HPE

eBook

THE NEED FOR SPEED IN CYBER RESILIENCE

Why recovery time is your competitive advantage

Get started →

Table of contents

The high stakes reality of recovery

We can all agree that downtime is not an option. Whether it's ransomware, hardware failure, or a compliance misstep, every second lost puts your business at risk — financially, operationally, and reputationally.

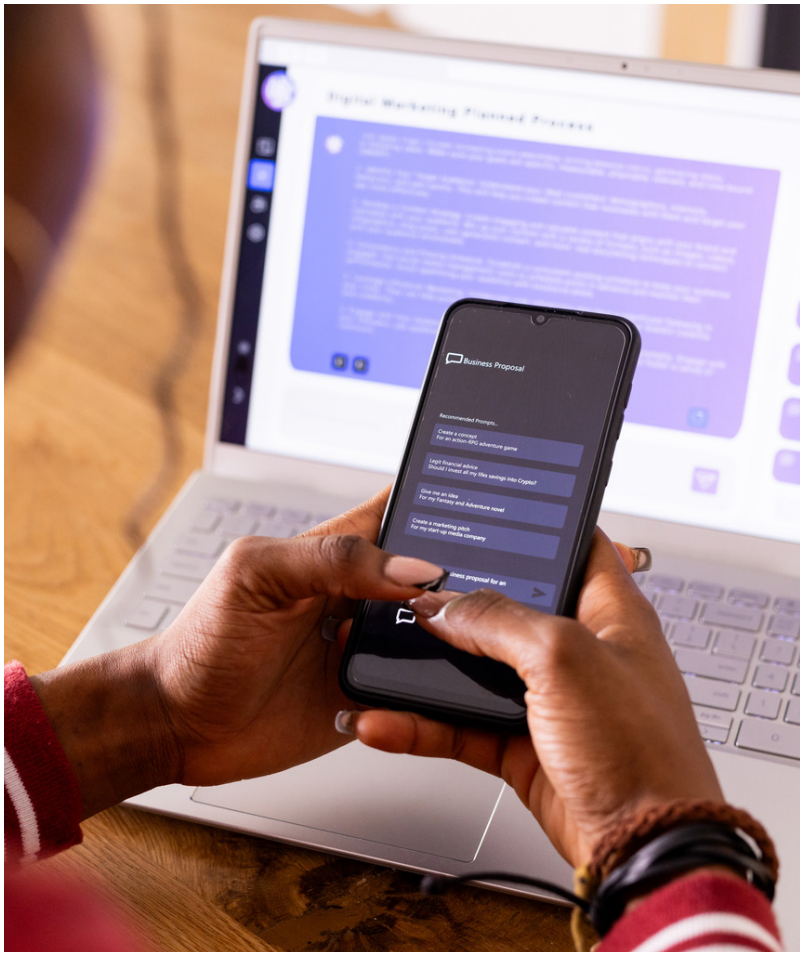
Some in the industry claim that RPOs and RTOs don't matter in a cyberattack, arguing that recovering too fast could make things worse. Others assume that because they have backups, they're protected. Let's be clear: That's not going to be fast enough.

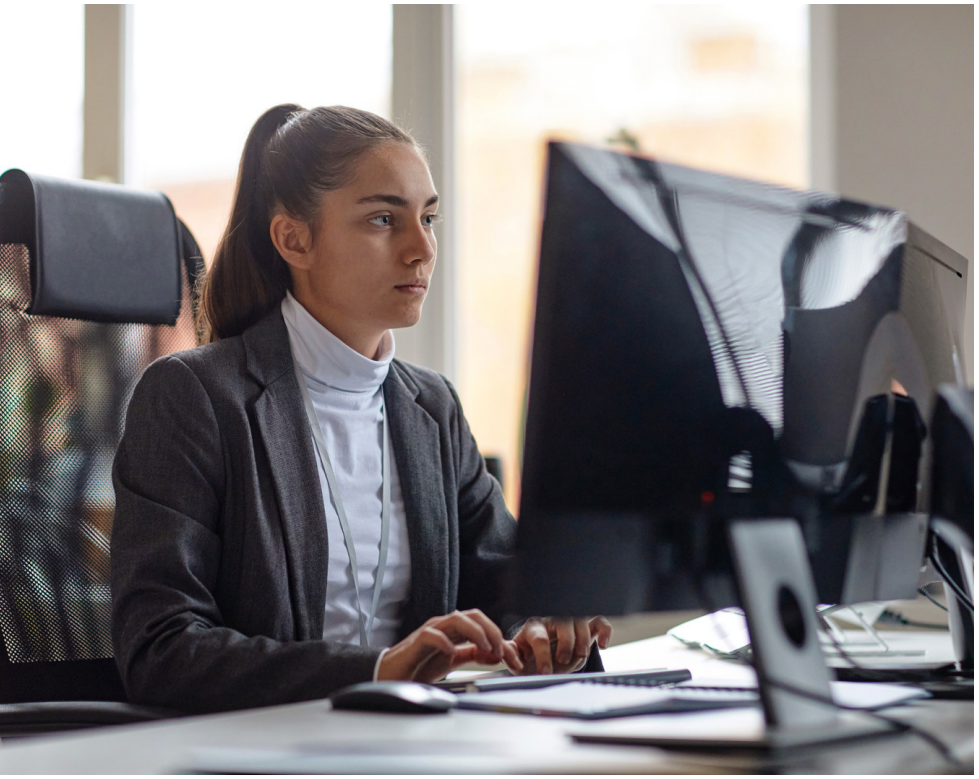
Traditional backups weren't built for today's threats because they're:

— Too slow
— Too fragmented
— Too vulnerable

If ransomware strikes, recovering from backups could mean hours or days of downtime, data loss, and corruption. In a world where attacks happen in seconds and compliance demands instant restoration, speed isn't optional. You shouldn't have to choose between acting quickly and trusting your recovery. True resilience demands both.

Debunk the myths around backup and slow recovery and learn how businesses can achieve both speed and trust with modern disaster recovery.





Slow recovery can pose a bigger threat

If speed doesn't matter, then why does every second of downtime cost thousands of dollars? Certain vendors argue that aiming for "super-fast recovery" can be risky or that recovery point objectives (RPOs) and recovery time objectives (RTOs) lose their significance during a cyberattack. Conversely, some believe that simply having a backup is enough. However, if speed is not a critical factor, why does each second of downtime result in substantial financial losses?

Let's break down the reality.

Backup ≠ disaster recovery

Many organizations still rely on traditional backups, thinking they're covered. But here's the problem:

— **Backups are point-in-time snapshots.** If ransomware hits, your last backup could be hours or days old, leaving massive data gaps.

— **Restoring from backup is painfully slow.** Large datasets can take hours or even days to restore, delaying your return to operations.

— **Backups can be compromised.** 94% of organizations report ransomware attackers target backups. If your production data is at risk, so are your backups.[1]

— **Backups are for retention, not resilience.** Disaster recovery must be measured in seconds, not hours, because when an attack happens every moment counts.

	Primary purpose	Recovery time (RTO)	Recovery point (RPO)	Automation	Ransomware protection
Backup	Data retention and compliance	Hours to days	Hours or daily snapshots	Manual restores required	Vulnerable (backups targeted)
Disaster recovery (DR)	Business continuity and uptime	Minutes	Seconds (real-time protection)	Instant failover	Fast rollback to clean data

The takeaway? If your only recovery strategy is backup, your business is not truly resilient.

[1] The Impact of Compromised Backups on Ransomware Outcomes.

RPOs and RTOs aren't optional

When disaster strikes, every second counts. Yet some vendors suggest you don't need guaranteed RPOs and RTOs. That's like saying you don't need a fire extinguisher because it's better to rebuild carefully after the flames die down.

The takeaway? If you can't recover quickly and confidently, your business is at risk.

With **continuous data protection (CDP) from HPE Zerto Software:**

— **RPOs are measured in seconds** — Minimal data loss
— **RTOs take minutes** — Not hours or days
— **Quick rollbacks enable clean recovery** — No need to choose between speed and trust

You shouldn't have to choose between acting quickly and trusting the integrity of your recovery. True resilience demands both.

"Before [HPE] Zerto, we were always afraid of risk. Now, after [HPE] Zerto, we can mitigate the risks of attacks and migrations."[2]

– **Carlos Barrios Hernandez**, Director HPC Center, Universidad Industrial de Santander

[2] UserEvidence

The high cost of downtime

When you can't recover instantly and confidently, the risks multiply.

1.

Financial losses

— $14,056 per minute[3] — This is the average cost of downtime ($843,360 per hour).
— $4.88 million[4] — This is the average cost of a ransomware attack.

2.

Compliance and legal risk

— GDPR, HIPAA, DORA, NIS2 — These regulations require rapid recovery or face fines.
— Failed audits — Regulators expect proof of resilience.
— Breach notifications — Slow recovery amplifies reputational damage.

3.

Competitive disadvantage

— Your competitors aren't waiting — These regulations require rapid recovery or face fines.
— Stock prices drop after cyber events — Regulators expect proof of resilience.

[3] BigPanda/Enterprise Management Associates IT Outages: 2024 costs and containment.
[4] The Cost of data breach.

The takeaway? Your business doesn't just need recovery, it needs recovery at the speed of today's threats.

The false choice: speed vs. trust

Some say, "If you're too hasty and recover too fast, you can make matters worse." But does recovery speed really put your data at risk?

— **Ransomware doesn't wait**. Attackers move fast, encrypting data in seconds. The longer recovery takes, the more time threats have to spread and increase damage.

— **Slow recovery doesn't mean safer recovery**. It means delayed response, longer downtime, and more uncertainty while you scramble to find clean data.

— **Faster recovery into an isolated environment, the faster remediation**. Containing the blast radius is critical. The longer you wait, the harder it becomes.

— **Speed and trust aren't opposites**. True resilience means recovering fast and with confidence, knowing you're restoring clean, uncompromised data.

The truth? Slow recovery isn't safer, it's riskier.

Recovery built for speed

Unlike legacy solutions that force you to choose between fast recovery and data integrity, HPE Zerto delivers both.

- **RPOs of seconds and RTOs of minutes:** Recover near-instantly by rewinding and resuming from any clean point in time.
- **Immutable recovery copies:** Leverage the HPE Cyber Resilience Vault or S3 compatible storage. Ransomware can't encrypt what it can't touch.
- **Rapid failover and rollback:** Fail over in minutes, roll back in seconds with no manual rebuilds or risk delays.
- **Ready-made for compliance:** Get automated, audit-ready reports for DORA, NIS2, HIPAA, and more. Prove compliance in seconds, not hours.
- **Ransomware detection:** Built-in anomaly detection alerts you within seconds of suspicious encryption activity.
- **Multicloud mobility:** Replicate anywhere: on-premises, to/from/within the cloud, or across multiple combinations simultaneously.
- **Software-only hypervisor-based replication:** Gain always-on protection with no infrastructure lock-in for complete flexibility.
- **Multisite visibility across HPE Zerto deployments:** HPE Zerto analytics provides real-time, unified visibility of protection and recovery across your applications.

Accelerating resilience across industries

Slovenj Gradec General Hospital needed a disaster recovery solution that reduced downtime, mitigated ransomware risk, and provided continuous patient care. With medical systems at stake, a slow recovery could mean delayed treatments and loss of critical patient data.

— Near-zero data loss
— Rapid recovery
— Seamless scalability

"The most important thing for our doctors, nurses, and patients is that all systems implemented work constantly, without disruptions."

– **Dr. Janez Lavre**, MD, CEO, Slovenj Gradec

TenCate Protective Fabrics, a global textiles company, learned the cost of slow recovery firsthand. After a ransomware attack before implementing HPE Zerto, they lost 12 hours of data and took two weeks to recover. But after deploying HPE Zerto, the next attack had a different outcome.

— Ransomware recovery in minutes
— Seamless cloud mobility
— Confidence and control

"During the last attack, I was actually laughing during recovery. I knew I had a way out, I was confident, and my heart didn't sink."

– **Jayme Williams**, Senior Systems Engineer, TenCate

The Mississippi Department of Revenue needed to ensure statewide tax processing, vehicle registrations, and essential services remained operational, even in a disaster. Their old solution required manual tape-based recovery, taking multiple days. With HPE Zerto, that changed.

— RPOs of seconds, RTOs under an hour
— Disaster recovery testing
— Seamless scale for public sector needs

"Taking two to three hours to recover is not fast enough for us ... [HPE] Zerto is my silver bullet for those situations that pop up where I need to perform a miracle."

– **Mike Dehaan**, Infrastructure Service Manager and Enterprise Architect, Mississippi Department of Revenue

Can your recovery keep up?

For organizations where downtime isn't an option, HPE Zerto delivers speed you can count on and recovery you can trust.

If your disaster recovery solution can't match the speed of modern threats, your business is already at risk. So, ask yourself:

— Are we recovering in minutes, not hours or day?

— Can we restore from an attack with confidence?

— Is our data protected against ransomware encryption?

If not, it's time to rethink your disaster recovery strategy.

Learn more at

HPE.com/zerto-software

Visit HPE.com

Chat now

a00147514ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com