SOLUTION BRIEF

# IBM QRadar SIEM and Pure Storage Solution Brief

Enhance threat detection and reduce response time.

Data storage, including on-premises flash array appliances, remains a primary target for cyberattacks due to the value of the data held within these systems. Ransomware attacks in particular often target on-premises storage environments. It is essential to have a security solution that is automated and simple to set up, ensuring that critical data is protected against real-time threat from rogue employees, and hackers.

## Solution Overview

IBM QRadar and Pure Storage® have teamed up to deliver event ingestion from Pure Storage FlashArray™ systems to capture crucial information and faster responses to the events.

To protect your data, Pure Storage offers SafeMode™ Snapshots, immutable snapshots used to protect your critical data. SafeMode snapshots are read-only snapshots that cannot be altered, encrypted, or deleted by ransomware. They provide a virtual air gap that is automated and simple to set up, ensuring that critical data is protected against accidental deletions, rogue employees, or hackers. SafeMode Snapshots are easy to enable and can be integrated with a variety of data protection solutions from Commvault, Rubrik, Veeam, and Veritas. They offer customizable snapshot cadence and eradication scheduling, rapid restore capabilities, and investment protection. SafeMode Snapshots are included with FlashBlade® and FlashArray at no extra charge, and Pure Storage subscription or maintenance support contracts cover enhancements.

## FlashArray Event Collection

Collecting events from a FlashArray system is crucial for monitoring system health, detecting potential issues, and ensuring compliance with security requirements. Event ingestion from Pure Storage FlashArray involves the direct collection and storage of events from the FlashArray for analysis, monitoring, and security purposes. Pure Storage collaboration with IBM QRadar enables direct events singestion from FlashArray, shortening the time to event identification and enhancing threat detection and response capabilities. This integration allows organizations to streamline the process of collecting and analyzing events from their FlashArray appliances, ultimately strengthening their security posture and enabling more efficient incident response.

### Automate Snapshots

Gain cyber resilience for quick data restoration and maintain operational continuity.

### Streamline Security

Simplify security deployment strategies for on-premises FlashArray appliances with Universal Cloud REST API.

### Speed Event Detection

Capture security information with event log ingestion from FlashArray to enable faster detection of events.

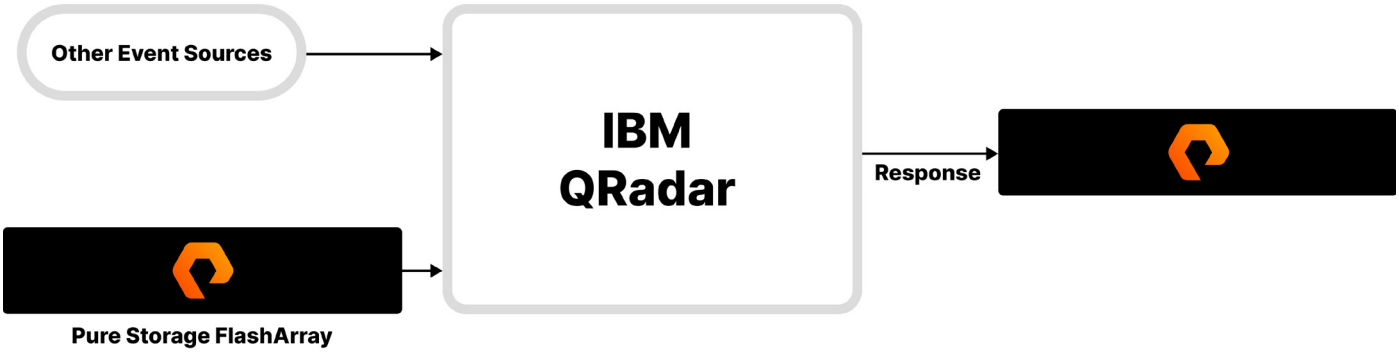


**FIGURE 1** IBM QRadar and Pure Storage Solution

## Universal Cloud REST API

The Universal Cloud REST API protocol is an outbound, active protocol for IBM QRadar. It allows you to customize the Universal Cloud REST API protocol to collect events from various REST APIs, including data sources that do not have a specific DSM or protocol.

The Universal Cloud REST API protocol behavior is defined by Workflow XML document and Workflow Parameter Values XML which contains the parameter values used directly by the workflow.

You can access the Workflow and Workflow Parameter XMLs for Pure Storage FlashArray on GitHub.

## IBM QRadar Action Script for Pure Storage FlashArray

With IBM QRadar, administrators can invoke a custom script and pass data to a script based on a rule response. IBM QRadar allows custom actions to select or define the value that is passed to the custom script to run the resulting action. For example, if malicious activity is detected on a FlashArray, an alarm can be raised, and a snapshot of the appropriate protection groups or volumes on the FlashArray can be taken. Other example actions and their use cases are provided in the following table.

| 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 snapshots | 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 local user | Removes a local user from FlashArray | A user account has been compromised and is trying to dump or delete critical data. |

**TABLE 1** Use case scenarios

For more information on Custom Scripts, refer to the PureStorage-OpenConnect/qradar-security-solutions Github.

## About Pure Storage FlashArray

Designed to be as easy to use as it is powerful, Pure Storage® FlashArray™ provides unified block and file storage with enterprise performance, reliability, and availability to power your critical business services. The all-NVMe architecture used in FlashArray storage provides the performance density that allows you to consolidate more business services—bigger databases, more applications, more users—on fewer arrays. The always-on quality of service (QoS) in Purity prevents workloads from hogging resources without setting artificial limits, so you're assured full performance of all your workloads. Consolidating workloads not only simplifies operations and decreases rack space requirements, but it also reduces power consumption and cooling costs to help you meet corporate green data center standards.

## About IBM QRadar SIEM

IBM QRadar is one of the most popular SIEM solutions in the market today. It helps users quickly uncover existing and potential threats through its advanced analytics capabilities. It provides many features, such as centralized visibility, flexible deployment, automated intelligence, machine learning, proactive threat hunting, and much more. QRadar uses a combination of flow-based network knowledge, security event correlation, and asset-based vulnerability assessment.

## About Pure Storage

Pure Storage uncomplicates data storage, forever. Pure 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. Our 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. We believe 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, our ever-expanding list of customers is among the happiest in the world.

## Additional Resources

- Security made easy with QRadar SIEM.
- Discover Pure Storage data protection solutions.
- Learn how SafeMode secures data from ransomware attacks.





PS2626-01-en 06/24