SOLUTION BRIEF

Pure Storage and IBM QRadar

Enhance threat detection and reduce response time.

Data storage systems, including on-premises Pure Storage® FlashArray™ and FlashBlade® appliances, are 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 threats from rogue employees, and hackers.

Solution Overview

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

To safeguard your critical data, Pure Storage offers SafeMode™ Snapshots—immutable, read-only snapshots that provide robust protection against ransomware and unauthorized manipulation. These snapshots are impervious to alteration, encryption, or deletion, ensuring data integrity even in the face of cyber threats.

Enhancing this robust data protection, the integration of Pure Storage FlashArray and FlashBlade with IBM QRadar elevates security by delivering enhanced visibility into storage environments. By leveraging QRadar's advanced SIEM capabilities, organizations gain real-time insights into potential threats through sophisticated log aggregation, event correlation, and comprehensive threat detection. The inclusion of automated response actions based on threat severity, enabling faster incident mitigation and strengthening the resilience of storage infrastructures—ultimately bolstering defenses against the ever-evolving landscape of cyber threats.

Automate Snapshots

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

Streamline Security

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

Speed Event Detection

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

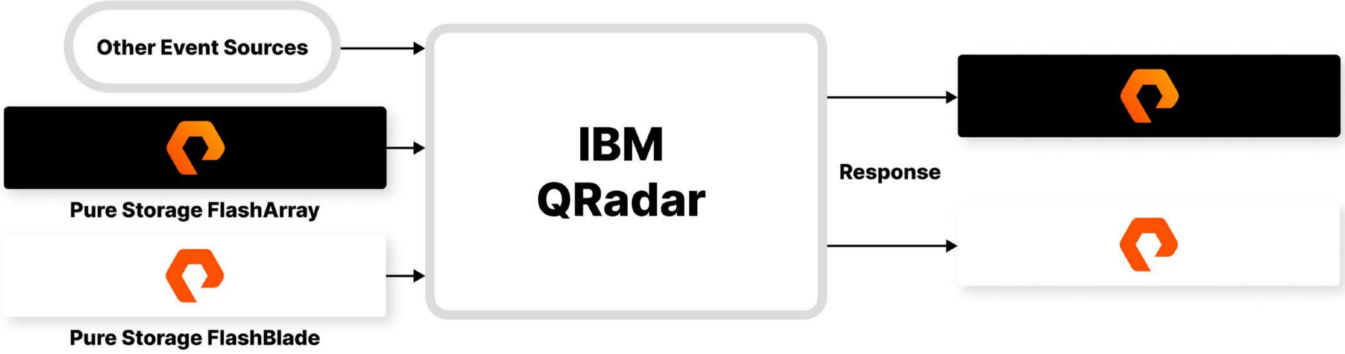

FIGURE 1 IBM QRadar and Pure Storage Solution

FlashArray and FlashBlade Event Collection

Collecting events from FlashArray and FlashBlade systems is crucial for monitoring system health, detecting potential issues, and ensuring compliance with security requirements. Event ingestion from Pure Storage FlashArray and FlashBlade involves the extraction of events through a pull mechanism, which are then ingested into IBM QRadar for comprehensive analysis, monitoring, and security. The collaboration between Pure Storage and IBM QRadar streamlines this process, reducing the time to identify events and significantly enhancing threat detection and response capabilities.

This integration allows organizations to streamline the process of collecting and analyzing events from their FlashArray and FlashBlade appliances, ultimately strengthening their security posture and enabling more efficient incident response.

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 and FlashBlade on GitHub.

IBM QRadar Action Script for Pure Storage FlashArray and FlashBlade

With IBM QRadar, administrators have the ability to invoke custom scripts and pass specific data based on rule responses. QRadar allows for flexible customization by enabling the selection or definition of values to be passed to these scripts, facilitating tailored actions in response to security events.

Once event mapping is established for incoming alerts, administrators can create custom rules to define the actions taken on critical events within QRadar. These rules not only trigger specific actions, but they also ensure that detected events are categorized as part of an offense when necessary. By configuring event rules or flow rules, actions can be initiated based on specific parameters, with these rules linked to custom scripts that execute predefined tasks, further automating responses to security incidents.

When a potential threat is detected, IBM QRadar parses and maps the event or alert, triggering the corresponding custom rule. This triggers a custom script that ensures timely and accurate responses, tailored to the event type and predefined rule sets..

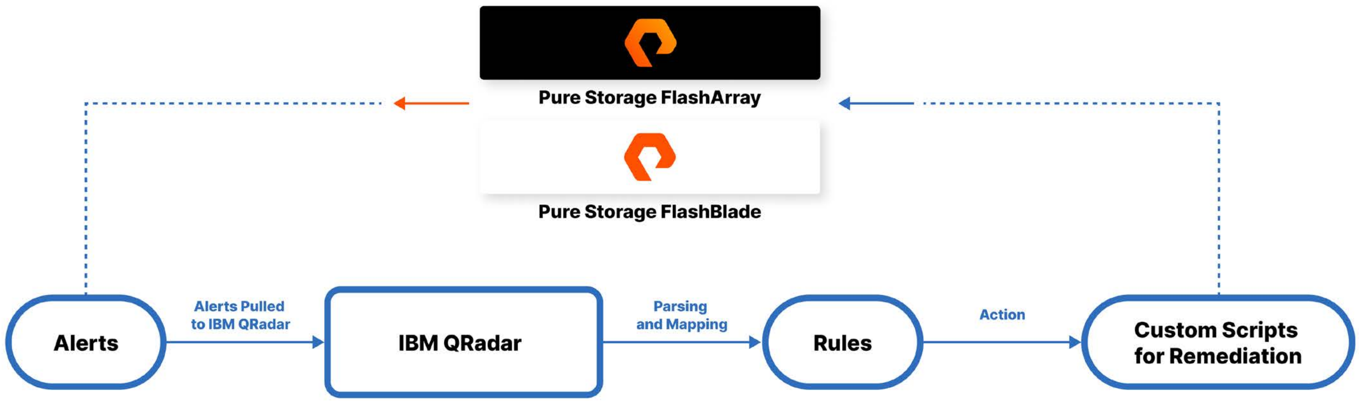

FIGURE 2 IBM Qradar threat response

For instance, if malicious activity is detected on a FlashArray or FlashBlade, an alarm can be triggered, and a snapshot of the relevant protection groups or volumes on the FlashArray, or the appropriate filesystems on the FlashBlade, can be captured. Other example actions and their use cases are provided in the following table.

Target	Action	Description	Use Case
FlashArray	Take protection group snapshot	Creates a snapshot of all volumes within a protection group	An attack is detected and a SafeMode Protected snapshot is taken to secure critical data.
	Take volume snapshots	Creates a snapshot of the volume.	An attack is detected and a SafeMode Protected snapshot is taken to secure critical data. Note: Volume level snapshots are only protected by SafeMode if SafeMode is enabled array-wide.
	Remove local user	Removes a local user from FlashArray.	A user account has been compromised and is trying to dump or delete critical data.
FlashBlade	Take File System snapshots	Creates snapshots of one or multiple file systems on FlashBlade.	An attack is detected and a file system snapshot is taken to secure 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 and FlashBlade

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.

Pure Storage FlashBlade offers unified file and object storage with unmatched scalability, performance, and simplicity for modern data workloads. The high-performance, massively parallel architecture of FlashBlade enables rapid data access and processing, making it ideal for a wide range of applications, including analytics, artificial intelligence, machine learning, and rapid restore environments. The system's elasticity allows you to scale out by simply adding more blades, ensuring that your storage infrastructure grows seamlessly with your data demands. The integrated quality of service (QoS) in a FlashBlade system ensures consistent performance across all workloads without the need for manual tuning. By consolidating diverse workloads on FlashBlade, organizations can simplify operations, reduce data silos, and accelerate time to insight.

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.