Joint Solution Brief

LogRhythm™

Mimecast

Combining LogRhythm's automated threat management and enterprise security with Mimecast's email security services

Benefits

- ✓ Accelerate response to phishing and business email compromise tactics
- ✓ Leverage multi-dimensional behavioral analytics to deliver real-time security intelligence
- ✓ Gain deep visibility into all aspects of user, network, and endpoint behavior activity throughout the IT environment
- ✓ Utilize shared high-fidelity indicators to accurately identify the root cause of an attack and remediate the threat

Solution overview

LogRhythm SIEM integrates Mimecast's email security with LogRhythm's enterprise threat management. LogRhythm's scenario- and behavioral- based analytics automatically consumes email security data from the Mimecast cloud service, along with other security data from across an organization to deliver real-time threat protection based on up-to-date situational awareness and comprehensive security analytics.

By leveraging Mimecast's Data Logging API to feed data into the LogRhythm platform, customers benefit from leading enterprise security and threat management capabilities. The combined solution delivers the ability to monitor and secure a range of systems and applications throughout the IT environment and to respond to security threats based on accurate, relevant, and up-to-date information.

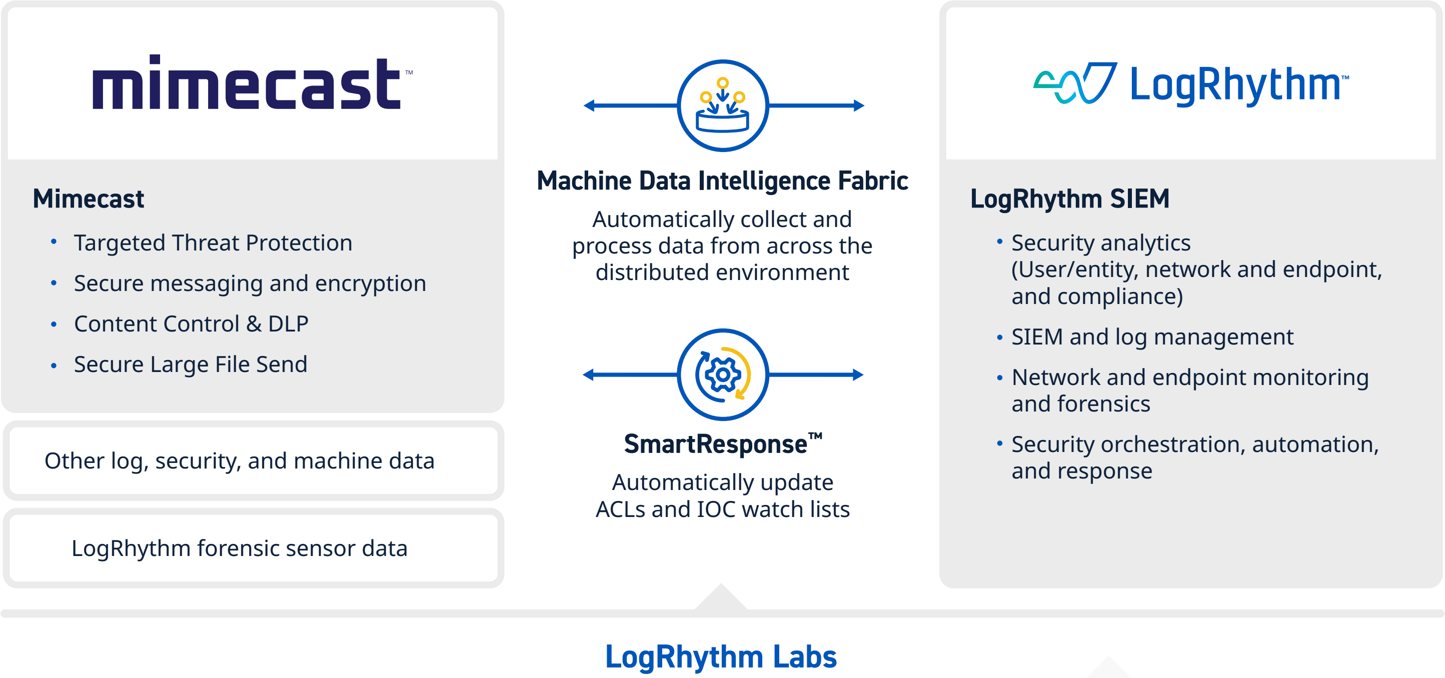
mimecast™

About LogRhythm and Mimecast

LogRhythm and Mimecast work together to help organizations around the globe increase email visibility and protect against modern cyberattacks. LogRhythm offers extensive support for and integration across the Mimecast's product portfolio. The combined solution empowers security teams to identify behavioral anomalies, internal and external threats, and to prioritize their responses based on accurate enterprise security intelligence. LogRhythm and Mimecast empower security teams to navigate a changing threat landscape with confidence. Together, LogRhythm and Mimecast are ready to defend.

Log collection

Securing any security operations center (SOC) begins with high-fidelity and trustworthy log data. While other vendors outsource their log collection methodology to the SOC analyst, LogRhythm provides log sources reviewed by dedicated security experts with dozens of years of security experience. LogRhythm Machine Data Intelligence (MDI) Fabric optimizes and stabilizes the ideal route of collection for over 950 log sources. Our security teams review these sources and ensure that relevant security data is normalized with other consumable security data. The results are trusted logs and alerts that allow for precision rule creation and comprehensive remediation efforts in the event of an attack.



Mimecast

- Targeted Threat Protection
- Secure messaging and encryption
- Content Control & DLP
- Secure Large File Send

Other log, security, and machine data

LogRhythm forensic sensor data

Machine Data Intelligence Fabric

Automatically collect and process data from across the distributed environment

SmartResponse™

Automatically update ACLs and IOC watch lists

LogRhythm SIEM

- Security analytics (User/entity, network and endpoint, and compliance)
- SIEM and log management
- Network and endpoint monitoring and forensics
- Security orchestration, automation, and response

LogRhythm Labs

How it works

LogRhythm SIEM collects from every device, application, and sensor in an environment. Our MDI Fabric classifies and contextually structures every log message.

When used with Mimecast, the LogRhythm platform connects to the Mimecast Data Logging API and collects logs. Data is then parsed and normalized to the LogRhythm schema using features such as our patented TrueTime™ process, which records the actual time of occurrence, automatically correcting time zone, device clock offsets, and collection offsets. The data is incorporated by LogRhythm into automated advanced correlation rules to deliver highly focused alerts that identify when an organization is experiencing an email-borne attack and/or suspicious activity is occurring within their environment. Normalized data is used by LogRhythm SIEM for analysis, storage, and reporting via a consolidated dashboard of all security events. If an alarm is detected, it is logged and displayed in LogRhythm's Web Console for centralized investigation and action.

Use Case

Combined data sharing for end-to-end threat management

Challenge:
Organizations need the ability to correlate the data from their disparate security products and services and distinguish the real threats from false alarms.

Solution:
LogRhythm can incorporate the data from Mimecast's Data Logging API into automated advanced correlation rules. This delivers highly focused alerts that identify when an organization is experiencing an email-borne attack or suspicious activity is occurring within their environment.

Defend against email-borne attacks

Challenge:
91% of cyberattacks begin with some type of phishing attack.[1] Protecting against routine spam and malware is important but defending against targeted attacks is also needed.

Even with extensive user training, phishing emails are still opened and acted upon. Automatically protecting the organization against email-borne attacks should be a top priority.

Solution:
Mimecast addresses critical email security issues with:

- Targeted threat protection
- Spam and multi-layered malware protection
- Secure messaging and encryption
- Data leak prevention
- Secure large file sharing

The Mimecast cloud-based service means always-on, always up-to-date protection without the complexity and cost of traditional offerings.

How automated workflows work

To streamline security response workflows, organizations can use LogRhythm SmartResponse™, which is part of LogRhythm's security orchestration, automation, and response (SOAR) solution. LogRhythm SmartResponse accelerates response to suspicious emails and URLs contained within the messages. While LogRhythm has a dedicated engineering team that builds actions, this is by nature an open framework that enables Mimecast customers to modify actions or write their own custom integrations to protect their unique IT or operational technology (OT) environments.

The LogRhythm SmartResponse for Mimecast contains actions that are configured to execute automatically in the event of an alarm or manually through analyst workflow. Security teams can enable LogRhythm SmartResponse actions to block senders (user or domain) or create a managed URL allowing the teams to blacklist or whitelist URLs contained in an email message. Each action can be configured to require approval before execution.

[1] What Is Spear Phishing?, KnowB4, 2022.

LogRhythm SmartResponse actions for Mimecast

Action	Description	Use Case
Create Configuration File	Execute this response and rerun it before using other available actions whenever you change the fixed-value parameter	Functionality must run first before other SmartResponse functions can execute
BlackList Domain	Adds a domain to the blacklist	Add malicious domain to blacklist
Block a Domain from URL	Blocks a specified URL containing a suspicious domain	Block malicious domain from a URL
Block Sender	Blocks a specific sender	Block the sender of suspicious emails
Block URL	Blocks a specific URL	Block suspicious URL
Get Group Members Information	Displays information about members of a specified group	Fetch information about members of a specified group
Get Profile Information	Displays information about a sender of suspicious emails	Fetch information about a sender of suspicious emails

For more information, request a LogRhythm demo.
logrhythm.com/demo