PURESTORAGE®
Uncomplicate Data Storage, Forever

SOLUTION BRIEF

Threat Detection and Response in a Flash

Pure Storage® and LogRhythm secure data with improved threat detection, automated responses and orchestrated recovery to security events.

Security teams are struggling to keep up with the increase in quantity and complexity of security threats. Ransomware is on the rise, data breaches can tarnish hard earned brand reputation, and increased regulatory compliance requirements strain the capabilities of security teams and systems. The complexity of heterogenius hardware and software providers, on-premises, cloud, and hybrid workloads, and an evolving connected experience means limited time and resources to manage at scale in the modern data center.

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.

Developing a security strategy is a never-ending process due to an ever-changing data landscape, attack vectors, and threats in the modern hyper-connected world. IT and security specialists are struggling to maintain the massive number of touchpoints that exist within today's corporate environments: traditional desktops, servers, and network devices; employee-owned mobile devices; public, private, and semi-private cloud environments; shared data access points. Compound the number of touchpoints with the ever-growing number of configuration options and states that each hardware and software vendors offer, and the matrix of discovery, monitoring, and manageability becomes nearly impossible to handle. These integration silos open the door for security threats to go unidentified—increasing your exposure to damage from those threats.

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.

Decrease Risk Through Better Detection and Identification

Pure Storage and LogRhythm have teamed up to deliver direct event log ingestion from FlashArray to shorten the time to event identification. The faster an event is identified, the faster the resolution 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. Spend your time on impactful work instead of maintaining, caring for, and feeding your SIEM. You can automate repetitive tasks and labor-intensive work with embedded security orchestration, automation and response (SOAR) capabilities so your team can focus on your business outcomes. Extending the log management capabilities to the storage tier allows LogRhythm SIEM to effectively collect and normalize event data to enable accurate and reliable analysis. With real-time visibility across your environment, you can quickly identify and prioritize potential security issues.

Automated Responses Reduce Threat Impact

LogRhythm SIEM provides a complete view of events happening in your network and uses the power of Machine Learning (ML) to identify, alert and respond to security events and alarms. With innovative SmartResponse™ automation, you can plan how to handle a security alert before they happen to reduce any impact with pre-programmed responses. With out of the box responses to common alerts, your team can focus on business specific responses to alerts to meet your business needs. This lets your team overcome the endless manual security task list and accelerate threat qualifications, investigations, and responses. You can even choose from fully automated playbook actions or semi-automated, approval-based response actions that allow users to review before countermeasures are executed, giving you total control over your business. With these security orchestration capabilities, your team will be able to centralize all associated case evidence in LogRhythm's evidence locker repository for final resolution and easy access in the future.

Orchestration Secures Critical Data

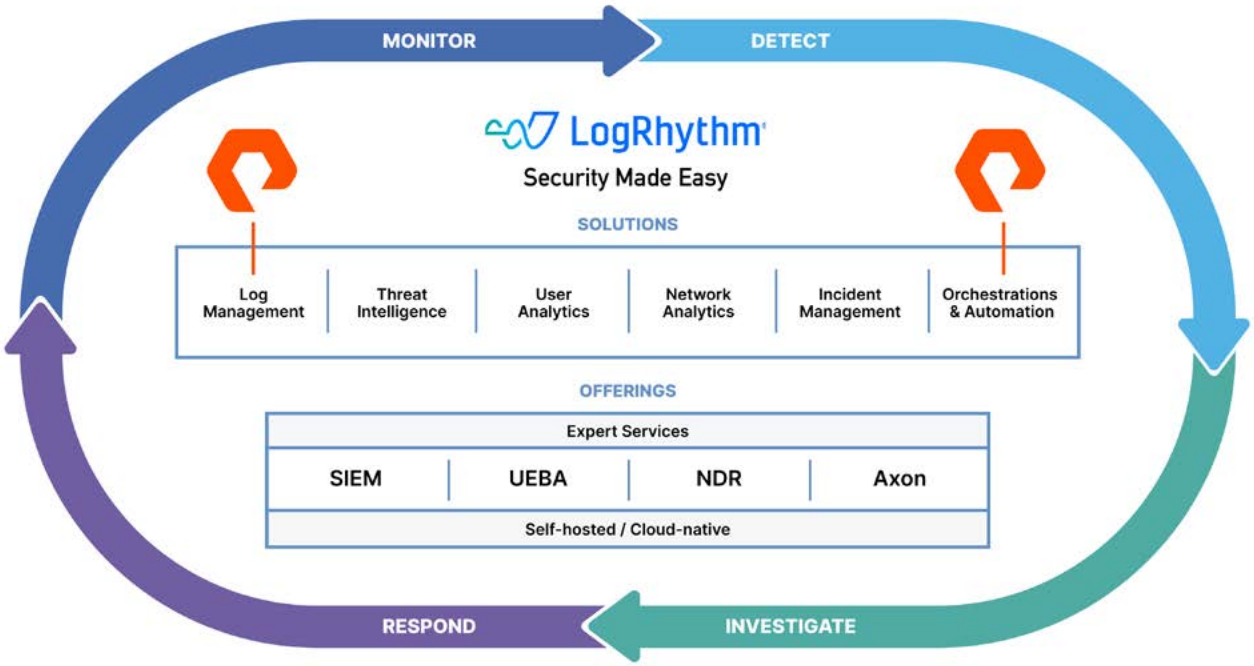
Orchestration of threat responses remove manual steps and potential risk. Pure Storage SafeMode™ is an immutable snapshot capability used to protect your data in the event of a ransomware, malware or other bad actor attack. The best part is, bad actors cannot delete, modify, or encrypt the snapshot even if the administrator's credentials are compromised. Your data is safe, and your snapshots are locked. Pure Storage arrays offer rapid recovery capabilities to get your business back up and running as quickly as possible. No ransom needs to be paid since you have control over your data instead of the intruder.

Added Benefits, Zero Cost

Identifying patterns, making security decisions, and deploying responses to threats to your business are the cost of doing business in the hyper-connected world. LogRhythm and Pure have teamed up to secure your data with improved threat detection, automated response resolutions, and orchestrated recovery to simplify your security story. The best part is that it's free. No long and required materials to read, understand, and master, no lengthy deployments, and simple goodness to your business.

Integration Closes Gaps and Reduces Cost

The power of Pure Storage and LogRhythm combined simplify the deployment of world class storage and SIEM platform to close the gaps in security coverage and ease operational burden. Shining a light across your entire workload minimizes places for an attacker to hide without a deep investment in staff training and knowledge—reducing the total cost of the solution while raising the bar for an attack.



Additional Resources

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

©2023 Pure Storage, Inc. All rights reserved. Pure Storage, the P logo mark, and SafeMode are trademarks or registered trademarks of Pure Storage, Inc. All other names may be trademarks of their respective owners.

PS2528-01-en 11/23