PURESTORAGE®
Uncomplicate Data Storage, Forever

SOLUTION BRIEF

Merged Threat Detection and Response in a Flash

Integrating Pure Storage FlashArray™ with LogRhythm SIEM

LogRhythm and Pure Storage work together to help organizations of all sizes increase visibility into their modern flash data storage. LogRhythm offers integration of alert logs automatically incorporating, normalizing, and contextualizing log flow and event data captured from the industry leading all-Flash arrays from Pure Storage. The combined solution helps security teams to identify internal and external threats while minimizing the cost of implementing, managing, and monitoring the platforms.

Solution Overview

Data storage is the most common target for attack—holding data at ransom or taking of data by an insider. Slow response to these threats means data can be stolen or the company held hostage for payment. Often, security applications do not have deep insight into the activity on the storage systems hiding activity that signal an event.

Pure Storage and LogRhythm have teamed up to deliver direct event log ingestion from FlashArray to shorten the time to event identification and SmartResponse actions to automate responses to those events. The faster an event is identified, the faster a response can be executed protecting your data and business from harm. By adding log event data at the storage level, LogRhythm SIEM can filter out the noise and give you and your team actionable insight.

To protect your data, Pure Storage offers SafeMode™ Snapshots, immutable snapshots used to protect your critical data. Ransomware can't delete, modify, or encrypt the snapshot—shielding your data from loss, infection, encryption, or other attacks. Your operations are either minimally interrupted or not impacted at all. And forget about paying the ransom. In other words, you have control over your data, not the intruder. What makes this even better? SafeMode functionality is built into Pure Storage products. There's no complicated setup, no professional services engagement, and no compromises.

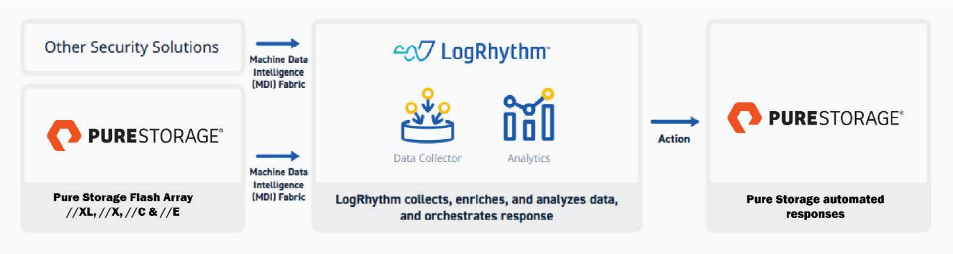
Other Security Solutions
Machine Data Intelligence (MDI) Fabric
PURESTORAGE®
Machine Data Intelligence (MDI) Fabric
Pure Storage Flash Array //XL, //X, //C & //E
LogRhythm
Data Collector
Analytics
LogRhythm collects, enriches, and analyzes data, and orchestrates response
Action
PURESTORAGE®
Pure Storage automated responses

FIGURE 1 Pure Storage and LogRhythm SIEM integration

Protect Data Assets

- Immutable snapshots stop attacks from encrypting or deleting backups and critical data.
- Native integration of storage workflows increases adoption in alarm workflows.

Deep Storage Insights

- Automated responses to common security alerts reduce risk and shortens time to event closure.
- Security event automation is handled within normal SOC engineering/operations.

Benefits

- Increase visibility into the storage stack—the most common target for attack
- Protect your most critical data with automated responses including SafeMode Snapshots
- Simplify security deployments for on-premises FlashArray appliances

FlashArray Log Collection

Managing 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 1,000 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.

For Pure Storage FlashArray, syslog alerts from the appliance are evaluated for common attack indicators. Software configuration changes, network configuration changes, and drops in data compression or reduction rates can all be indicators of something innocuous or sinister. LogRhythm's AI Engine rules are triggered for logs that get ingested and automated or manual actions can be taken based on rule or policy. Sending these alerts to LogRhythm SIEM enables full visibility into the actions happening in your environment and allows the tools and your security team to evaluate and act as needed.

How Automated Workflows Work

To streamline security response workflows, organizations can use SmartResponse automated actions, which are part of LogRhythm's security orchestration, automation, and response (SOAR) solution. LogRhythm SmartResponse accelerates response to malware threats to minimize damage, eliminating manual intervention by security analysts. This advanced capability is delivered to end users through the LogRhythm SmartResponse for Pure Storage FlashArray.

The SmartResponse for FlashArray contains multiple workflows that are configured to execute automatically in the event of an alarm or manually through the analyst workflow. For example, if malicious activity is detected on any endpoint, an alarm can be raised and a snapshot of the appropriate protection groups or volumes on the FlashArray can be taken. The LogRhythm SmartResponse for Pure Storage FlashArray centralizes functionality of manual or automated response between the LogRhythm SIEM and Pure Storage's Flash Arrays. Other example actions and their use cases are provided in the table below.

SmartResponse Automated Actions for Pure Storage FlashArray

Action	Description	Use Case
Take Protection Group Volume Snapshot	Creates a point-in-time snapshot of the contents of a protection group	An attack is detected and a storage SafeMode snapshot is taken to secure critical data
Take Volume Snapshot	Creates a point-in-time snapshot of the contents of a volume	An attack is detected and a storage SafeMode snapshot is taken to secure critical data
Remove Directory User	Deletes one or more local users	A malicious user is downloading data in a data breach
Remove Directory Service Local Member	Removes a local user from a directory services group local user group	A user account has been compromised and is trying to dump or delete critical data

TABLE 1 LogRhythm SmartResponses for Pure Storage FlashArray

About LogRhythm

LogRhythm helps security teams stop breaches by turning disconnected data and signals into trustworthy insights. From connecting the dots across diverse log and threat intelligence sources to using sophisticated machine learning that spots suspicious anomalies in network traffic and user behavior, LogRhythm accurately pinpoints cyberthreats and empowers professionals to respond with speed and efficiency.

With cloud-native and self-hosted deployment flexibility, out-of-the-box integrations, and advisory services, LogRhythm makes it easy to realize value quickly and adapt to an ever-evolving threat landscape. Together, LogRhythm and our customers confidently monitor, detect, investigate, and respond to cyberattacks.

About Pure Storage

Pure Storage uncomplicates data storage, forever. Pure Storage delivers a cloud experience that empowers every organization to get the most from their data while reducing the complexity and expense of managing the infrastructure behind it. Pure Storage's commitment to providing true storage as-a-service gives customers the agility to meet changing data needs at speed and scale, whether they are deploying traditional workloads, modern applications, containers, or more. Pure Storage believes it can make a significant impact in reducing data center emissions worldwide through its environmental sustainability efforts, including designing products and solutions that enable customers to reduce their carbon and energy footprint. And with a certified customer satisfaction score in the top one percent of B2B companies, Pure Storage's ever-expanding list of customers are among the happiest in the world.

Additional Resources

- Security Made Easy with LogRhythm
- Discover Pure Storage data protection solutions
- Learn how SafeMode secures data from ransomware attacks

purestorage.com

800.379.PURE

PURESTORAGE®
Uncomplicate Data Storage, Forever