

arcserve®

White Paper

Cyber Resilient Immutable Storage:

Defending Against Ransomware and Insider Threats

Protecting Business Data with OpenZFS-Based Immutable Architecture
and NIST-Aligned Security Control



Executive Summary

Modern organizations face unprecedented threats from ransomware attacks and malicious insiders that can encrypt, delete, or exfiltrate critical business data. Traditional backup approaches are no longer sufficient to defend against attackers who specifically target backup repositories to prevent recovery¹. Organizations need immutable storage solutions that provide defense-in-depth protection while maintaining operational efficiency and regulatory compliance.

This white paper introduces Arcserve Cyber Resilient Storage and its immutable storage architecture built on the enterprise-grade OpenZFS file system, hardened Linux operating system, and alignment with the NIST Cybersecurity Framework (CSF) 2.0 principles².

The solution delivers:

- True immutability through file system-level write-protection and snapshot technology
- Defense against privileged account compromise via constrained administrative interfaces
- Standards-based security controls aligned with NIST CSF, FIPS compliance, and regulatory requirements
- Protection against ransomware, malicious deletion, and unauthorized modification
- Rapid recovery capabilities with point-in-time restore options

By combining OpenZFS data-integrity features with defense-in-depth security controls, Arcserve delivers air-gap-equivalent protection without operational complexity, keeping backup data available even when primary systems are compromised.

The Evolving Ransomware Threat Landscape

Ransomware Targets Backup Infrastructure

Ransomware attacks have evolved from opportunistic infections to sophisticated, multi-stage campaigns specifically designed to compromise backup and recovery systems³.

Modern attack patterns include:

- Credential harvesting to gain administrative access to backup repositories
- Lateral movement to identify and encrypt backup storage
- Dwell time attacks where adversaries remain dormant for weeks, studying backup schedules
- Backup deletion before encrypting production data, eliminating recovery options

Around 83% of breaches involved external actors, with ransomware remaining the most common attack pattern affecting organizations. Average ransom demands have exceeded \$5 million, with recovery costs often reaching 10× the ransom amount when backups are compromised⁴.

Insider Threats and Privileged Access Abuse

Malicious insiders with legitimate credentials pose equally serious risks⁵:

- Administrators with administrative access can delete backup data
- Disgruntled employees may sabotage recovery infrastructure before departure
- Compromised privileged accounts enable external attackers to act as insiders
- Accidental deletion by well-intentioned staff during troubleshooting

Traditional access controls are insufficient when the attacker possesses legitimate administrative credentials. Organizations require immutability that persists even against root-level access.

Regulatory and Compliance Drivers

Beyond threat mitigation, regulatory frameworks increasingly mandate immutable storage for data retention:

- SEC Rule 17a-4(f) requires financial records in non-rewritable, non-erasable format
- HIPAA mandates safeguards for electronic protected health information (ePHI)
- GDPR requires appropriate technical measures to ensure data integrity
- SOX Section 404 demands reliable financial data retention and audit trails

Failure to maintain compliant data protection can result in significant fines, litigation, and reputational damage.

What Defines Immutable Storage?

Defining Immutability

Immutable storage implements Write-Once-Read-Many (WORM) semantics, ensuring that once data is written, it cannot be altered, encrypted, or deleted for a defined retention period⁶.

This creates a tamper-proof data state that survives:

- **Ransomware encryption attempts** – data remains readable in original form
- **Administrative deletion commands** – retention locks prevent premature removal
- **File system corruption or malicious modification**
- **Time-based attacks** that manipulate system clocks to bypass retention

Immutability Versus Air-Gapping

Traditional air-gapped backups physically disconnect storage from networks. While effective, air-gapping introduces operational challenges.

Capability	Air-Gapped	Immutable Storage
Protection from network attacks	High	High
Operational accessibility	Manual/Delayed	Continuous
Recovery time objective (RTO)	Hours to days	Minutes to hours
Automation support	Limited	Full
Cost and complexity	High	Moderate

Table 1: Comparison of air-gapped vs. immutable storage approaches

Modern immutable storage solutions deliver air-gap-equivalent protection through logical controls—combining the security benefits of physical isolation with the operational efficiency of connected systems⁷.

The Role of File System-Level Immutability

OpenZFS provides native immutability capabilities that operate at the block level, beneath the operating system and application layers⁸:

Copy-on-write architecture: Original data blocks are never overwritten; modifications create new blocks

Atomic transactions: All operations complete fully or not at all, preventing partial corruption

Snapshot technology: Point-in-time copies consume minimal space via block-level referencing

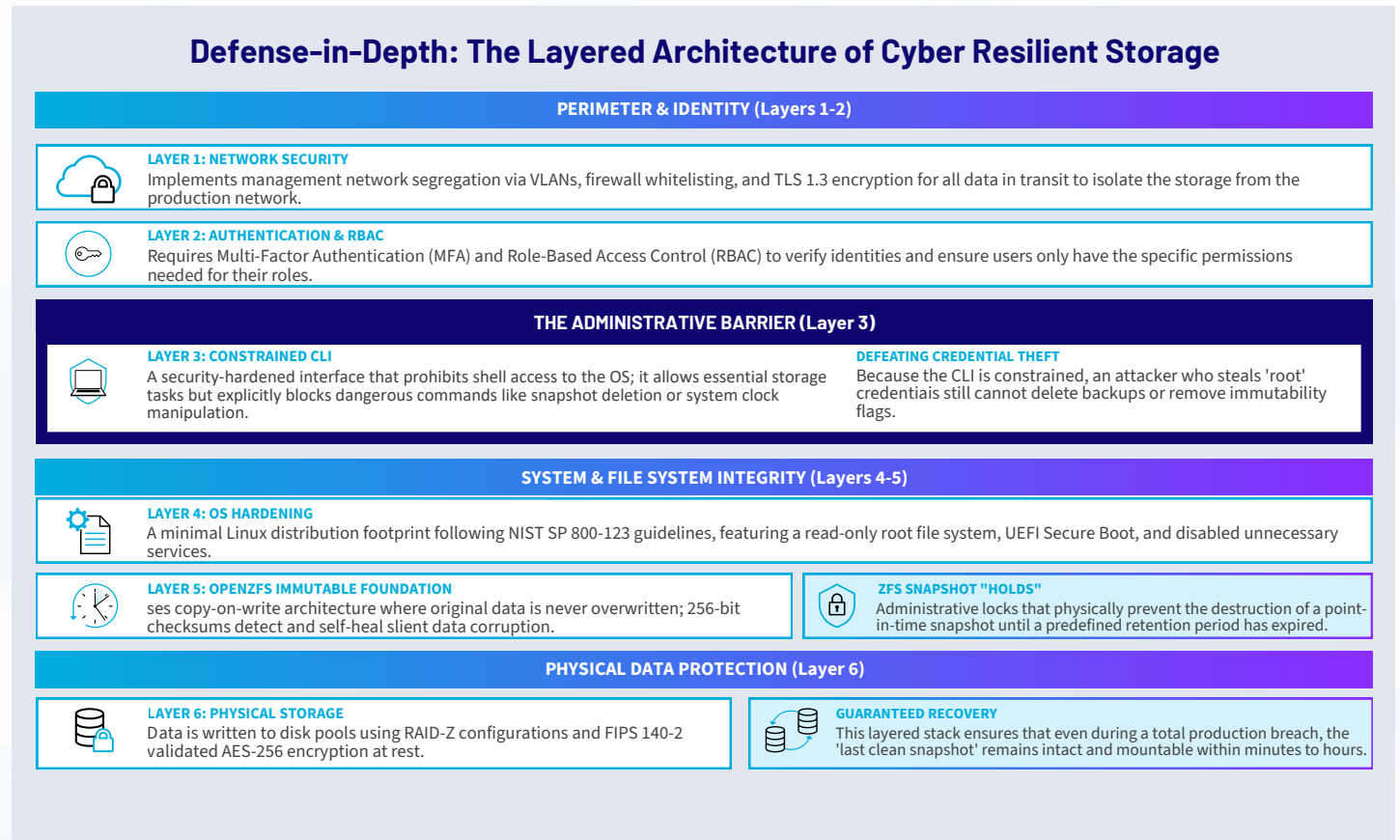
ZFS holds: Prevent snapshot deletion until retention expires, even with root access

End-to-end checksums: Detect silent data corruption and enable self-healing

This architecture means ransomware attempting to encrypt files on an immutable ZFS dataset encounters read-only errors and cannot modify the underlying snapshots.

Solution Architecture

System Overview



The immutable storage solution combines multiple layers of protection:

- **Hardened Linux Foundation:** Minimal OS footprint based on NIST guidelines, eliminating unnecessary services and attack surfaces
- **OpenZFS File System:** Enterprise-grade storage with native immutability, compression, and data integrity
- **Constrained CLI:** Limited command set preventing dangerous operations while enabling required administration
- **Multi-Factor Authentication:** Verify identity before granting administrative access
- **Role-Based Access Control (RBAC):** Segregate duties across storage, network, and user management
- **Audit Logging:** Tamper-proof logs capturing all administrative actions
- **Encryption:** FIPS 140-2 compliant algorithms for data at rest and TLS 1.3 for data in transit

OpenZFS as the Immutable Foundation

OpenZFS was selected for its proven track record in enterprise environments and inherent security properties.

Data Integrity Features:

- 256-bit checksums on all data and metadata blocks
- Automatic detection and correction of silent corruption
- Self-healing when redundant copies exist (RAID-Z configurations)
- Transaction-based consistency even during power failures

Immutability Mechanisms:

- Snapshots create instant, space-efficient point-in-time copies
- Read-only datasets prevent any modification attempts
- ZFS holds lock snapshots against deletion by any user, including root
- Arcserve UDP data resilience platform retention policies enforce minimum hold periods aligned with compliance needs

Performance and Efficiency:

- Inline compression reduces storage footprint (typical 2:1 ratios)
- Block-level deduplication for redundant data elimination
- Adaptive prefetching and intelligent caching
- Scalability from terabytes to petabytes

Constrained Command-Line Interface (CLI)

The system implements a security-hardened administrative interface that limits available commands to essential operations⁹.

Allowed Operations:

- User creation and permission management without sudo/root escalation
- Network configuration (IP addressing, bonding, routing)
- Physical storage management (disk addition, RAID-Z pool creation)
- Logical storage provisioning (datastore creation, Cyber Resilient Storage file system creation)
- System monitoring and health checks
- Support bundle generation for troubleshooting

Explicitly Prohibited:

- Shell access to underlying operating system
- Package installation or system modifications
- Snapshot deletion during retention periods
- Immutability flag removal
- System clock manipulation
- Direct file system access bypassing ZFS controls

This approach follows the principle of least privilege—administrators can perform necessary tasks without gaining capabilities that could compromise immutability. Even if an attacker compromises administrative credentials, the constrained interface prevents backup deletion.

Hardened Operating System

Cyber Resilient Storage employs a minimal Linux distribution aligned with NIST SP 800-123 guidance for server hardening¹⁰:

- **Minimal package set:** Only essential services installed, reducing attack surface and maintaining a very small footprint
- **Time source management:** Protected Network Time Security (NTS) to prevent time-based retention attacks

Network Isolation and Access Control

An ideal implementation with multi-layered network security limits exposure:

- **Management network segregation:** Separate VLAN for administrative access
- **Firewall policies:** Whitelist approach allowing only required protocols
- **TLS 1.3 encryption:** All network communications encrypted in transit
- **Certificate-based authentication:** Mutual TLS for service-to-service communication
- **Rate limiting:** Protection against brute-force authentication attempts

Encryption Standards

Data protection at rest and in transit used by UDP and Cyber Resilient Storage meets industry standards¹¹.

Data at Rest:

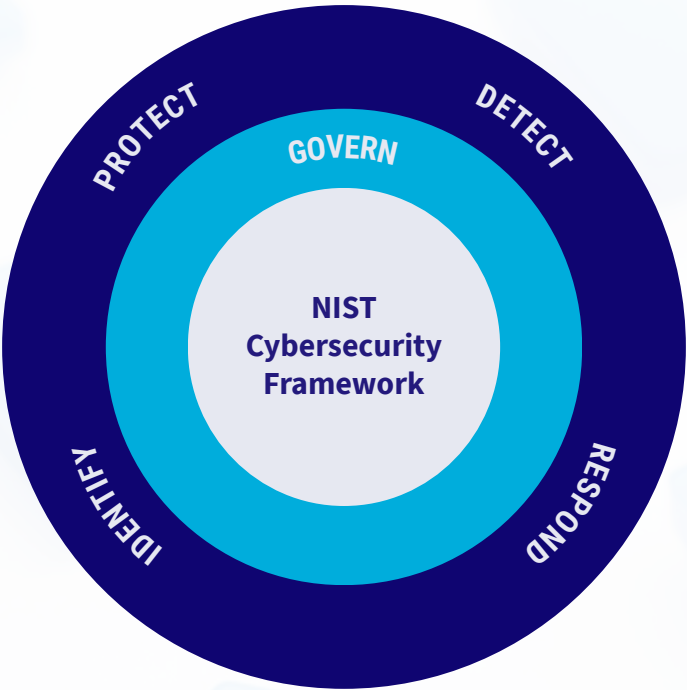
- AES-256 encryption
- FIPS 140-2 compliant cryptographic modules
-

Data in Transit:

- TLS 1.3 with perfect forward secrecy (PFS)
- Strong cipher suites (AES-256, ChaCha20-Poly1305)
- Encrypted replication for off-site copies

Alignment with NIST Cybersecurity Framework

The solution architecture of UDP and the Cyber Resilient Storage maps directly to NIST CSF 2.0 core functions, providing a structured approach to cyber risk management¹².



NIST Function	Implementation in Immutable Storage
Govern (GV)	Establish cybersecurity governance through policy-driven retention, RBAC, and audit logging aligned with business objectives and compliance requirements
Identify (ID)	Asset inventory of storage resources, data classification, vulnerability scanning, and risk assessment of backup infrastructure
Protect (PR)	Access control via constrained CLI, data-at-rest encryption, immutable snapshots, hardened OS, and network segmentation
Detect (DE)	Audit logging, integrity monitoring via ZFS checksums, anomaly detection for unusual access patterns, and SIEM integration
Respond (RS)	Incident response procedures, forensic snapshot preservation, isolation capabilities, and communication protocols
Recover (RC)	Rapid restoration from immutable snapshots, documented recovery procedures, business continuity planning, and post-incident improvement

Table 2: NIST CSF 2.0 function mapping

Govern: Policy and Risk Management

- **Cybersecurity governance:** Policy-based retention automatically enforced
- **Risk management strategy:** Quantified RPO/RTO targets with immutable backups
- **Compliance oversight:** Automated evidence collection for audits

Identify: Asset and Risk Understanding

- **Asset inventory:** Automated discovery of protected datasets
- **Risk assessment:** Continuous vulnerability scanning of storage infrastructure
- **Data classification:** Tagging and categorization of sensitive data

Protect: Safeguards for Critical Assets

- **Access control (PR.AC):** MFA, RBAC, least privilege via constrained CLI
- **Data security (PR.DS):** Encryption, immutability, data-at-rest protection
- **Protective technology (PR.PT):** Audit logs, integrity checking, secure configurations

Detect: Timely Discovery of Events

- **Anomaly detection:** Unusual access patterns, failed authentication attempts (available in UDP 10.3 and above)
- **Security monitoring (DE.CM):** Real-time alerting on integrity violations
- **Audit log analysis:** Correlation of administrative actions with business context

Respond: Action Against Detected Events

- **Response planning (RS.RP):** Documented procedures for compromise scenarios
- **Incident communication:** Automated notifications to security teams
- **Forensic preservation:** Immutable snapshots provide evidence for investigations

Recover: Restoration of Capabilities

- **Recovery planning (RC.RP):** Tested restore procedures with defined RTOs
- **Restoration from immutable copies:** Guaranteed clean recovery points
- **Improvements (RC.IM):** Post-incident reviews and control enhancements

Ransomware Protection Mechanisms

Defense-in-Depth Strategy

Protection against ransomware requires multiple coordinated controls that collectively prevent, detect, and recover from attacks¹³:

- **Prevention:** Block ransomware from reaching backup storage
- **Detection:** Identify ongoing encryption attempts
- **Containment:** Isolate compromised systems
- **Recovery:** Restore from known-good immutable copies

How Immutability Stops Ransomware

- **Scenario:** Ransomware gains root access to backup server

Attack Step	Control Response
Attack attempt: Ransomware tries to encrypt backup files or delete snapshots	ZFS response: Copy-on-write architecture and snapshot holds prevent modification
Privilege escalation: Attacker attempts to use root access	Constrained CLI: Even root cannot execute commands to remove retention locks
Result	Ransomware fails; immutable snapshots remain intact and accessible

Table 3: Ransomware attack sequence and defensive controls

Technical Mechanism:

When ransomware attempts file encryption on a ZFS dataset with active snapshots:

- 1.ZFS snapshots of UDP Data Store files appear to be in read-only or protected state
- 2.Snapshot data blocks are referenced by immutable ZFS metadata
- 3.Hold tags prevent snapshot destruction
- 4.Retention policies enforce minimum hold periods (e.g., 14, 30, 90 days)
- 5.Even privileged users receive "operation not permitted" errors

Protection Against Time Manipulation Attacks

Sophisticated attackers may attempt to manipulate system clocks to expire retention periods prematurely.

Countermeasures:

- **NTP authentication:** Signed timestamps from trusted time servers using Network Time Security (NTS)
- **Alert on time anomalies:** Sudden clock changes trigger security notifications

Snapshot-Based Recovery

Immutable snapshots enable rapid recovery with minimal data loss.

Rapid Recovery with Immutable Snapshots: A Ransomware Defense Timeline

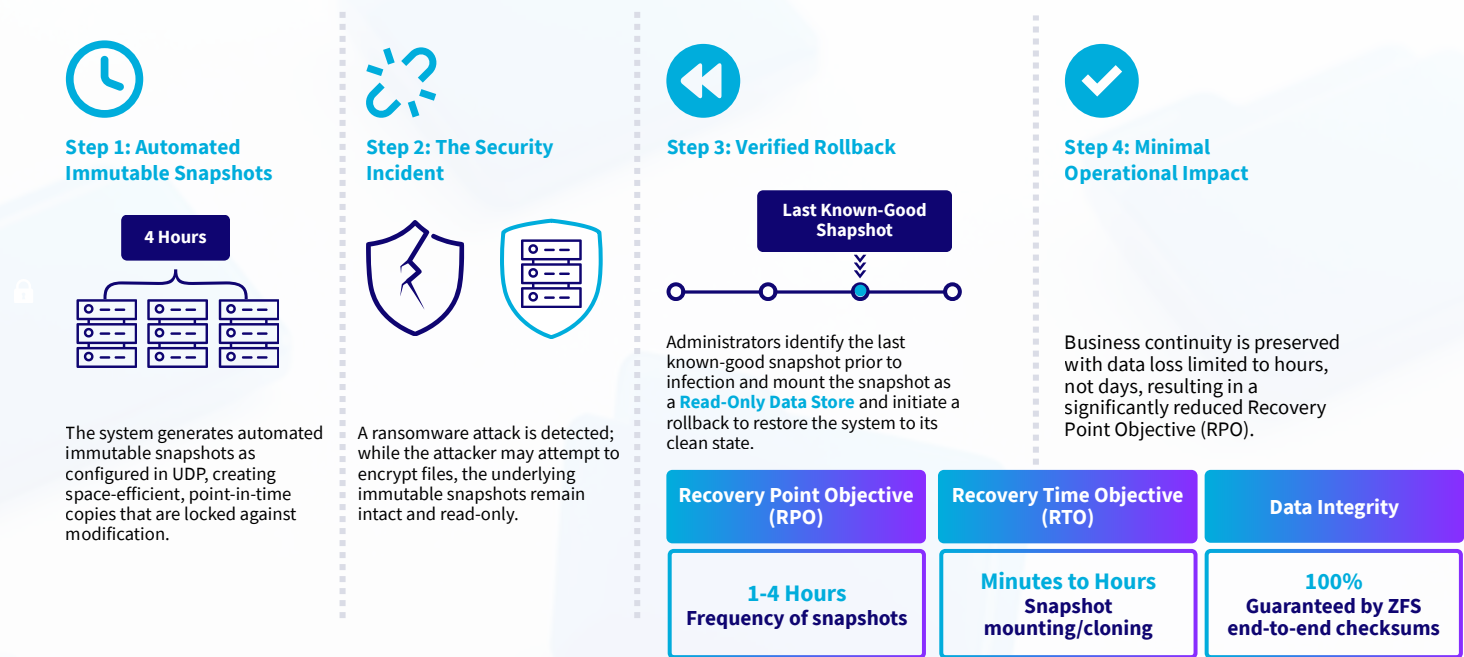


Figure 2: Snapshot-based recovery timeline

Recovery Process:

- Identify last known-good snapshot prior to ransomware infection
- Mount snapshot to new read-only data store
- Restore data to production environment
- Resume operations with minimal downtime (minutes to hours, not days)

Recovery Point Objective (RPO): Limited only by snapshot frequency (typically 1–4 hours)

Recovery Time Objective (RTO): Minutes for mounting snapshots; hours for full restore

Protection Against Malicious Insiders

Insider Threat Scenarios

Organizations must defend against multiple insider threat patterns.

Threat Actor	Attack Vector
Disgruntled administrator	Intentional deletion of backups before leaving organization
Compromised credentials	External attacker using stolen admin passwords
Negligent staff	Accidental deletion during troubleshooting
Third-party vendor	Excessive access granted to managed service providers

Table 4: Insider threat scenarios

Constrained CLI as Insider Defense

The limited command interface prevents abuse of administrative privileges.

What Insiders CANNOT Do:

- Delete snapshots during retention periods
- Disable immutability flags on datasets
- Gain shell access to modify system files
- Install malware or backdoors
- Manipulate system clocks
- Disable audit logging

What Insiders CAN Do:

Using the CLI:

- Manage user accounts within defined roles
- Configure network settings for connectivity
- Monitor system health and performance
- Generate support bundles for troubleshooting

Using Consoles:

- Create new backup policies with approved retention

Separation of Duties

RBAC implementation segregates administrative functions¹⁴:

- **Storage Administrators:** Manage physical disks, pools, and datasets using the constrained CLI of Cyber Resilient Storage
- **Backup Operators:** Configure backup policies and schedules using the consoles
- **MSP Monitors or Tenant Monitor roles:** Review audit logs and reports to ensure that the backups and immutable snapshot jobs run successfully
- **Network Administrators:** Configure network settings and firewall rules

No single role possesses sufficient privileges to compromise immutability.

Audit Logging and Forensics

Comprehensive, tamper-proof audit trails enable detection and investigation.

Logged Events:

- Authentication attempts (successful and failed)
- User account creation, modification, deletion
- Configuration changes (storage, policies)
- Snapshot creation and attempted deletion
- System events (boot, shutdown, service changes)

Multi-Factor Authentication (MFA)

Access to administrative interfaces requires multiple proof factors¹⁵:

- **Something you know:** Password or passphrase
- **Something you have:** Hardware token, certificate, or OTP device

MFA significantly reduces the risk of credential theft enabling insider attacks.

Compliance and Regulatory Alignment

Key Regulatory Requirements

The solution addresses data protection requirements across multiple regulatory frameworks.

Regulation	Key Requirement Met
SEC Rule 17a-4(f)	WORM storage with retention locks, audit trails, non-rewritable format
FINRA Rule 4511(c)	Electronic records in tamper-proof format, timestamped integrity
HIPAA Security Rule	Administrative, physical, and technical safeguards for ePHI (access controls, audit logs, encryption)
GDPR Article 32	Appropriate security measures ensuring confidentiality, integrity, availability (encryption)
SOX Section 404	Internal controls over financial reporting (data integrity, retention policies)

Table 5: Regulatory compliance mapping

SEC Rule 17a-4(f): Financial Records Retention

Securities and Exchange Commission rules mandate broker-dealers to maintain records in non-rewritable, non-erasable format¹⁶.

Requirements:

- Records retained for specified periods (3–6 years depending on type)
- Write-once, read-many (WORM) format
- Verification of authenticity and integrity
- Immediate retrieval capability
- Audit trails of access

Solution Compliance:

- Cyber Resilient Storage immutable snapshots using ZFS snapshots with holds provide WORM semantics
- Retention policies automatically enforced
- Checksums verify data integrity
- Instant snapshot mounting for retrieval
- Comprehensive audit logs

HIPAA: Healthcare Information Protection

Health Insurance Portability and Accountability Act requires safeguards for electronic protected health information (ePHI).

Administrative Safeguards:

- Security management processes (risk analysis, policies)
- Workforce security (authorization, supervision)
- Information access management (unique user IDs, emergency access)

Physical Safeguards:

- Facility access controls
- Workstation and device security

Technical Safeguards:

- Access control (unique IDs, encryption)
- Audit controls (logging and monitoring)
- Integrity controls (ensure data not improperly altered)
- Transmission security (encryption, integrity controls)

Constrained CLI, RBAC, encryption, and audit logging in Cyber Resilient Storage directly satisfy HIPAA technical safeguard requirements.

GDPR Article 32: Security of Processing

General Data Protection Regulation requires appropriate technical and organizational measures:

- **Confidentiality:** Encryption at rest and in transit
- **Integrity:** Checksums, immutability, tamper-proof logs
- **Availability:** Rapid recovery from immutable snapshots
- **Resilience:** Hardened infrastructure, redundant storage

Immutable storage demonstrates state-of-the-art technical measures for data protection, supporting GDPR compliance and reducing breach liability.

Deployment Architecture and Use Cases

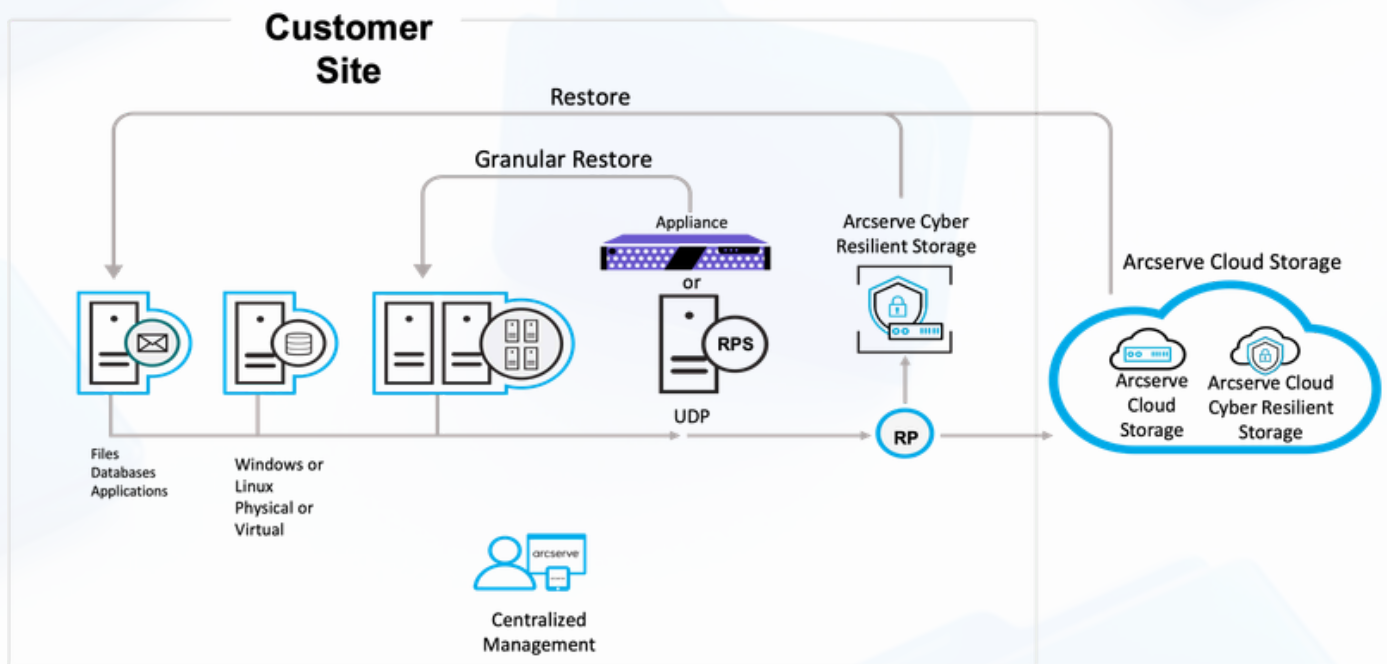
Deployment Models

The solution currently supports only the following deployment scenarios:

1. **ISO deployment:** Bootable ISO image for bare-metal installation Support for the following deployment scenarios are expected soon -
2. **On-premises appliance:** Physical hardware with pre-configured immutable storage
3. **Virtual appliance:** VM deployment in existing virtualization infrastructure (VMware, Microsoft Hyper-V, KVM)

Integration with Backup Software

Cyber Resilient Storage integrates with Arcserve UDP as a hardened repository target.



Backup Workflow:

- Backup software writes data to the data store in Cyber Resilient Storage
- Automated snapshots of the data store capture point-in-time state
- Retention locks activate based on policy (e.g., 30 days)
- Backup software believes it has full control but cannot delete protected snapshots
- Immutable snapshots are mounted as a read-only data store from the console
- Recovery initiated from backup console, reading from the read-only data store

Use Case: Ransomware Defense

Scenario: Fortune 500 company with 5,000 employees and 500TB of critical data.

Requirements:

- Protect backups from ransomware that compromises domain admin credentials
- Meet SOX and PCI-DSS compliance for financial data retention
- Achieve 4-hour RPO and 8-hour RTO
- Support existing Arcserve UDP backup infrastructure

Implementation:

- Deploy immutable storage appliance with 600TB capacity
- Configure as UDP hardened repository
- Enable daily automated snapshots with 30-day retention
- Implement constrained CLI with RBAC for separation of duties

Outcome:

- Ransomware attack detected on day 12 of infection
- Primary backups encrypted by ransomware
- Immutable snapshots remain intact on hardened repository
- Recovery completed from day 11 snapshot with 8 hours data loss
- Total downtime: 12 hours vs. weeks without immutable backups
- Zero ransom paid; full operational recovery

Use Case: Healthcare Data Protection

Scenario: Regional hospital system with 3 facilities and 250TB of ePHI.

Requirements:

- HIPAA-compliant data retention and access controls
- Protection against insider threats (terminated employees)
- 6-year retention for medical records
- Encryption for data at rest and in transit

Implementation:

- Hybrid deployment with on-premises appliance and cloud replication
- AES-256 encryption for all datasets
- Multi-factor authentication for all administrative access
- 6-year retention policy with graduated snapshot schedules
- Quarterly compliance reporting for HIPAA audits

Outcome:

- Passed HIPAA Security Rule audit with zero findings
- Disgruntled IT admin attempted backup deletion before termination
- Constrained CLI prevented snapshot destruction
- Security team notified via audit log alerts
- No data loss; all backups remained intact

Use Case: Financial Services Compliance

Scenario: Investment firm managing \$10B in client assets.

Requirements:

- SEC Rule 17a-4(f) compliant WORM storage
- 7-year retention for trade records
- Tamper-proof audit trails
- Sub-hour recovery for trading systems

Implementation:

- Dedicated immutable storage cluster for compliance data
- Automated ingestion from trading platforms
- ZFS holds configured for 7-year + 6-month retention
- Real-time replication to geographically distant site
- Integration with legal hold system for litigation preservation

Outcome:

- SEC examination confirmed WORM compliance
- Trading system failure required 3-year-old data restoration
- Retrieved archived data in 45 minutes from immutable snapshot
- Avoided \$2M in potential regulatory fines
- Zero data loss or integrity issues during recovery

Key Capabilities and Business Benefits

Sizing and Capacity Planning

Storage Capacity Factors:

- Primary data volume (baseline)
- Change rate (daily/weekly delta)
- Retention period requirements
- Compression ratio (typical 2:1 for mixed data)
- Snapshot overhead (5–20% depending on change rate)

Capacity Formula:

Required Capacity = (Primary Data × (1 + Change Rate × Retention Days)) / Compression Ratio

Example:

- Primary data: 100TB
- Daily change rate: 5%
- Retention: 30 days
- Compression: 2:1

Capacity = (100TB × (1 + 0.05 × 30)) / 2 = 125TB raw

Network Configuration

Best practices for optimal performance:

- Dedicated backup network (isolated VLAN)
- 10GbE or faster connectivity for large environments
- Jumbo frames (MTU 9000) for improved throughput

Snapshot Schedules

Balanced approach to RPO and storage efficiency:

Snapshot Frequency	Retention	Purpose
Daily	30 days	Weekly/monthly restore points
Weekly	12 weeks	Quarterly compliance
Monthly	12 months	Annual retention, long-term
Yearly	7 years	Regulatory compliance (SEC, HIPAA)

Table 6: Recommended snapshot retention schedule

Security Hardening Checklist

Post-deployment security configuration:

- Change all default passwords and credentials
- Configure multi-factor authentication for all admins
- Implement network segmentation (separate management VLAN)
- Enable encrypted replication for off-site copies
- Document and test recovery procedures
- Schedule quarterly access reviews and permission audits
- Configure alerting for failed authentication attempts
- Establish retention policies aligned with compliance requirements

Testing and Validation

Regular verification of protection and recovery:

- **Monthly:** Validate snapshot creation and retention enforcement
- **Quarterly:** Perform test restores from immutable snapshots
- **Annually:** Conduct ransomware simulation exercises
- **After changes:** Test recovery procedures following any system modifications

Ransomware Simulation:

- Create test dataset with sample data
- Attempt to encrypt files as privileged user
- Verify immutability prevents modification
- Attempt snapshot deletion with admin credentials
- Confirm retention locks prevent premature removal
- Document results and update procedures

Operational Considerations

Backup and Recovery Operations

Daily Operations Workflow:

- Backup software writes data to immutable storage target
- Assured Recovery testing validates the recoverability of the backups
- Automated snapshots capture state at scheduled intervals
- Monitoring validates successful snapshot creation
- Retention locks activate automatically per policy
- Expired snapshots removed only after retention period ends
- Administrators review audit logs for anomalies

Recovery Workflow:

- Identify required recovery point (date/time)
- Locate corresponding immutable snapshot
- Verify integrity via ZFS checksums
- Mount snapshot as a Read-Only Data Store
- Backup software initiates a restore from the Read-Only Data Store
- Validate restored data before returning to production

Monitoring and Alerting

Critical Metrics for Operational Health:

- Storage capacity utilization and growth trends
- Snapshot creation success/failure rates
- Retention policy compliance
- Authentication failures and access anomalies
- ZFS pool health and disk errors
- Network throughput and latency
- Backup job completion status

Alert Thresholds:

- Storage capacity: 80% warning; 90% critical
- Snapshot creation failure
- Failed authentication attempts: ≥ 5 in 15 minutes
- ZFS checksum errors detected
- Retention policy violations
- Unauthorized configuration changes

Maintenance and Updates

Planned Maintenance Activities:

- Security patches applied monthly (automated where possible)
- Firmware updates quarterly for storage hardware
- ZFS pool scrubs monthly to verify data integrity
- Capacity planning reviews quarterly
- Access control reviews semi-annually
- Disaster recovery testing annually

Update Process:

- Review security bulletins and patch notes
- Test updates in non-production environment
- Schedule maintenance window with stakeholders
- Create pre-update snapshot for rollback capability
- Apply updates via secure, validated mechanism
- Verify system functionality post-update
- Document changes and update runbooks

Disaster Recovery and Business Continuity

Multi-Site Protection Strategy:

- Primary immutable storage at main data center
- Encrypted replication to geographically distant site
- Retention locks applied at both locations
- Automated failover capability for disaster recovery scenarios
- Regular disaster recovery testing (quarterly recommended)

Recovery Time Objectives by Scenario:

Scenario	RTO	RPO
Individual file restores	15 minutes	Last snapshot
Application/database restore	1–4 hours	Last snapshot
Full system disaster recovery	8–24 hours	Last replication
Ransomware recovery	4–12 hours	Pre-infection snapshot

Table 7: Recovery objectives by scenario

Cost-Benefit Analysis

Total Cost of Ownership (TCO)

Cost Components:

- Initial hardware/software acquisition
- Implementation and configuration services
- Annual maintenance and support (typically 18–22% of purchase price)
- Storage capacity (disk hardware)
- Network infrastructure (if upgrades required)
- Training for IT staff
- Ongoing monitoring and management

Cost Savings and Risk Mitigation:

- Elimination of ransom payments (average \$5M per incident)
- Reduced recovery time (hours vs. weeks), minimizing business disruption
- Avoided regulatory fines for non-compliance
- Reduced cyber insurance premiums (10–30% discount possible)
- Elimination of tape infrastructure and off-site storage costs
- Lower administrative overhead vs. air-gapped manual processes

Return on Investment (ROI)

Sample Calculation for Mid-Sized Businesses:

Estimated Costs (3-year TCO):

- Immutable storage solution: \$150,000
- Implementation services: \$25,000
- Annual support (3 years): \$81,000
- Staff training: \$10,000
- Total 3-year cost: \$266,000

Benefits:

- Avoided ransom payment (probability-weighted): \$1,500,000
- Reduced downtime (20 days × \$50K/day): \$1,000,000
- Avoided regulatory fines: \$500,000
- Cyber insurance discount (3 years): \$75,000
- Eliminated tape costs (3 years): \$45,000
- Total 3-year benefit: \$3,120,000

ROI Calculation:

• $ROI = (Benefits - Costs) / Costs \times 100 = (3,120,000 - 266,000) / 266,000 \times 100 = 1,073\%$
Even with conservative probability adjustments (e.g., 20% chance of ransomware attack), ROI remains strongly positive at 214%.

Intangible Benefits

Beyond quantifiable ROI, immutable storage delivers:

- **Confidence in recovery capabilities:** Assurance that data can be restored
- **Reputation protection:** Avoid breach disclosure and customer trust erosion
- **Competitive advantage:** Demonstrate security leadership to customers
- **Operational resilience:** Reduced concern about backup integrity among IT leadership
- **Board confidence:** Demonstrable cyber resilience aligns with fiduciary duty

Cost-Benefit Analysis

Why OpenZFS-Based Immutability?

Advantages over alternative approaches:

Approach	Limitations	OpenZFS Advantage
OS-level file flags	Require root to set; root can remove	ZFS holds prevent removal even with root
Object storage locks	Requires S3-compatible infrastructure	Native file system feature; no dependencies
Tape/WORM hardware	High cost; slow recovery; manual processes	Fast random access; automated; cost-effective
Air-gapped systems	Manual intervention; delayed recovery; operational friction	Continuous availability; instant recovery

Table 8: Immutability approach comparison

Key Differentiators:

- **Native file system immutability:** Built into ZFS, not a bolt-on solution
- **Constrained CLI:** Prevents administrative abuse (unique to this solution)
- **NIST alignment:** Explicit mapping to CSF 2.0 functions
- **Minimal OS:** Reduced attack surface vs. general-purpose Linux distributions
- **Integrated encryption:** End-to-end data protection without performance penalty
- **Proven reliability:** OpenZFS deployed in millions of systems globally

Market Positioning

Target Segments:

- **Primary:** Small and Mid-market Businesses (100–5,000 employees) seeking affordable cyber resilience
- **Secondary:** Large Organizations requiring supplemental immutable tier
- **Tertiary:** Managed service providers (MSPs) offering backup-as-a-service

Value Proposition by Segment:

- **Mid-market:** Enterprise-grade ransomware protection without enterprise complexity or cost
- **Large Organizations:** Defense-in-depth immutable tier complementing existing backup infrastructure
- **MSPs:** Multi-tenant immutable storage enabling differentiated backup services

Conclusion

Modern cyber threats demand modern solutions. Traditional backup approaches that rely solely on perimeter defenses and access controls are insufficient against ransomware and insider threats that specifically target backup infrastructure.

Immutable storage built on OpenZFS foundations, hardened Linux, and NIST-aligned security controls provide:

1. **Guaranteed recovery:** Snapshots survive ransomware and malicious deletion
2. **Compliance confidence:** Meet SEC, HIPAA, GDPR, and other regulatory mandates
3. **Operational efficiency:** Air-gap-equivalent protection without manual processes
4. **Reduced risk:** Eliminate ransom payment scenarios and business disruption
5. **Proven technology:** OpenZFS's 15-year track record in enterprise environments

Organizations that implement immutable storage as part of a comprehensive cyber resilience strategy position themselves to survive and rapidly recover from the inevitable next attack. The question is not whether your organization will face a cyber incident, but whether your backups will survive intact. Immutable storage ensures the answer is yes.

References

- [1] Halcyon AI. (2025). Last Year in Ransomware: Threat Trends and Outlook for 2025. <https://www.halcyon.ai/blog/last-year-in-ransomware-threat-trends-and-outlook-for-2025>
- [2] National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework 2.0. <https://www.nist.gov/cyberframework>
- [3] Cybersecurity and Infrastructure Security Agency. (2024). Ransomware Guide. <https://www.cisa.gov/stopransomware>
- [4] Verizon. (2024). 2024 Data Breach Investigations Report. <https://www.verizon.com/business/resources/reports/dbir>
- [5] Ponemon Institute. (2023). Cost of Insider Threats: Global Report. <https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats>
- [6] Airiam. (2024). How to Recover from a Ransomware Attack with Immutable Backups. <https://airiam.com/blog/recover-ransomware-immutable-backups>
- [7] ISA Global Cyber Alliance. (2025). *Ransomware Resiliency for Storage Backup: Trends, Threats, and Tips*. <https://gca.isa.org/blog/ransomware-resiliency-for-storage-backup-trends-threats-and-tips>
- [8] AWS Documentation. *Security in Amazon FSx for OpenZFS*. <https://docs.aws.amazon.com/fsx/latest/OpenZFSGuide/security.html>
- [9] Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *NIST SP 800-123: Guide to General Server Security*. National Institute of Standards and Technology. <https://csrc.nist.gov/publications/detail/sp/800-123/final>
- [10] Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *NIST SP 800-123: Guide to General Server Security*. National Institute of Standards and Technology. <https://csrc.nist.gov/publications/detail/sp/800-123/final>
- [11] National Institute of Standards and Technology. (2024). *FIPS 140-2 Cryptographic Module Validation Program*. <https://csrc.nist.gov/projects/cryptographic-module-validation-program>
- [12] National Institute of Standards and Technology. (2024). *NIST Cybersecurity Framework 2.0*. <https://www.nist.gov/cyberframework>
- [13] National Institute of Standards and Technology. (2024). *Implementation Examples for the NIST Cybersecurity Framework 2.0*. <https://www.nist.gov/document/csf-20-implementations-pdf>
- [14] National Institute of Standards and Technology. (2020). *NIST SP 800-53 Rev. 5: Security and Privacy Controls*. <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
- [15] National Institute of Standards and Technology. (2017). *NIST SP 800-63B: Digital Identity Guidelines*. <https://pages.nist.gov/800-63-3/sp800-63b.html>
- [16] Securities and Exchange Commission. (2022). *Electronic Storage of Broker-Dealer Records: 17 CFR 240.17a-4*. <https://www.sec.gov/rules/interp/2022/34-96034.pdf>

About Arcserve

Arcserve, the pioneer in unified data resilience, protects data from ransomware, cyberattacks, and disasters through simple, flexible, and affordable data protection solutions for small and mid-size organizations.

Arcserve is trusted by customers, channel partners, and managed service providers around the globe. Arcserve delivers AI-enabled cyber resilience protection and world class customer support, so IT teams can have streamlined, cost-effective data management and recovery with low TCO. Learn more at arcserve.com.