

arcserve®

White Paper

Arcserve Cyber Resilient Storage

Immutable Backup Defense Against Modern Ransomware Threats



Executive Summary

Ransomware attacks increasingly target backup repositories, with over 90% of attacks now specifically compromising backup data to eliminate recovery options¹.

Small and mid-sized organizations face particular risks since they are a target for almost 50% of all cyberattacks.

Cybercriminals see SMBs and mid-sized organizations as a “low-hanging fruit” without the cybersecurity budgets and dedicated IT and cybersecurity teams that larger enterprises employ².

You can take decisive action against ransomware by leveraging immutable backup protection that addresses critical vulnerabilities.

By using Arcserve Cyber Resilient Storage for immutable backup storage, you protect valuable data and keep assets secure — without compromising cost-efficiency or operational simplicity.

The Evolving Ransomware Threat Landscape

Small and mid-sized organizations face a particularly challenging situation as they often manage valuable data with limited IT resources—an attractive target for attackers seeking maximum impact with minimal resistance. The spread of ransomware-as-a-service models means that sophisticated cyber weapons are now in the hands of a broader range of threat actors.

That’s why it doesn’t come as a surprise that 44% of all breaches over the past year involved ransomware³. The fact that 88% of all ransomware breaches target smaller organizations underscores the value of cyber resilience for SMB and mid-market organizations⁴.

1. Sophos, The impact of compromised backups on ransomware outcomes, March 2024

2. Forbes, The Ransomware Epidemic: Why SMEs Are The New Primary Target, February 2025

3. Verizon, 2025 Data Breach Investigations Report

4. Mimecast, The modern Ransomware Playbook: Phishing and GenAI Attacks

The Critical Role of Immutable Backup Protection

Immutable backups are essential for a modern cyber resilience strategy. These immutable backups—those that cannot be altered or deleted once written—provide the ultimate protection against ransomware encryption attempts.

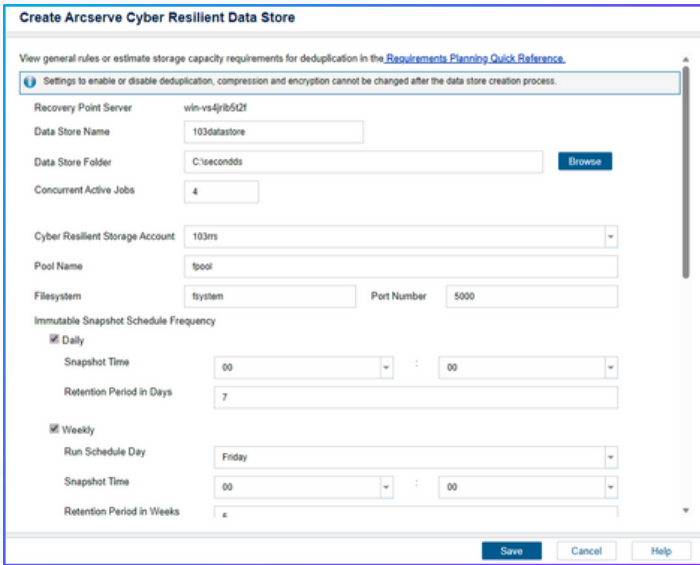
The strategic importance of immutable backups extends beyond mere data protection, as they provide benefits that can have financial and operational impact.

Immutable backup is the most important tool against ransomware according to most managed service providers that deliver IT and data protection services to small and medium enterprises⁵.

- ✔ **Rigid Recovery Points:** When conventional backups are compromised, organizations face complete data loss or expensive ransom payments. When created on a regular schedule, immutable backups ensure viable recovery points remain available regardless of attack sophistication.
- ✔ **Accelerated Recovery Timelines:** With immutable backups, organizations can restore operations more quickly, as organizations often don't need to verify data integrity given its rigid and untouched state during recovery.
- ✔ **Regulatory Compliance Assurance:** Immutable backups simplify compliance with regulations like NIST, GDPR, and HIPAA, which increasingly require verifiable data integrity and protection measures.
- ✔ **Defense Against Insider Threats:** Even sophisticated attacks leveraging compromised credentials cannot alter immutable backups, creating a truly "air-gapped" protection layer within digital systems. Solutions like Arcserve Cyber Resilient Storage also provide access controls (RBAC) to ensure that only a limited number of authorized employees have access to the data.
- ✔ **Passive Ransomware Defense:** Some solutions, like the Arcserve UDP data resilience platform, include the ability to detect malware in backups and prevent reinfection when compromised backups are restored.
- ✔ **AI-Driven ransomware detection:** Every IT leader can use extra ransomware defenses.

5. Infracore, What is Immutable Backup - Guide for MSPs, January 2025

Arcserve Cyber Resilient Storage delivers essential ransomware protection capabilities through:



Immutable Storage: Data integrity through immutable snapshots that are locked to unauthorized modifications. Keep critical business data tamper-proof and recoverable

Advanced Security and Governance: Multilayered security architecture that creates and maintains a barrier between threats and data

Policy-Driven Defenses: Intelligent automation that enforces compliance and protection, ensuring consistent security standards

Solution Overview: Purpose-Built Immutable Protection

Arcserve Cyber Resilient Storage provides immutable backup storage for cloud, on-premises, and hybrid workloads with seamless integration into existing Arcserve environments.

It is designed to work with the unified interface for managing backups and storage for Arcserve UDP (for organizations), as well as Arcserve ImageManager* (for managed service providers), delivering enterprise-grade protection without requiring significant additional investment or specialized expertise.

Arcserve UDP and its integration with Arcserve Cyber Resilient Storage offers a unified interface that simplifies the management of backups and immutable storage, eliminating the need to juggle multiple tools or platforms.

This single-pane-of-glass experience allows IT teams to configure, monitor, and manage data protection workflows from one intuitive dashboard—reducing complexity, saving time, and minimizing the risk of misconfiguration.

For existing Arcserve UDP users, this seamless integration means organizations can extend their cyber resilience strategy without disrupting familiar workflows while gaining the added benefits of immutable storage, improved compliance, advanced governance, and flexible cloud region selection—all from the same trusted environment they already use.

Meet your RPO/RTOs: With continuous data protection, immutable snapshots, and instant recovery capabilities.

Built-in orchestration, automation, and simplified management tools enable lean IT teams to meet their RTO and RPO targets – ensuring operations return to normal with minimal downtime and data loss

* only Cloud Cyber Resilient Storage

Key Capabilities and Business Benefits



arcserve®
Cyber Resilient
Storage®

Cost Optimization Technologies

- Built-in deduplication and compression dramatically reduce storage requirements once combined with Arcserve UDP
- Only changed object versions are stored, optimizing efficiency
- Snapshot architecture creates lightweight indexes rather than full data clones
- No additional network traffic charges caused by recovery and replication source (egress or API requests)

Operational Efficiency

- Self-healing capabilities for disk failures enhance reliability while reducing administrative overhead
- Single intuitive interface provides holistic visibility and control across storage locations
- Reduced complexity allows efficient management without specialized expertise
- High availability at 99.9% when stored in a single region, and 99.99% when utilizing two regions

True Storage-Layer Immutability

- WORM (Write once read many) technology ensures backup data cannot be altered or deleted once written
- Creates an impenetrable barrier against ransomware attacks targeting backup repositories
- Guarantees clean recovery points availability regardless of attack sophistication

Deployment Flexibility

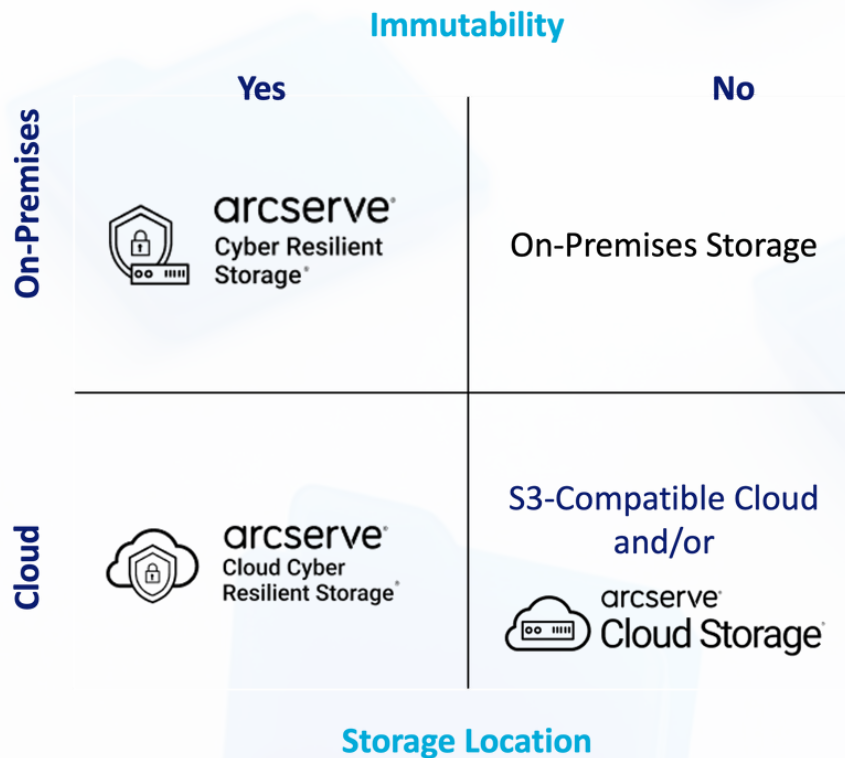
- Supports both cloud and on-premises deployment models
- 9 available cloud regions for geographic distribution and compliance alignment

Simplified Compliance and Governance

- Immutability settings are definable at the data store level for granular control
- Simplified compliance with NIST, GDPR, and HIPAA through verifiable data integrity
- Reduced cloud retention burden with minimum retention windows as low as 30 days
- Users can choose between Governance and Compliance mode to allow or prevent a user with root privileges to modify immutable snapshot data, respectively

Strategic Business Value

Arcserve covers key immutability scenarios with on-premises or cloud options.

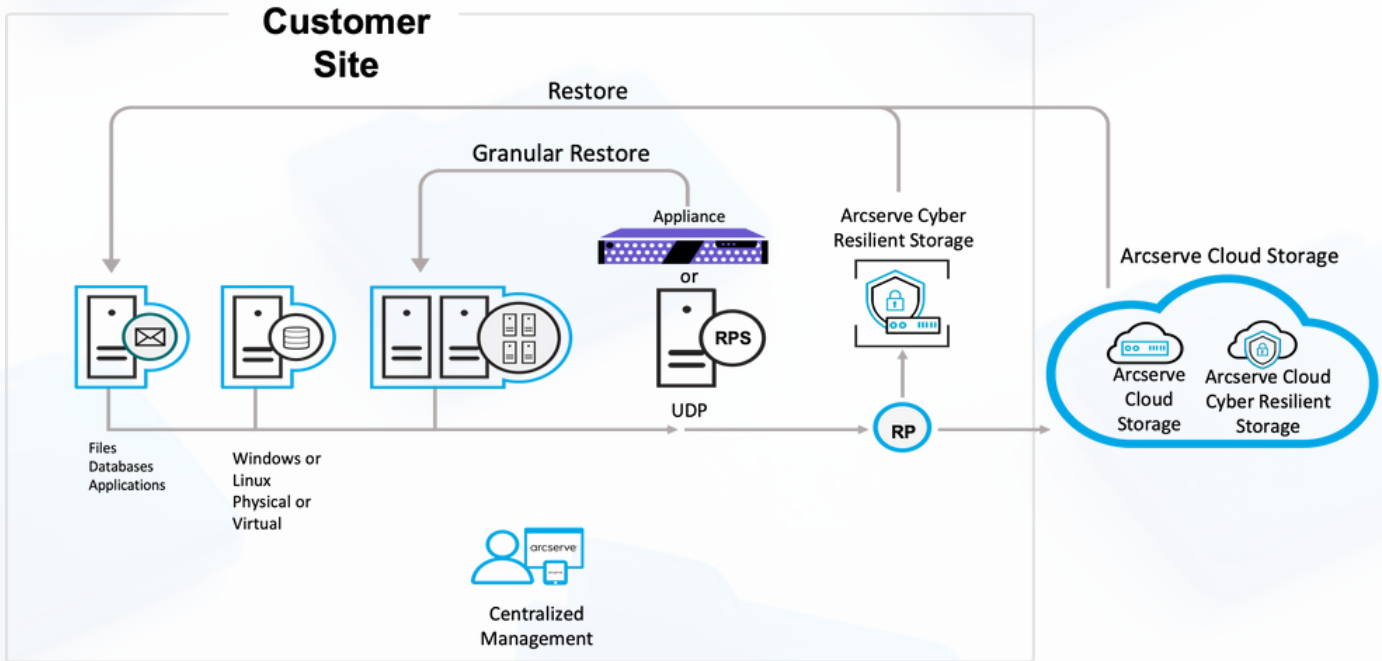


Arcserve Cyber Resilient Storage represents a strategic business asset enabling organizational resilience against evolving cyber threats. By ensuring recovery options remain viable even during sophisticated attacks, Arcserve Cyber Resilient Storage provides business continuity assurance that extends beyond IT concerns to core business operations and reputation management.

Organizations can right-size their immutable storage based on current business needs while retaining flexibility for future changes, allowing businesses to strengthen their resilience posture immediately.

Immutable Storage	Cost Upfront	Complexity	Speed	Control	Compliance
Cloud	✓	✓	✓✓	✓	✓
On-Premises	✓✓	✓	✓✓✓	✓✓✓	✓✓✓
Hybrid	✓✓✓	✓	✓	✓✓	✓✓

Solution Architecture



Arcserve Cyber Resilient Storage delivers consistent, immutable backups while minimizing storage costs through advanced deduplication, compression, and governance. The snapshot architecture creates lightweight indexes rather than full data clones, enabling daily snapshots without additional storage impact while maintaining complete recovery capabilities. It can be used for both backup and replication purposes.

Compatibility

Arcserve Cyber Resilient Storage is integrated with Arcserve UDP. If you're running an older version of UDP, you won't be able to take advantage of Arcserve Cyber Resilient Storage until you upgrade to UDP 10.2 or higher.

As a standalone product, it needs to be purchased separately. For existing customers using solutions like Arcserve Cloud Hybrid, migration is easy with datastore-to-datastore replication.

Cyber Resilient data stores can be used everywhere traditional UDP data stores can be used. Recovery from Cyber Resilient data stores is 100% consistent with UDP restore experience: Bare Metal, Full VM, File & Folder, Instant VM, Virtual Standby, Jumpstart.

Arcserve Cyber Resilient Storage and UDP – Your Advantage Against Ransomware

Immutable storage capabilities and UDP Premium edition features like AI-driven anomaly detection and Assured Security™ combine to provide another layer of protection to your backup and recovery strategy.

Comprehensive Data Resilience

Ransomware attacks have become increasingly sophisticated, and small and mid-sized businesses are particularly vulnerable. They face a large portion of all cyberattacks, as cybercriminals see them as "low risk" targets due to their limited data protection capabilities.

Arcserve, the pioneer in unified data resilience, is dedicated to helping small- and mid-sized organizations strengthen their cyber resilience and rapidly bounce back from ransomware attacks, cyberattacks, and disasters.

Arcserve Cyber Resilient Storage exemplifies this commitment by delivering immutable backup storage that integrates seamlessly with existing Arcserve products. It addresses a critical gap in cyber resilience for small and mid-sized organizations by providing robust, streamlined, and affordable ransomware and cyber threat protection.

To discover how Arcserve Cyber Resilient Storage can strengthen your organization's defense against ransomware and other cyber threats, [try it for free for 30 days](#).

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.