

## SOLUTION BRIEF

# Gain Infrastructure Visibility with Pure Storage and Microsoft Sentinel

Unparalleled data storage protection through seamless integration

Data storage systems housing sensitive information face constant threats due to the valuable data they contain. Earlier this year, the [SANS Institute reported](#) an approximate 73% increase in ransomware cases from 2022 to 2023. Delay in detection provides attackers with a substantial window to exfiltrate data or deploy ransomware, jeopardizing business continuity and resulting in significant financial losses. Rapid attack detection remains essential; however, ensuring swift and automated response mechanisms is equally crucial. Attackers specifically target these vulnerable periods to maximize disruption before effective responses can be implemented.

## Solution Overview

Pure Storage® has partnered with [Microsoft Sentinel and their cloud-native SIEM Solution](#) to provide advanced visibility into storage infrastructure. This partnership utilizes cloud-native SIEM (security information and event management) and SOAR (security orchestration, automation, and response) services. This collaboration empowers the collection and correlation of security data from storage components, delivering a unified solution for threat detection and rapid response. This integrated approach ensures an enhanced security posture and streamlined management, bolstering your defenses against evolving cyber threats across your infrastructure.

## FlashArray and FlashBlade Log Collection

Syslog alerts produced by the Pure Storage FlashArray™ and FlashBlade® appliances are analyzed to identify potential attack indicators. Changes in software configuration, network settings, and both successful or unsuccessful administrator logins may indicate benign activities or more malicious actions.

Several preparatory steps are necessary before initiating log ingestion into the Microsoft Sentinel workspace. These include configuring the syslog server, adding the server details to the FlashArray and FlashBlade systems, and installing the Azure Monitor Agent on the syslog server. This process entails onboarding the machine to Azure as an Arc-managed device, creating data collection rules (DCRs), and installing the Azure Monitoring Agent (AMA).



### Empowered Security

Gain advanced visibility into storage infrastructure. This partnership utilizes cloud-native SIEM.



### Proactive Mitigation

Seamless integration of Microsoft Sentinel's SmartResponse and Pure Storage FlashArray.



### Peace of Mind

Automated workflows activate in response to alerts or incidents.



## Use Case Scenarios

The following table lists common use case scenarios.

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

## About the Microsoft Sentinel Cloud-native SIEM Solution

Microsoft Sentinel is a cloud-native SIEM platform designed to swiftly identify both existing and potential threats. Leveraging its advanced analytics capabilities, Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. Offering a comprehensive solution, it enables attack detection, threat visibility, proactive hunting, and effective threat response, all within a single platform.

## About Pure Storage

Pure Storage offers a cloud experience that empowers every organization to maximize their data's potential while minimizing the complexity and cost of managing the underlying infrastructure. Our commitment to providing true storage as-a-service enables customers to adapt to evolving data needs rapidly and efficiently, whether deploying traditional workloads, modern applications, containers, or more.

We believe we can significantly reduce data center emissions worldwide through our environmental sustainability initiatives, which include designing products and solutions that help customers decrease their carbon and energy footprint. With a certified customer satisfaction score in the top one percent of B2B companies, our continuously growing list of customers ranks among the most satisfied in the world.

## Additional Resources

- Cloud-native SIEM solution with [Microsoft Sentinel](#)
- Pure Storage and Microsoft Sentinel Solution on the Azure [marketplace](#).
- Discover Pure Storage [data protection solutions](#)
- Learn how [SafeMode](#) secures data from ransomware attacks

