WHITE PAPER

10 Best Practices for Storage Cyber Resilience

Storage as a foundation for cybersecurity and recovery

Executive Summary

Cyberattacks are evolving rapidly. What were once isolated incidents are now common, coordinated, persistent campaigns designed to disable, encrypt, and extort. And today's threats go beyond stealing your data; they can now cripple your recovery. Once your recovery data is gone, paying ransom is often the only option to avoid a catastrophic disruption to your operations.

Cyber resilience strategies must now extend from traditional backup to layered, operationally-ready recovery. Read on to learn 10 field-proven best practices for secure, cyber-resilient storage, derived from real-world customer experiences and aligned to Pure Storage cyber-resilient architecture. These guidelines go beyond traditional data protection; they deliver intelligent visibility, rapid recovery, and operational confidence in the face of modern cyberthreats.

Contents

1 Deploy High-performance, Secure, Resilient Storage

Best Practice

Cyber resilience isn't just about preventing attacks; it's about ensuring recovery is always possible—no matter how sophisticated or destructive the threat. Pure Storage defines cyber resilience through solutions that align your storage platform, data protection stack, and security operations into a unified defense and recovery model. And every second matters. With a foundation of high-performance flash storage, it accelerates threat detection and recovery, minimizing downtime during cyberattacks.

These three solutions are:

1. **Native performance and resilience capabilities:** Resilience begins with the storage platform itself. It must be built to resist tampering, enforce protection, and retain recovery points even under credential compromise. Immutability, indelibility, and access control are critical at this layer. Your storage should protect itself.
2. **Integration with backup and recovery partners:** Backup and disaster recovery platforms extend protection across your environment. Integrations with trusted vendors like Commvault, Rubrik, and Veeam help organizations deploy a modern 3-2-1 strategy for data protection. The performance and resilience of these solutions can be amplified by all-flash performance and native storage resilience capabilities, such as snapshots and replications. These best-of-breed partner integrations also provide policy-based orchestration, snapshot offload, cataloging, threat hunting, and SLA-aligned restore. This ensures you can scale protection and recovery across hybrid infrastructures.
3. **Threat detection and response integration:** Your storage platform can provide amplified performance and resilience for security analytics on premises. Storage is no longer just infrastructure. It's an active component to ensure the speed and availability of critical threat detection, response, and investigation.

Together, these solutions create a complete cyber resilience strategy that supports operational recovery, response coordination, and compliance—even under active attack.

Why It Matters

Modern ransomware doesn't just encrypt data; it disables your ability to recover. Threat actors delete snapshots, corrupt backups, and sabotage recovery metadata. Without a layered model, you're left with one shot at recovery, and that's rarely enough.

A three-layer architecture ensures:

- **Built-in protection** that survives system compromise
- **Partner-based orchestration** that spans your full data estate
- **Security integration** that aligns storage with incident response

It also enables collaboration between IT, backup, and security teams. Each working within their tools, but aligned to a shared goal—resilient recovery.

The Pure Storage Advantage

Pure Storage delivers a three-layer architecture in an integrated platform:

Layer 1: Native security and resilience capabilities

- SafeMode™ Snapshots which are immutable and undeletable, aka indelible—even by admins
- Synchronous and asynchronous replication
- Cloud DRaaS via Pure Protect™
- Built-in, AI-based anomaly detection
- Disaster recovery as a service and cyber recovery SLAs
- Role-based access control (RBAC), access management (IAM) SAML single sign-on (SSO), multi-factor authentication (MFA), secure multi-tenancy, and secure firmware pipelines
- Enforced snapshot retention with eradication delay (up to 400 days)
- Data confidentiality and integrity is ensured with FIPS 140-2 encryption for data at rest, and TLS 1.3 for data in transit

Layer 2: Integration with data protection backup partners

- Native snapshot orchestration with Veeam, Commvault, and Rubrik
- SLA-based recovery policies and hybrid backup workflows
- FlashBlade® and FlashArray™ as high-speed all-flash backup/restore targets
- Seamless offload and recovery from snapshot-based backups

Layer 3: Integration with SecOps

- Log streaming to CrowdStrike LogScale, Rubrik Security Cloud, Splunk, Superna,, QRadar, Elastic, and others
- Snapshot creation and rollback triggered via incident response SOAR playbooks
- API integration with XDR platforms for investigation and containment
- Pure1® for shared security visibility and configuration monitoring

With Pure Storage, layered cyber resilience is practical, adaptable, effective, and ready for real-world recovery—not just theoretical design.

2 Enforce Immutable and Indelible Data Protection

Best Practice

One of the first things a sophisticated ransomware attacker will try to do is delete your snapshots, wipe your backup indexes, and disable your protection policies. Immutability isn't enough. You need indelibility—the ability to guarantee that protected recovery points cannot be deleted, even by someone with administrator credentials.

How you can ensure indelibility:

- Implement snapshot retention policies that prevent deletion until scheduled expiration.
- Protect not just snapshots, but also backup metadata, indexes, and schedules.
- Use out-of-band, multi-party administrative approval for any changes to critical data protection settings.
- Apply these policies across production, backup, and disaster recovery environments.
- Maintain audit logs to prove retention and tamper resistance.

Indelibility should not be optional. It must be embedded in your data protection strategy and enforced at the platform level.

Why It Matters

Attackers frequently don't encrypt data until they've disabled recovery capabilities. If your snapshots and backup catalogs are vulnerable to deletion—accidental or malicious—your entire recovery plan is undermined.

Indelibility ensures:

- A guaranteed rollback point that cannot be tampered with or destroyed
- Support for legal holds, regulatory audits, and evidence preservation
- Protection against insider threats and external threat actors compromise
- Confidence that even if you're breached, you can still recover

Without it, even the most sophisticated snapshot and backup strategy can be silently erased before you know there's an attack.

The Pure Storage Advantage

Pure Storage SafeMode™ technology enforces indelible protection that goes beyond traditional immutability:

SafeMode Snapshots

- Cannot be deleted—even by storage administrators
- Protected by a built-in eradication delay (up to 400 days)
- Configured and modified only through a multi-party, out-of-band approval process involving Pure Support

Indelible metadata protection

- Snapshot schedules, backup indexes, and policy configurations are all protected
- Prevents attackers from sabotaging future recovery options

Secure configuration and access control

- MFA and RBAC prevent unauthorized access
- Full audit logging provides traceability for compliance, forensics, and remediation

Replication

- Pure Storage synchronous replication: Typically used for high availability, it provides real-time, zero-data-loss replication between two FlashArrays by ensuring data is written to both sites simultaneously before acknowledging completion.
- Pure Storage asynchronous replication: Typically used for site failover, it enables efficient, time-delayed replication between arrays, allowing data to be copied at scheduled intervals to balance protection and performance across geographic distances.

Platform independence

- SafeMode is available on FlashArray and FlashBlade, covering both structured and unstructured workloads
- Works with all partner integrations to ensure end-to-end resilience

Pure Protect™ //DRaaS

- Pure Protect //DRaaS provides disaster recovery for VMware by automating the orchestration of failover and recovery for virtual machines using policy-driven snapshots, replication, and rapid provisioning on secure, isolated infrastructure

With Pure Storage, indelible protection is not a feature; it's a guarantee that your data is always recoverable, even when your systems are under siege.

3 Optimize for Fast Recovery

Best Practice

In a cyber resilience strategy, data protection is only as valuable as your ability to recover fast. Too often, organizations focus on backup performance, but when ransomware strikes, it's recovery speed that determines whether the business survives or pays the ransom.

A modern recovery plan must emphasize restore-first architecture, with the ability to bring critical applications, files, and services online in minutes—not days. This means designing storage environments that support:

- **Instant rehydration of snapshots** for near-zero RTO
- **Parallel recovery** of large-scale workloads and multi-tiered environments
- **Application dependency awareness,** ensuring recovery occurs in the proper operational order (e.g., authentication must be re-established prior to opening your ERP tools)
- **Clean-room recovery validation,** where snapshot restores are checked for threats and vulnerabilities and tested before being promoted into production

Speed is only part of the equation. Precision and control are equally vital. And recovery must be orchestrated, safe, and verifiable.

Why It Matters

Most ransomware victims don't pay ransom because their data is gone; they pay because they lack the capabilities to efficiently recover or because recovery takes too long. Every hour of downtime carries cost: lost revenue, operational paralysis, customer churn, brand damage, and legal exposure.

Fast recovery enables:

- Ransom resistance: the faster you restore, the less leverage an attacker has
- SLA compliance with defined RTOs and business priorities
- Business continuity: restoration of critical systems before revenue impact
- Controlled, step-by-step recovery for complex interdependent services

Fast recovery is not just about performance; it's about business resilience under pressure.

The Pure Storage Advantage

Pure Storage architecture and ecosystem integrations are built for rapid, orchestrated recovery at scale:

FlashBlade//S™ for ultra-fast recovery

- Delivers up to 100TB/hr throughput for snapshot restore
- Enables restoration of petabyte-scale environments in hours—not days
- Ideal for large unstructured data sets, virtual machines, and database environments

Instant snapshot mounting and rehydration

- Snapshots can be cloned and brought online instantly without waiting for rehydration
- Supports recovery into clean-room environments for malware scanning and validation

Parallel, SLA-aware orchestration

- Restores can be prioritized and sequenced across applications based on business criticality
- Integrates with Veeam, Rubrik, and Commvault to support SLA-driven orchestration and testing

Secure testing in isolated recovery zones

- IT and Incident Response (IR) teams can validate restores before promoting to production
- Clones support multi-team workflows (IR, compliance, operations)

Pure Protect //DRaaS

- Disaster recovery-as-a-service offering from Pure Storage optimizes disaster recovery processes for VMware environments
- Protects virtual environments by leveraging Amazon Web Services (AWS) for disaster recovery

With Pure Storage, rapid recovery isn't theoretical; it's engineered into the platform, tested by real customers, and available when it matters most.

4 Use All-flash across All Storage Layers

Best Practice

Flash storage has traditionally been reserved for performance-critical production workloads. But in a cyber-resilient architecture, speed matters everywhere—not just for applications, but for recovery, analytics, investigation, and compliance. That's why flash should consistently extend across snapshots, backups, logs, and long-term retention layers.

When a security team needs to search logs across years of history, when a compliance audit calls for immediate access to records, or when disaster recovery teams need to restore terabytes of data quickly, performance becomes critical across the full data lifecycle.

Cyber resilient organizations implement flash at every level by:

- Using consistent, all-flash platforms, such as FlashArray and FlashBlade, for fast access to production data, short-term snapshots, and SIEM ingestion
- Leveraging high-capacity QLC flash arrays like FlashBlade//E™ and FlashArray//E™ for cold or archived data sets
- Eliminating tiering complexity by standardizing on flash performance
- Ensuring real-time search, rapid analytics, and zero-delay recovery across all workloads

Why It Matters

Many ransomware incidents unfold over weeks or months. Security teams often need to investigate activity that took place months before the encryption event. If those logs or snapshots are stored on slow, deduplicated, or cloud-tiered platforms, IR and recovery timelines suffer.

Flash across every layer enables:

- Immediate access to years of telemetry and recovery points
- Real-time querying of forensic data during active investigations
- Simplified infrastructure with no tier migration overhead
- Better user experience for IT, security, and compliance teams

Speed isn't just about performance; it's about decisive action in a crisis.

The Pure Storage Advantage

Pure Storage makes all-flash feasible and cost-effective across the data lifecycle:

FlashArray and FlashBlade for hot and warm tiers

- Supports primary workloads, snapshots, and recent logs
- Low-latency performance ideal for SIEM tools, backup restore, and analytics

FlashBlade//E and FlashArray//E for cold and archive tiers

- High-capacity QLC flash delivers flash speed at near-disk cost
- Perfect for long-term backup, historical logs, and compliance data sets
- Keeps cold data accessible for search, recovery, and legal response

No tiering penalties or migration hassles

- Flash performance is always on—no need to rehydrate, recall, or re-tier
- Simplifies operations while enhancing security response capability

Unified platform experience

- Flash-based snapshots and recovery work the same across all Pure Storage platforms
- Delivers predictability and speed at every recovery point

With Pure Storage, you don't have to choose between performance and protection. You get **flash everywhere** which means you're ready for anything.

5 Create a Secure Isolated Recovery Environment

Best Practice

In the aftermath of a cyberattack, the riskiest move is to restore directly into a potentially compromised production environment. Without first validating your recovery data, you risk reinfection, re-encryption, or re-exposure of sensitive data. That's why cyber resilient organizations implement a secure isolated recovery environment (SIRE)—a clean, logically or physically segmented infrastructure where data can be safely restored, scanned, validated, and approved before returning to production.

A properly designed SIRE allows you to:

- **Isolate** recovery infrastructure from production networks
- **Restore** from immutable snapshots into clean, quarantined environments
- **Validate** workloads using malware scanning, indicators of compromise (IOC) analysis, and application testing
- **Collaborate** across incident response, security, compliance, and legal teams in parallel
- **Control** promotion of recovered workloads through clear go/no-go criteria

SIREs are not just technical—they're operational playbooks that support legal chain of custody, evidentiary documentation, and business risk management.

Why It Matters

Even if you have snapshots or backups, they won't help if you restore compromised data into production. Reinfection is one of the most common—and costly—failures in post-breach recovery. Without a SIRE, you're restoring blind.

A SIRE provides:

- A secure, isolated environment to test recovery points before go-live
- A staging ground for forensic analysis and compliance documentation
- Controlled, auditable workflows for recovery decision-making
- Confidence that recovered systems are truly clean and secure

Most importantly, a SIRE restores trust—not just files.

The Pure Storage Advantage

Pure Storage provides the infrastructure and flexibility to enable enterprise-grade SIRE strategies:

Evergreen//One cyber SLA support

- Standby hardware provisioned next business day
- Ready-to-deploy Pure Storage arrays for isolated clean-room infrastructure

Snapshot cloning and multi-team collaboration

- Instant snapshot clones enable concurrent use by IR, compliance, legal, and ops teams
- Supports forensic investigation and recovery validation simultaneously

SafeMode enforcement in SIRE

- Snapshots restored into the SIRE remain immutable
- All recovery points are protected—even while under analysis or testing

Seamless promotion to production

- Once validated, SIRE workloads can be restored directly into production
- Supports fast, secure resumption of service

With Pure Storage, a SIRE isn't just possible; it's practical. You get the recovery control you need with the infrastructure performance and support to make it work in a real crisis.

6 Automate and Scale Snapshots

Best Practice

Snapshots are one of the most effective tools in any cyber-recovery strategy. They're fast to create and enable space-efficient, near-instant rollback to a known-good state. But they're only effective if they're taken frequently, protected against tampering, and applied consistently across all workloads.

The challenge for many organizations is that snapshotting is still too manual. Policies often vary by team. Application growth can outpace protection schedules. And human error often leads to inconsistent or missing recovery points.

To address this, cyber resilient organizations implement automated, policy-driven snapshot orchestration that scales across applications, environments, and lifecycle stages.

Effective snapshot strategy includes:

- Policy-based snapshot scheduling aligned to RPO/RTO and data tier
- Automatic protection group assignment for workloads as they are created
- Sub-minute snapshot intervals for Tier 1 workloads
- SafeMode protections to ensure snapshots can't be altered or deleted
- Integration with backup, DR, and orchestration platforms (e.g., Veeam, Commvault, Rubrik)
- Coverage verification through monitoring and reporting tools

Snapshot automation eliminates gaps, standardizes protection, and ensures you're always ready to recover.

Why It Matters

Manual snapshot practices are error-prone and can leave critical workloads exposed. A missed snapshot policy, a shortened retention window, or accidental deletion can eliminate your ability to recover.

Automated snapshot strategies provide:

- Consistent protection across all workloads and sites
- SLA compliance for RPOs
- Reduced reliance on slower, deduplicated backup platforms
- Simplified and scalable management as environments grow
- Confidence that every important system is always covered

In an environment where speed, consistency, and recoverability matter, automation isn't a convenience; it's a necessity.

The Pure Storage Advantage

Pure Storage offers advanced, scalable snapshot orchestration with no performance penalty:

Protection groups and policy automation

- Automatically assign snapshot schedules based on workload tier or application role
- Apply consistent frequency and retention settings across environments
- Dynamically adapt to infrastructure changes

Zero-impact snapshot creation

- Snapshots are thin, deduplicated, and take milliseconds to create
- No impact on IOPS, latency, or production performance

SafeMode enforcement

- Prevents snapshot deletion—even by administrators
- Retention policies locked via multi-party approval and out-of-band control

Integration with backup and orchestration tools

- Seamless compatibility with Veeam, Rubrik, Commvault, and Kubernetes-based platforms
- Snapshots feed directly into broader backup and DR workflows

Visibility and compliance through Pure1 and Pure Fusion™

- Monitor policy coverage, enforcement, and drift across the entire fleet
- Get alerts for workloads missing protection or violating policy thresholds

With Pure Storage, snapshot protection isn't manual; **it's automatic, scalable, and always aligned to business risk**.

7 AI-based Monitoring for Threat Detection

Best Practice

Cyber resilience requires more than protection; it demands awareness. You can have SafeMode snapshots, backup orchestration, and strong retention policies, but if those protections are misconfigured, drifting, or inconsistently applied, your recovery plan is already compromised.

That's why AI-powered monitoring is essential. Cyber-resilient organizations use machine learning and advanced analytics to identify configuration drift, missed snapshots, anomalies in storage behavior, and violations of protection SLAs.

This is about moving from manual oversight to intelligent, proactive monitoring that helps:

- Identify under-protected workloads
- Detect anomalous patterns like unexpected deletions or data spikes
- Identify secure settings that may create vulnerabilities
- Surface gaps in snapshot schedules, retention windows, or backup health
- Provide clear, actionable remediation guidance
- Enable ongoing compliance with internal security policies and external regulations

With AI-based monitoring, you're not just waiting for a breach to happen, you're actively reducing your exposure in real time.

Why It Matters

Most organizations are unaware that they have protection gaps until they attempt to recover and find the snapshot is missing, expired, or corrupted.

Threat actors are betting on this. Their goal is to disable your recovery silently. Without continuous insight into protection status, snapshot health, and recovery readiness, your resilience could be at risk.

AI-based monitoring helps ensure:

- All workloads are protected—automatically
- Alert fatigue is minimized by focusing on what actually matters
- Configurations don't drift silently into unsafe territory
- SLA alignment is visible and actionable
- Issues are identified and corrected long before a crisis

It gives infrastructure teams a way to **prove they're ready,every day**.

The Pure Storage Advantage

Pure Storage AI-driven management platform, Pure1®, along with policy automation via Pure Fusion™, provides the intelligence and visibility required for continuous protection assurance:

Anomaly detection engine

- Tracks system and workload behavior over time
- Detects deviations, such as sudden spikes in data usage, failed snapshot jobs, or unplanned retention changes
- Flags behaviors commonly associated with insider threats or automation misuse

Resilience and security scoring

- Assigns a protection score to each array, volume, and snapshot policy
- Surfaces where your protections are misaligned with Pure Storage best practices
- Highlights areas where coverage is missing or ineffective

AI-driven remediation recommendations

- Provides exact steps to correct deviations from the desired state (configuration drift), improve protection, or enhance recoverability
- Flags overdue snapshots, missing schedules, or unsafe retention configurations

Fleet-wide policy enforcement with Pure Fusion

- Automatically applies and enforces snapshot and protection policies across all arrays
- Ensures no workload is left unprotected—even as new applications are deployed

Security-aware dashboards and alerting

- Allows collaboration between storage and security teams
- Streams log and relevant anomaly data to SIEM and Security Operations Centers (SOCs) for integrated incident response

With Pure Storage, monitoring doesn't just tell you what went wrong; it helps you make it right, before it's too late.

8 Secure Every Layer of Storage Infrastructure

Best Practice

Zero Trust doesn't end at the network perimeter. In a cyber-resilient architecture, your storage infrastructure must be treated as part of the attack surface and secured accordingly. If attackers gain access to your storage control plane, they can disable your snapshots, alter your protection policies, or delete backup indexes. That makes storage-layer security fundamental to your recovery strategy.

Cyber-resilient organizations secure storage across five key domains:

1. **Access control**: Enforce strong identity and authentication using RBAC, MFA, and SSO integrations, or leverage native IAM capabilities. Ensure only authorized users can modify protection settings.
2. **Encryption**: Encrypt data at rest and in transit using modern, validated cryptography standards, such as AES-256 for data at rest and TLS 1.3 for data in transit. This prevents interception and ensures data privacy.
3. **Configuration integrity**: Lock down protection schedules, snapshot policies, and retention windows with SafeMode or similar safeguards. Prevent unauthorized modifications, even from privileged accounts.
4. **Firmware and software validation**: Implement secure firmware supply chains. Validate updates through cryptographic signing and integrity checks.
5. **Auditing and telemetry:** Log all access, changes, and protection events. Stream logs to a centralized SIEM, UEBA, or analytics platform for real-time visibility.

By securing every layer of the storage stack, you reduce risk and ensure that recovery mechanisms are safe, trusted, and verifiable.

Why It Matters

Attackers will delete snapshots, disable retention policies, and compromise backup tools before triggering encryption. Even well-prepared organizations can lose their ability to recover if their storage layer isn't hardened.

Securing every layer ensures:

- Only trusted users can manage protection
- Critical retention policies cannot be bypassed
- Backdoor firmware cannot be installed
- Every action is auditable and attributable
- Recovery remains trustworthy—even after a breach

The Pure Storage Advantage

Pure Storage builds security into the very DNA of its storage architecture, eliminating the need for bolt-on solutions or downstream remediation:

Strong authentication and access controls

- RBAC for least-privilege management
- SAML 2.0 SSO and MFA
- SafeMode control change requests require multi-party authorization through Pure Support
- Pure Storage IAM provides multi-party authorization

Secure firmware and software supply chain

- Cryptographically signed and validated firmware updates
- Secure boot with rollback prevention
- Automated integrity verification at every stage

Immutable configuration and snapshot protection

- SafeMode prevents any snapshot or retention policy from being modified or deleted through normal admin paths
- Retention windows can't be shortened without going through a controlled, human-validated process

Built-in encryption

- AES-256 encryption at rest on all volumes
- TLS 1.3 for all management and data plane traffic
- FIPS 140-2 validated modules for regulatory compliance

Full audit logging and log streaming

- Detailed logs of every change, snapshot, access, and setting modification
- Compatible with CrowdStrike, Rubrik Security Cloud, Superna, Splunk, Elastic, QRadar, and other enterprise SIEMs

With Pure Storage, storage doesn't just survive attack; it defends itself, records everything, and supports compliance before, during, and after an event.

9 Integrate with SecOps

Best Practice

In modern cyber-resilience strategy, storage can no longer operate in a silo. It must become part of your organization's broader security operations ecosystem. This means aligning your storage infrastructure with the tools and workflows used by your security team, so storage can actively contribute to detection, investigation, and recovery.

SecOps integration is about enabling bi-directional visibility and action between the storage layer and security operations platforms:

- **Security Information and Event Management (SIEM) platforms**, such as Splunk and CrowdStrike LogScale, ingest logs and telemetry from Pure Storage arrays to correlate with broader threat signals.
- **User and Entity Behavior Analytics (UEBA) platforms**, such as Varonis, retrieve log historical data to identify the origins of unauthorized, undetected access, and to simplify forensic analysis and evidence gathering.
- **Extended Detection and Response (XDR) platforms** include storage in their investigations, using immutable snapshots to identify lateral movement or isolate malware activity.
- **Threat-hunting platforms**, such as Rubrik Security Cloud, allow organizations to quickly identify IoCs in critical storage workloads.

By integrating with security tools, storage becomes intelligent, responsive, and contextual. It doesn't just store data—it defends it.

Why It Matters

In the absence of integration, security and infrastructure teams operate in silos. The SOC has no visibility into storage protection status or activity. The infrastructure team doesn't know when a security incident is underway.

This disconnect slows response, increases risk, and leads to missed opportunities to contain or recover from an attack.

With SecOps integration:

- Security teams can trigger snapshots when threats are detected
- SOC analysts can search logs and access history to identify compromise
- Storage can automate rollback or isolation actions as part of SOAR playbooks
- IR teams can analyze clean copies of data in isolated environments for forensics or legal review

You shorten the gap between detection and action, making recovery part of the response, not the aftermath.

The Pure Storage Advantage

Pure Storage enables deep, seamless integration with security operations platforms across your environment:

SIEM and UEBA integration

- Storage logs, snapshots, retention changes, and anomalies are streamable to tools like CrowdStrike, Rubrik Security Cloud, Varonis, Superna, Splunk, QRadar, and Elastic.
- Events can be correlated with user activity, endpoint behavior, or network traffic to detect broader compromise.

SOAR orchestration via API

- Snapshot creation and rollback can be triggered automatically when a threat is detected.
- Playbooks can initiate isolation of a volume or flag a protection policy violation.

XDR and forensic readiness

- Pure Storage snapshots provide immutable restore points for investigation.
- Forensic tools can analyze historical recovery data without fear of contamination.
- Snapshots can be cloned for legal teams, IR partners, and compliance investigators.

With Pure Storage, storage is a partner to the SOC, actively participating in your threat detection and response workflow, rather than just a passive system waiting for recovery orders.

10 Ensure Operational and Financial Flexibility

Best Practice

Cyber resilience isn't just a technical challenge, it's also a logistical and financial one. Even the best-designed recovery architecture will fail if you can't scale it quickly or fund it in a crisis. When disaster strikes, you don't have time to submit a purchase order or wait for hardware provisioning.

That's why modern recovery strategies must include built-in elasticity in both infrastructure and funding models. Storage should be consumed as a service, with recovery support included, and the ability to scale instantly without needing a CAPEX approval cycle.

A financially and operationally resilient storage strategy includes:

- On-demand capacity provisioning to handle burst recovery workloads
- Subscription-based storage with elastic scaling during emergencies
- SLA-backed recovery support including hardware availability and failback assistance
- Embedded expert guidance from storage professionals to lead recovery operations
- Quarterly readiness reviews to ensure your architecture remains aligned with evolving threats

It's not just about having a plan; it's about being ready to execute that plan without delay or red tape.

Why It Matters

Recovery timelines are often extended by technology, not by operations and procurement. Without flexible provisioning, service-level guarantees, and budget-aligned delivery models, even well-prepared teams are stuck waiting for approvals.

Financial and operational agility ensures:

- You can recover when you need to—not just when finance signs off
- Infrastructure is never the bottleneck to resilience
- SLAs for recovery readiness are contractually enforced
- Your team isn't navigating vendor relationships or supply delays in a crisis

Resilience requires actionability. Flexibility turns theory into execution.

The Pure Storage Advantage

Pure Storage delivers operational and financial agility through Evergreen//One and cyber-focused recovery SLAs:

Elastic storage-as-a-service

- Capacity can be scaled up or down based on real-time needs
- OPEX-friendly subscription model eliminates CapEx delays
- Usage-based billing aligns cost with actual business demand

Cyber-recovery SLA

- Next-business-day delivery of clean arrays for recovery use.
- Pure Storage-led recovery workflows and snapshot restoration assistance.
- Defined timelines for standby hardware provisioning and escalation support.

Expert recovery assistance

- Access to Pure Storage engineers who assist with failback planning, orchestration, and post-breach validation
- Removes complexity and pressure from internal teams during crisis response

Quarterly resilience reviews

- Architectural assessments and SLA alignment checks
- Recommendations for protection policy improvement and testing cadence

With Pure Storage, cyber resilience is always funded, always ready, and always executable without infrastructure bottlenecks or financial friction.

Conclusion

Cyber resilience is no longer optional. It's a requirement for business continuity, brand protection, and compliance. Modern attackers are targeting more than data; they're targeting your ability to recover. When that ability is compromised, your organization becomes vulnerable to ransom demands, regulatory violations, and reputational damage.

This white paper has outlined 10 best practices to help organizations build a proactive, layered, and operationally viable cyber-resilience strategy. These practices are derived from the real-world experiences of Pure Storage customers who have survived ransomware attacks and recovered successfully.

What sets this framework apart is that it does not stop at backup. It integrates protection, detection, orchestration, and automation into every part of the storage stack, then connects that stack to your security operations workflows.

With Pure Storage, cyber resilience becomes:

- Built-in, not bolted on
- Enforceable, not optional
- Actionable, not aspirational
- Aligned, across IT, security, and compliance

Each of the practices outlined, whether securing recovery points with SafeMode, automating snapshot enforcement, integrating with SecOps platforms, or recovering in clean-room environments, delivers a tactical capability that helps organizations not just bounce back, but leap forward.

Because in an era of ubiquitous cyber incidents, resilience is not just how you avoid attacks; it's how you prepare, survive, and thrive after one.

To learn more, visit the Pure Storage Cyber Resiliency page.

Addendum: Customer Stories

Want to learn more about how real-world organizations are leveraging Pure Storage solutions for cyber resiliency? These customers were once where you are and are now more prepared and resilient, thanks to Pure Storage.

City of New Orleans

PUBLIC SECTOR, NORTH AMERICA

Outcome

Critical systems restored within 48 hours after ransomware.

Why It Matters

SafeMode + FlashBlade deliver forensic-ready, rapid recovery.

Read Their Story

HealthEdge

HEALTHCARE SAAS, NORTH AMERICA

Outcome

DR reduced from 14 hours to under 4.

Why It Matters

Cyber Recovery SLA and DRaaS enable clean, fast recovery.

Read Their Story

AC Milan

MEDIA AND ENTERTAINMENT, EMEA

Outcome

Near-zero RPO/RTO, 10x faster content delivery.

Why It Matters

Performance, security, and resiliency fuel fan engagement.

Read Their Story

Perdoceo Education

EDUCATION, NORTH AMERICA

Outcome

Restores take 5 mins instead of 8 hours.

Why It Matters

Cloud-native recovery model reduces downtime and cost.

Read Their Story

DXC Technology

TECHNOLOGY/MANAGED SERVICES, GLOBAL

Outcome

RPO ~0, RTO <60 minutes with Portworx® DR.

Why It Matters

Meets SLAs for global financial clients with Kubernetes-based DR.

Read Their Story

CM1697-01-en 06/25