PAC STORAGE

How PAC Storage Helps with Ransomware Protection

Layered Storage Protection for Backup, Recovery, and Business Continuity

Ransomware has become one of the most disruptive threats facing modern organizations. Attacks can encrypt production data, disable applications, spread across connected infrastructure, and increasingly target backup repositories to prevent recovery. For IT teams, the challenge is no longer just preventing an attack. The real question is whether the organization can recover quickly with clean, protected copies of critical data.

PAC Storage helps organizations strengthen ransomware resilience with a layered storage architecture designed to protect primary workloads, backup repositories, archives, and replicated copies. With support for NAS, SAN, and S3-compatible object storage in a single platform, PAC Storage gives organizations flexible deployment options while maintaining enterprise-class data protection features such as snapshots, replication, S3 object immutability, WORM retention, encryption options, and high availability.

PAC Storage is software agnostic, allowing organizations to integrate with their preferred backup, virtualization, media, archive, and disaster recovery workflows. Whether used with backup software, file services, virtual machine repositories, media project storage, or long-term archive workflows, PAC Storage provides a secure foundation for protecting data before, during, and after a ransomware event.

The Ransomware Recovery Challenge

Traditional backup strategies were often built around the idea that a copy of data was enough. Modern ransomware has changed that. Attackers may attempt to encrypt production files, delete snapshots, compromise backup credentials, or destroy secondary copies before launching the final attack. If backup and recovery data can be altered or deleted, recovery becomes uncertain.

Organizations need storage systems that can help preserve clean recovery points, isolate protected copies, and support fast restoration. They also need the flexibility to protect different types of data across file, block, and object environments without locking into one application or workflow.

PAC Storage addresses this challenge through a multi-layered approach:

- **Protect production and backup data with point-in-time recovery copies.**
  Snapshots provide fast rollback points that can help restore data to a clean state after corruption, accidental deletion, or ransomware encryption.
- **Use immutability to prevent protected data from being changed or deleted**.
  S3-compatible object storage with Object Lock / WORM-style retention can help protect backup and archive data from unauthorized modification or deletion during the defined retention period.
- **Maintain additional recovery copies through replication and cloud gateway options.**
  Remote replication and cloud-integrated workflows can help preserve additional copies outside the primary production environment.
- **Keep storage available with dual active-active architecture.**
  High availability helps reduce the risk of storage downtime and supports business continuity when rapid recovery matters most.

PAC STORAGE

Key PAC Storage Ransomware Protection Features

- **Immutable Snapshots**

Snapshots provide point-in-time copies of data that can be used for rapid recovery. If production files are encrypted or corrupted, administrators can roll back to a previous clean snapshot instead of attempting to rebuild from scratch.

This is especially valuable for file shares, application data, virtual machine storage, media repositories, and departmental workloads where users need fast access to previous versions of data. Snapshot protection can help reduce recovery time and limit the operational impact of ransomware.

- **S3 Object Immutability and WORM Protection**

For backup and archive workflows, PAC Storage supports S3-compatible object storage with immutability features such as Object Lock and retention policies. When enabled, protected objects cannot be modified, overwritten, or deleted until the retention period expires.

This provides WORM-style protection for critical backup and archive data. Even if ransomware or an unauthorized user attempts to encrypt or delete protected objects, the retained copy remains preserved during the lock period. The older Veeam solution brief describes this concept as using S3 Object Lock API support to retain data for a defined period and prevent unauthorized modification, deletion, or encryption.

Because PAC Storage is software agnostic, this protection can support a wide range of S3-compatible backup and archive workflows, not just one backup application.

- **Local Recovery for Fast Rollback**

Local snapshots allow organizations to recover quickly without always needing to pull data from a remote site or cloud archive. This helps improve recovery time objectives when ransomware affects recently changed files or active workloads.

For many organizations, this is the first line of recovery: restore the most recent clean version locally, validate the data, and resume operations as quickly as possible.

- **Remote Replication for Disaster Recovery**

PAC Storage can help maintain protected copies at a secondary site using replication. Remote replication adds another layer of resilience by keeping data available outside the primary storage environment.

If a ransomware incident affects the primary site, a replicated copy can help support disaster recovery, failover planning, and business continuity. Replication is especially useful for organizations that need a secondary recovery location for critical workloads, backup repositories, media archives, or project data.

- **Cloud Gateway Option**

For organizations using cloud storage as part of their data protection strategy, PAC Storage cloud gateway options can help extend protected copies to cloud-based storage targets. This gives IT teams another layer of recovery flexibility while supporting encryption and policy-based movement of data.

A cloud copy can be useful for long-term retention, disaster recovery, offsite protection, and hybrid data protection strategies.

- **Dual Active-Active High Availability**

Ransomware recovery depends not only on having protected copies, but also on keeping the storage platform available. PAC Storage systems are designed with dual active-active controller architecture to help eliminate single points of failure and maintain access to data.

High availability is important during normal operations and even more critical during recovery. When an organization is trying to restore data, validate backups, or resume production workloads, the storage infrastructure must remain stable, resilient, and accessible.

Protocol Flexibility with Software-Agnostic Protection for Mixed Workloads

PAC Storage supports NAS, SAN, and S3 object storage in one platform, giving organizations flexibility to consolidate mixed workloads without compromising data protection. This allows IT teams to support file shares, virtual machines, databases, backup repositories, media workflows, project storage, and archive data from a single storage architecture.

Because PAC Storage is software agnostic, organizations can use the backup, virtualization, archive, or recovery software that best fits their environment. PAC Storage provides the secure storage foundation, while customers retain flexibility in how they manage data protection policies, retention schedules, and recovery workflows.

Business Benefits

PAC Storage helps organizations improve ransomware resilience by focusing on practical recovery outcomes:

- **Reduce downtime** by restoring from clean snapshots or protected backup copies.
- **Protect backup and archive data** with S3 object immutability and WORM-style retention.
- **Improve recovery flexibility** with local snapshots, remote replication, and cloud gateway options.
- **Support mixed workloads** across NAS, SAN, and S3 object storage.
- **Maintain availability** with dual active-active architecture and no single point of failure.
- **Avoid software lock-in** with a platform designed to integrate into a wide range of backup and recovery environments.

Conclusion

Ransomware protection requires more than one tool, one backup job, or one copy of data. Organizations need a layered storage strategy that can preserve clean recovery points, protect backups from deletion or encryption, replicate critical data, and keep infrastructure available during recovery.

PAC Storage provides this foundation with enterprise-class storage features including snapshots, S3 object immutability, WORM retention, replication, cloud gateway options, and dual active-active high availability. By supporting NAS, SAN, and S3 object storage in one software-agnostic platform, PAC Storage helps organizations strengthen ransomware resilience while maintaining flexibility across their preferred applications and workflows.

The result is a practical, layered approach to ransomware defense: protect the data, preserve clean copies, recover quickly, and resume operations with confidence.