SOLUTION BRIEF

Data and Cybersecurity Capabilities from Pure Storage

Increase your cyber resilience with AI-driven security to prevent, detect, and remediate threats.

Secure, cyber-resilient solutions from Pure Storage® offer comprehensive protection, detection, remediation, and rapid restoration, safeguarding critical data against advanced cyberattacks, providing additional security and protection over traditional defenses. Customers gain an unshakeable foundation for data security, ensuring data availability and integrity, allowing organizations to confidently face evolving threats and minimize destruction disruptions of their operations.

Critical Challenges to Securing Cyber-resilient Storage

Organizations face a multifaceted array of challenges in securing their storage infrastructure and ensuring cyber resilience, including:

- **Identity and access management complexity**: Managing user identities, roles, and access permissions across diverse storage environments can be cumbersome and prone to errors. Inadequate identity and access management (IAM) often leads to over-privileged accounts, creating easy entry points for malicious actors or insider threats.
- **Data sovereignty and compliance**: Strict regulatory requirements (e.g., DORA) and increasing demands for data sovereignty necessitate granular control over encryption keys and data residency, adding layers of complexity to security operations.
- **Platform integrity risks**: Ensuring that storage platforms only run authorized, untampered software is crucial. Malicious bootloaders or unauthorized software can compromise the entire infrastructure, leading to data breaches or system failures.
- **Delayed threat detection and remediation**: Many security systems lack real-time visibility into storage operations, leading to significant delays in detecting anomalies or active attacks. Slow detection translates directly to increased data loss and recovery costs.

Accelerated Incident Response

Minimize potential damage with real-time threat detection, automated remediation, and instant alerts.

Proactive Risk Reduction

Gain actionable guidance for quicker resolution of risks and a stronger overall security posture.

Enhanced Security Visibility

A holistic view of user behavior and access patterns allows security teams to efficiently investigate and address insider threats and anomalies.

- **Inefficient incident response and recovery**: Recovering from a major cyber incident, especially ransomware, is often a chaotic, time-consuming, and resource-intensive process. Manual recovery efforts can lead to prolonged downtime, significant data loss, and immense operational stress.
- **Visibility gaps**: A lack of unified visibility across file operations, user behavior, and security events makes it challenging for SecOps teams to identify emerging threats or investigate insider activity effectively.

Advanced AI Security to Meet These Challenges

Cyber-resilient storage from Pure Storage directly addresses these challenges by embedding security deep within the storage architecture with:

- **Built-in Security:** By integrating zero-trust principles, including multi-factor authentication (MFA) and role-based access control (RBAC), Pure Storage ensures that only authenticated and authorized users and processes can access data. This continuous verification model eliminates implicit trust, significantly reducing the attack surface. Native identity and access management (IAM) capabilities, including robust single sign-on (SSO) support for both authentication and authorization, streamline user management and boost overall security by ensuring only authorized users and groups can access the system. Furthermore, support for customer-provided encryption keys (Bring Your Own Key) offers maximum data sovereignty and compliance, empowering organizations to maintain unique security postures tailored to their specific regulatory and data residency requirements. At the foundational level, trusted platform module (TPM) and UEFI Secure Boot guarantee platform integrity, preventing unauthorized bootloaders and ensuring that only software signed by Pure Storage runs, thereby protecting the environment from malicious and unauthorized software.
- **Connected detection**: Pure Storage leverages continuous, real-time threat evaluation and automated response mechanisms through native capabilities and deep integrations, such as with Superna, Varonis, and CrowdStrike. This powerful combination enables the automatic detection and immediate remediation of malicious activity affecting VM-based applications and critical data within the storage environment. Upon detection, the system can automatically update security policies, replicate and isolate critical systems to contain threats, and trigger instant alerts to notify response teams for swift review and action.

Real-time malware scanning and detection leveraging ICAP, achieved by integrating with leading endpoint security platforms, provides next-gen antivirus (AV) capabilities for file workloads. This integration identifies malicious malware, allows for the quarantine and deletion of infected files, enables granular control over administrative access, and permits the configuration of policies directly at the file workload level. Additionally, the Security Assessment 2.0, powered by the Pure Storage AI Copilot, provides quick identification of security risks, offering actionable guidance for anomaly alerts and facilitates faster resolution of vulnerabilities, including critical CVEs.

For simplified investigation and threat hunting, the Pure1® Log Center provides a centralized and secure integration point within the broader security ecosystem. It seamlessly consumes detailed file audit logs, offering a holistic view of access management and user behavior across the Pure Storage platform. This comprehensive logging capability eliminates the need for customers to rely on disparate third-party tools to piece together a complete security picture. The rich insights provided by the Log Center significantly simplify threat hunting activities, enabling security operations (SecOps) teams to efficiently investigate potential insider threats and anomalous user access patterns, thereby accelerating incident response and reducing the time to resolution.

Key Security Capabilities

Pure Storage solutions include critical security capabilities, including:

- **Zero-trust security**: MFA, RBAC, native IAM, SSO, and granular access roles
- **Data sovereignty**: Customer-provided encryption keys (BYOK) for compliance
- **Platform integrity**: TPM and UEFI Secure Boot ensure authorized software
- **Real-time threat detection**: Continuous monitoring, anomaly detection and integrations to leading SecOps platforms
- **AI-powered guidance**: Pure Storage AI Copilot for security posture and vulnerability remediation
- **Integrated malware scanning**: Next-gen AV for file workloads, quarantine, and deletion
- **Centralized logging**: Pure1 Log Center for holistic access and behavior insights
- **Automated recovery zones**: Isolated, virtualized environments for de-contamination and restoration

Additional Resources

- Learn more about Pure Storage SIEM Integrations.
- Read about how Pure Storage protects your critical data resources in our Security and Assurance Packet.
- Explore how to optimize your security analytics.

ID5815-01-en-12/25