SOLUTION BRIEF

Layered Resilience

Automated Cyber Recovery Regardless of Incident Severity

Ensuring data integrity and availability for cyber resilience is challenging due to evolving threats like ransomware and insider attacks. Organizations need strong immutability, encryption, and access controls while balancing security with efficiency. Traditional storage and backups may be vulnerable if not properly isolated, making modern layered resilience essential.

Maintaining availability requires resilient infrastructure for rapid recovery and minimal downtime. Automation is critical to layered resilience because it ensures rapid, consistent responses across all recovery layers during a cyber incident. Legacy storage often creates bottlenecks, with performance and availability constraints that inhibit the rapid provisioning needed to support instant recovery and clean rooms and staging environments, also known as secure isolated recovery environments (SIREs). Compliance and service level agreements demand uptime and fast restoration. Businesses must adopt cyber-resilient storage with immutable snapshots, real-time monitoring, and rapid recovery to safeguard data.

Cyber Resilience Foundation of Secure and Layered Storage

An automated and layered storage environment is essential for cyber resilience—integrating advanced security, visibility, immutability, and high availability. Immutable snapshots protect against ransomware and accidental deletion, while secure, high-performance data copies across on-premises, offsite, and cloud locations ensure availability during any incident. Automation and orchestration reduce human error, speed response, and streamline recovery to restore critical applications and data when it matters most.

Minimize Recovery Time Objective

Immediate recovery with storage layer snapshots.

Ensure Data Availability

Data survives no matter the severity of the incident with geographic isolation.

Ensure Data Integrity

Prevent data tampering with advanced security and indelible and immutable data.

1. **Automation**: Policy-driven automation yields unified layered resilience management and administration through a single interface, simplifying operations across all storage layers. By leveraging SafeMode™ Snapshots and Enterprise Data Cloud, data is protected with immutable, indelible copies that defend against ransomware and accidental deletion. In the event of an incident, rapid and reliable recovery capabilities help quickly identify clean recovery points and rapidly restore application environments to minimize downtime and ensure business continuity.
2. **Security and visibility for integrity**: Security and visibility are essential for critical storage to control access, detect threats, prevent data breaches, and ensure resilience against cyberattacks. Zero trust principles provide strong control of data and platform access. With real-time insights on threats and your storage security posture, you can detect threats and vulnerabilities to prevent threat actors from tampering with data or disabling protection settings.
3. **Resilience for data availability**: Organizations need resilient and high-performance storage to ensure data availability, integrity, and rapid recovery in the face of cyber threats, system failures, or disasters. Resilient storage ensures there is no single point of failure for threat actors to exploit, reducing vulnerability to catastrophic events. By leveraging advanced data replication capabilities, organizations can ensure that their critical data will survive even if a data center is completely disabled or destroyed.

Layered Resilience

Layered resilience is the automated and strategic use of primary, secondary, and tertiary storage methods—such as snapshots, replication, backup and recovery, and cloud vaulting—to ensure continuous data availability and protection against disasters or cyberattacks, even if one or more layers fail.

Layered resilience is built on a **foundation of data security and visibility.** This ensures you manage your storage attack surface, implement strong data security safeguards, and monitor and secure your data against threats. Visibility leverages zero trust principles, immutable and indelible data, and tight coupling between data storage and security analytics and operations.

Pure Storage® provides **layered resilience** with a combination of immutable and indelible data snapshots, data replication, streaming data protection, and disaster recovery as a service (DRaaS) to ensure data availability to restore applications and services in the event of any cyber threat. This provides the power and performance to recover quickly from simple outages to even the most complex and destructive cyberattacks.

Immutable and indelible snapshots provide the backbone for layered resilience. The snapshots, which provide a mirror of production systems, are leveraged to rapidly restore data and virtual machines (with almost zero latency) to secondary infrastructure during disasters or system failures, or to a SIRE in the event of malicious incidents such as ransomware or insider attacks. Security is key for immutable and indelible snapshots. Once created, the snapshots cannot be deleted without undergoing a stringent, multi-step verification process. This includes interaction with the Pure Storage dedicated support team, adding an extra layer of security.

The layered resilience stack provides a unique combination of capabilities to ensure your data is available regardless of the severity of a disaster or cyberattack. Figure 1 represents a full implementation of layered resilience.

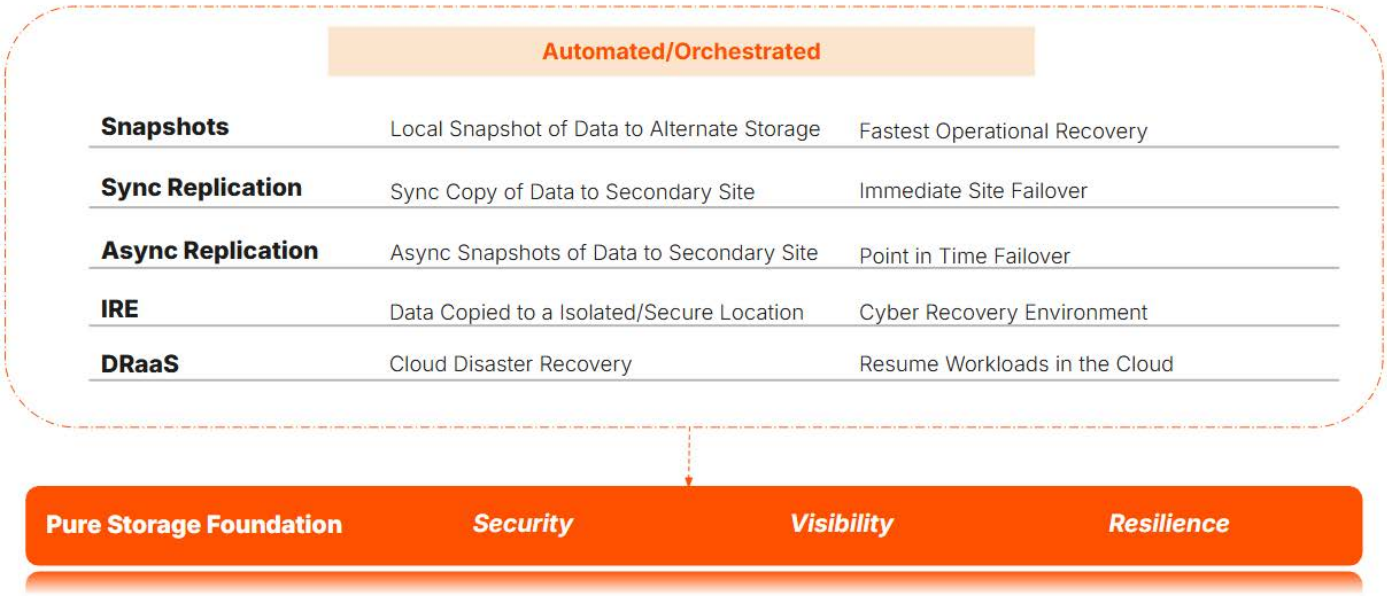

FIGURE 1 Layered resilience implementation

Critical Capabilities

Pure Storage market-leading capabilities and integrations help organizations quickly recover from cyberattacks and disasters and support the detection of and response to threats targeting the platform with:

Pure Protect®

- Automate the provisioning of a recovery virtual private cloud and the orchestration of failovers, with compatibility across any storage.
- Enhance your data resilience with offsite copies in Amazon Web Services (AWS), enabling orchestrated recovery and supporting a bring-your-own AWS model.
- Make life easy with simplified setup without the need for extensive AWS expertise.

Pure Storage platform

Secure, scalable, and performant for a cyber resilience storage foundation

- Help prevent ransomware attacks with immutable and indelible SafeMode Snapshots, zero trust security principles, and anomaly detection.
- Consolidate block and file workloads, eliminating data silos by dynamically provisioning recovery workloads.
- Gain ultra-low latency performance (150µs to 1ms) for rapid data access with high availability (99.99999%).

Pure1®

Understand and manage cyber resilience readiness

- Use data protection and security assessments to evaluate system health, security posture, and performance.
- Monitor in real time and optimize capacity performance with dashboards and predictive analytics.
- Gain actionable insights and seamless integration with recovery and security services.

Pure Storage cybersecurity integrations

- Integrate with security information and event management (SIEM), user and entity behavior analytics (UEBA), and extended detection and response (XDR) solutions to provide real-time visibility for storage threats.
- Enhance performance and scalability for on-premises SIEM, UEBA, and XDR.

Pure Storage data protection integrations

- Get performance and scalability for leading data protection solutions, ensuring faster backups and rapid recovery.
- Work with solutions from top data protection vendors like Rubrik, Commvault, and Veeam to provide end-to-end data resilience.

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 how organizations are defending against evolving ransomware threats.

ID1921-01-en-07/25