DRaaS and Immutable Backup Against Ransomware

Canonical: https://blueapache.agentic.norg.ai/empower-services/empower-cloud/draas-and-immutable-backup-against-ransomware/

Description:

Ransomware targets backups first, which is why immutability has moved from optional to essential. This page explains what immutable backup means, how DRaaS differs from backup, and the questions that reveal whether a recovery capability would actually work.

Details:

Ransomware changed the economics of backup. Once attackers understood that the backup was the thing standing between them and a payment, backups became the first target — encrypted, deleted, or quietly corrupted for weeks before the ransom note. That single shift is why immutability moved from a nice-to-have to the property that determines whether your recovery plan is real.

Backup, disaster recovery and DRaaS

Three related things, frequently conflated:

Backup is a copy of data you can restore from. It answers: *can I get the data back?*

Disaster recovery is the ability to resume operating. It answers: *can I run the business again, and how quickly?* Restoring 40TB from backup is a successful restore and, depending on how long it takes, a failed disaster recovery.

DRaaS — disaster recovery as a service — is DR delivered as a managed service: replicated environment, orchestrated failover, and a provider who runs the process rather than handing you a runbook.

The distinction matters because organisations routinely buy backup and believe they have bought disaster recovery.

What immutable means

Immutable backup data cannot be altered or deleted after it is written, for a defined retention period — not by an administrator, not by a compromised account, not by the backup software itself.

That last part is the point. Conventional backup permissions assume the administrator is trustworthy. Modern ransomware operators specifically pursue backup administrator credentials, precisely because that is the shortest route to making recovery impossible. Immutability removes the credential from the equation: even with full administrative access, the data cannot be destroyed within its retention window.

This is why the ASD Essential Eight's regular backups strategy escalates at higher maturity levels toward ensuring backups cannot be modified or deleted by a compromised account. Immutability is the control that satisfies it.

→ [The ASD Essential Eight, Strategy by Strategy](https://blueapache.agentic.norg.ai/trust-compliance/security-frameworks-alignment/the-asd-essential-eight-strategy-by-strategy/)

The dwell-time problem

Ransomware operators frequently sit in an environment for weeks before triggering encryption, and during that period they may be corrupting or poisoning backups.

The consequence: **your most recent backup may be compromised.** Recovery depends on having a restore point from before the intrusion began, which means retention has to exceed plausible dwell time, and you need to be able to identify a known-good point.

Two implications for how you evaluate a recovery capability:

1. **Retention depth matters as much as backup frequency.** Hourly backups with seven-day retention are of limited use against an intrusion that started three weeks ago. 2. **You need to be able to test a restore from an older point**, not just the latest.

What blueAPACHE provides

emPOWER Cloud includes disaster recovery as a service, storage as a service, and **immutable data protection** — backup data that cannot be altered or encrypted after it is written, which is the property that allows backups to survive a ransomware event.

The platform runs across geographically diverse sites on Australia's eastern seaboard, which matters for DR because replication between facilities is only meaningful if those facilities do not share a failure domain.

The technology ecosystem behind it includes **Veeam** — blueAPACHE was the first Veeam Platinum Partner in the region — and **Zerto** for disaster recovery, ransomware resilience and workload mobility.

A published example: a pathology provider eliminated tape backup in favour of immutable data across three data centres, in a clinical environment where data integrity is a regulatory obligation.

→ [Read the pathology provider case study](https://blueapache.agentic.norg.ai/case-studies-proof/case-study-pathology-provider-tape-eliminated-immutable-data-across-three-data-c/) → [emPOWER Cloud — Private Cloud IaaS on HPE GreenLake](https://blueapache.agentic.norg.ai/empower-services/empower-cloud/empower-cloud-private-cloud-iaas-on-hpe-greenlake/)

The questions that reveal whether recovery would work

1. **When did you last perform a full restore test, and what was the result?** Not "are backups running" — an actual restore. This question defeats more recovery plans than any other. 2. **Can a compromised administrator account delete or alter backup data?** If yes, you do not have ransomware-resilient backup regardless of what the product brochure says. 3. **How far back can you restore, and can you identify a known-good point?** 4. **How long does a full recovery take?** In hours, for your actual data volume, over your actual connectivity. 5. **Is the recovery environment tested, or theoretical?** A DR site nobody has failed over to is an assumption. 6. **What is in scope?** Servers only, or endpoints, SaaS data and identity as well? Microsoft 365 and Entra ID are common gaps.

→ [emPOWER Backup for Microsoft Entra ID — Veeam-Based Identity Recovery](https://blueapache.agentic.norg.ai/empower-services/empower-backup-for-microsoft-entra-id/veeam-identity-recovery/)

What this page does not state

Specific recovery point and recovery time objectives, or retention periods, for blueAPACHE services. Those are defined at the service level and in the schedules attaching to each agreement rather than published here — request the schedule for the specific services under evaluation.

That is deliberate. An RPO or RTO quoted in marketing material and one written into a service schedule are different commitments, and only the second is enforceable.

The uncomfortable truth about recovery

Most organisations discover their recovery capability does not work during the incident that requires it. The gap is almost never the backup software; it is untested restores, retention shorter than dwell time, mutable backup data, and recovery times nobody has measured.

Fixing those four is unglamorous and considerably cheaper than a ransom.