PURESTORAGE® VARONIS

SOLUTION BRIEF

Secure Critical Storage with Varonis and Pure Storage

Gain deep visibility of critical storage for the detection and remediation of data risks

As organizations struggle with massive data volumes and increasingly sophisticated attacks—ranging from ransomware to insider threats—traditional systems often fail to provide the necessary speed, security, and visibility to keep pace with the threat landscape. Threat actors seek to steal data and then destroy it to facilitate extortion and fraud. These incidents disrupt operations and threaten revenue goals, investor expectations, customer loyalty and regulatory compliance.

Challenges of Data Security and Resilience

Organizations face critical challenges in data security and resilience. They must identify sensitive data, enforce secure permissions, and detect abnormal access that may indicate exfiltration. Equally essential is robust cyber recovery to understand cyberattack impacts, protect critical data stores from destruction, and defend production and backup data from targeted exfiltration. These challenges demand integrated strategies with comprehensive visibility, strict access controls, and rapid recovery capabilities to maintain business continuity in an increasingly hostile digital landscape.

Pure Storage and Varonis Deliver on Data Security and Resilience

Together, Pure Storage® and Varonis provide the capabilities to resist and recover from destructive incidents. Pure Storage offers high-performance, immutable storage that guarantees rapid recovery and data integrity, while Varonis delivers data discovery and classification, automated remediation, advanced user behavior analytics, and threat detection. Together, they provide a unified defense that secures critical data, minimizes risk, and ensures data resilience to support business continuity.

The Pure Storage platform, featuring FlashArray™ systems, meets diverse requirements with unified block and file services running on a single storage pool. It consolidates disparate workloads, provides high-performance, scales to petabyte levels in an ultra-dense footprint, and offers advanced data reduction with intelligent deduplication and compression, effectively replacing legacy disk-based storage. Non-disruptive hardware upgrades allow seamless scaling or transitioning to more powerful systems without data migration or downtime.

Accelerate Cyber Resilience and Data Security

Gain high-performance storage built for modern workloads, allowing businesses to operate with speed, agility, and efficiency.

Unmatched UEBA and Data Risk Remediation

Automated remediation to detect and contain cyberattacks and insider threats with advanced user and entity behavior analytics.

Optimized Performance and Security for Critical Data Storage

Gain unmatched efficiency, security, and simplicity to ensure the security and resilience of critical data storage.

Varonis' Data Security Platform prevents data breaches by automatically discovering and classifying sensitive data, detecting threats, and remediating data risk and exposure. The platform maps data sensitivity to permissions and activity to provide deep visibility into risk and exposure. Automated remediations address issues like high-risk permissions and mislabeled files to reduce the blast radius. User behavioral analytics detects active threats and malicious insiders.

Solution Overview

The Pure Storage and Varonis integration allows for enhanced data security by enabling Varonis to directly access and analyze activity logs and data stored on Pure Storage arrays, providing detailed insights into user access patterns and potential security risks within the storage infrastructure, effectively detecting suspicious activity and potential data breaches on the Pure Storage platform.

Varonis leverages Pure Storage APIs to access data and metadata from storage arrays, enabling real-time analysis of file access patterns and user activity. It can directly query these arrays to gather comprehensive information on file access, user permissions, and data classification, which allows for automated remediation and threat detection. By analyzing access patterns and anomalies, Varonis identifies potential security threats, such as insider threats, unauthorized access, and malicious activity occurring within the Pure Storage environment.

Pure Storage and Varonis users benefit with enhanced visibility into data access and behavior on Pure Storage, enabling proactive measures to prevent data breaches. The integration provides streamlined data analysis and threat detection across the storage infrastructure, reducing investigation time and improving security response. Varonis helps improve cyber resilience with the early detection of potential security issues on Pure Storage systems, minimizing the impact of data breaches and ransomware attacks.

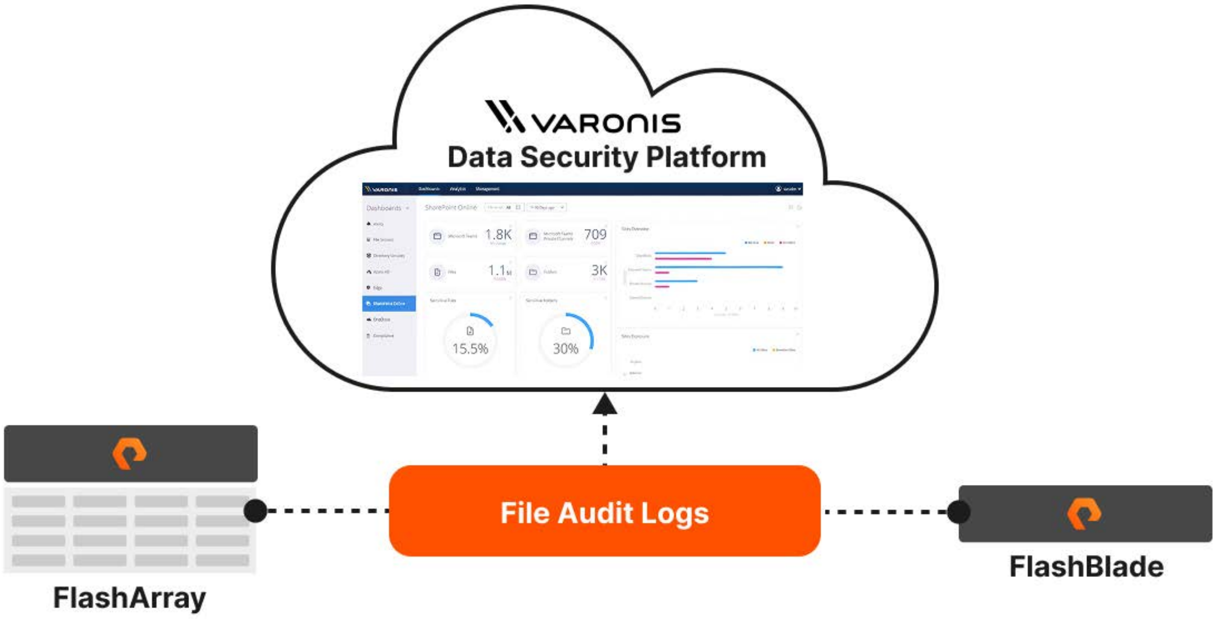

FIGURE 1 Pure Storage and Varonis integrated solution architecture

Critical Capabilities

Pure Storage and Varonis provide market-leading capabilities to help organizations improve performance and security for their file-based backup data.

Scalable and performant storage architecture from Pure Storage:

- Unified storage platform that consolidates block and file workloads into a single storage pool, eliminating data silos
- Eliminates the need to add new arrays or management
- Interfaces and scales with evolving applications that support artificial intelligence and machine learning
- Ultra-low latency performance (150µs to 1ms) for rapid data access
- High availability (99.99999%) with built-in business continuity and disaster recovery features to ensure data resiliency
- Advanced data reduction through intelligent deduplication and compression
- Simplified management through an intuitive, user-friendly interface

Data security and intelligence from the Varonis Data Security Platform:

- Data discovery and classification of sensitive data with 99% accuracy
- Permission and activity mapping to pinpoint where data is overexposed or at risk
- Automated remediation to right-size access, remove stale users, fix exposure, and reduce the blast radius
- Capturing critical events like when a file was created vs. modified to create a comprehensive audit trail for investigations and recovery
- Leverages behavioral analytics to detect suspicious activity, such as users accessing an unusual number of records, escalating privileges, or encryption of multiple files

For more information, see our Cyber Resilience Solutions page.

Additional Resources

- Explore Pure Storage Cyber Resilience
- Learn more about Pure Storage Technology Alliance Partners
- Learn about "How Organizations Are Defending against Evolving Ransomware Threats"

purestorage.com

800.379.PURE