DPX, AIE)		DEDICATED PLATFORM MANAGER (PM) (Includes AI Engine License)		DEDICATED DATA PROCESSOR (DP)		DEDICATED DATA INDEXER (DX)		DEDICATED AI ENGINE (AIE)		DATA COLLECTOR (DC)	NETWORK MONITOR (NM)		WEB APPLIANCE
Appliance Lines	4301	6400	5400	7400	5300	7400	5300	7400	5400	7400	3300	3300	5400	3300
Max Archiving Rates	10,000 MPS	25,000 MPS	N/A	N/A	10,000 MPS	50,000 MPS	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Max Processing Rates	1,000 MPS	5,000 MPS	N/A	N/A	5,000 MPS	15,000 MPS	N/A	N/A	30,000 MPS	75,000 MPS	N/A	1 Gbps	2.5 Gbps	N/A

THE SANS COMMUNITY

has voted LogRhythm the Best SIEM of 2014.

SANS INSTITUTE

> **LogRhythm earns HIGH MARKS**
>
> **“FROM READERS ACROSS THE BOARD.”**
>
> INFOWORLD

Software | Virtualization

In addition to pre-configured, high-performance appliances, LogRhythm software can be easily deployed on customer-provided hardware and on most virtualization platforms.

vmware® Windows Server 2012 CiTRIX® XenServer

LogRhythm Services & Support

LogRhythm delivers world class professional services and support across the globe to ensure customer success and satisfaction. The company’s professional services team offers a complete range of services from deployment services to training to proactive maintenance and health checks, and more. LogRhythm’s PS organization also has significant experience transitioning new customers from legacy SIM/SIEM solutions to LogRhythm’s next-generation platform. LogRhythm technical and user support is available worldwide on either a 11x5 or 24x7 basis and can be contracted in one, two or three year increments.

LogRhythm Labs

LogRhythm™ Labs

LogRhythm Labs is a team of Information Security subject matter experts and advanced threat researchers who act as a virtual security threat and compliance research team to deliver out-of-the box intelligence and embedded expertise for advanced threat management and compliance automation & assurance.

LogRhythm in Action

Detecting Custom Malware

Challenge: Custom malware tied to zero-day attacks is specifically designed to evade traditional security solutions built to detect known signatures and behaviors.

1. LogRhythm baselines “normal” host behavior and creates a whitelist of acceptable process activity.
2. Host Activity Monitoring independently detects a new process starting.
3. LogRhythm automatically recognizes that the new process is non-whitelisted.
4. LogRhythm’s machine analytics corroborates the event against related activity such as abnormal network traffic, accurately identifying the activity as high risk.
5. An alarm is sent to a Security Administrator, who can easily access forensic details to investigate.

Exposing Compromised Credentials

Challenge: With increasingly mobile workforces and growth in BYOD, enterprises are challenged to identify when a user’s credentials have been compromised.

1. LogRhythm can automatically establish “normal” profiles for specific users, including whitelists of acceptable activity and baselines of observed behaviors.
2. LogRhythm’s machine analytics detects abnormal user account activity, such as log-ins from suspicious locations, or deviations from normal behavior, like accessing unusual data sources or larger-then-normal volume of data and uploading that data to a non-whitelisted cloud sharing application.
3. SmartResponse™ can disable the account automatically or a more detailed forensic investigation.

Detecting Data Exfiltration

Challenge: The constant flow of data in and out of an enterprise makes it difficult to detect when sensitive data leaves the corporate network.

1. LogRhythm Network Monitor can provide critical visibility into network session activity and application use at network ingress/egress points.
2. LogRhythm’s machine analytics establishes various behavioral baselines across observed network activities.
3. Network-based anomalies are identified and corroborated against other log and machine data to detect high-risk activity associated with data exfiltration.
4. SmartCapture™ automatically captures all packets associated with the suspicious activity for full session reconstruction.

To learn more about LogRhythm’s SSIM Migration Program, email LogRhythm at

sales@logrhythm.com