TECHNICAL PAPER 05

The last clean point

05

Restoring after ransomware is not the same as restoring.

> After an attack, the hard question isn't "do we have backups?" It's "which one is clean, and how much work do we lose by going back to it?" ImmuBDR answers both before you have to ask.

Every restore point is examined

Each new restore point that reaches our data centre is compared with the one before it. The platform looks for the traces that attacks actually leave, and ignores the noise of normal updates. Signature and rule-based scanning run alongside.

Everything is examined directly from the backup data: nothing is mounted, and nothing touches the protected system. The detection was developed together with Maastricht University.

Suspicion changes behaviour

A suspicious restore point doesn't just raise a flag. It holds the last clean point so retention can never remove it, marks the system, and raises a critical alert that stays until an Immutec engineer has reviewed it.

An attacker who has been inside for weeks, waiting for your clean backups to age out, finds that they don't.

Clean restore: go back, without losing everything since

Going back to the last clean point usually means losing every legitimate file created after it. ImmuBDR offers a third option.

> A clean restore starts from the last clean point, then adds only the new user files from later points that show no sign of the attack. Each file is checked again right before it is added. **If a scanner is not running, the restore stops rather than proceeding unchecked.**

The result is a system that is clean and as current as it can safely be.

And it’s provable

Combined with weekly DR tests and immutable, time-locked storage, we can show exactly which points were clean, which were held, and that the restore chosen actually boots and serves.

ABOUT IMMUBDR

ImmuBDR is Immutec’s backup and disaster-recovery platform, delivered as a fully managed service. It protects virtual machines, physical servers, databases and file shares, keeps every restore point verified and immutable, and recovers them on our own infrastructure, even when your own hypervisor or site is gone.

Our engineers run the platform for you. Customers have no access to backup or restore functions; every request runs through a ticket. Your production and your recovery are held by different people, by design.

Need the technical detail? A full version of this paper is available under NDA.

Proven weekly	Immutable	Own infrastructure
Every system booted and tested, with evidence.	Time-locked restore points nobody can release early.	Storage, DR capacity, network and AI, run by us.

Want to see a failover live? Ask us for a demo. www.immutec.ae