Quarantine for AWS Backups

Isolate Infected Recovery Points Before They Spread

Elastio's Quarantine feature for AWS Backup automatically isolates infected or suspicious recovery points, ensuring ransomware-free recoverability.

The Quarantine feature from Elastio adds an essential layer of data integrity to AWS Backups. By automatically validating, isolating, and managing recovery points based on real scan results, Elastio helps ensure that your last known clean copy is always ready, safe, provable, and recoverable.

Why Quarantine Matters More Than Ever
Malware detection alone isn't enough. Attackers now bypass EDR tools and compromise backups quietly, leaving infected restore points hidden until recovery.

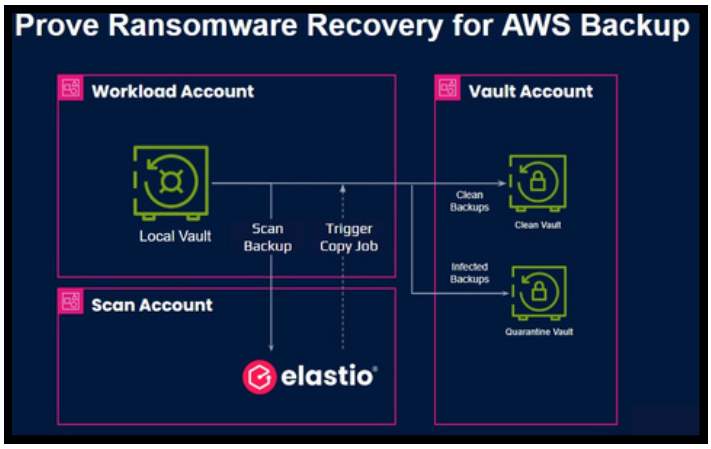
To restore with confidence, organizations need provable recovery—proof that backups are clean, recoverable, and compliant.

Elastio delivers that proof with an agentless recovery control that continuously validates backups, identifies the last known clean point, and turns recovery integrity into verifiable evidence.

Efficient scans are critical — but more importantly, provable clean recovery eliminates the leverage ransomware has and satisfies board-level and compliance demands. Elastio and AWS ensure your backups aren't just stored – they are validated, resilient, and ready for recovery.

What Is Quarantine for AWS Backup?
Elastio Quarantine is a feature that automatically isolates infected or suspicious backup points, preventing reinfection and preserving forensic evidence. It ensures your clean vaults stay clean and your recovery chain remains trusted—so you can restore safely, with proof.

Control your recovery ›› elastio.com



How It Works: Elastio automatically scans backups in your Local Vault and routes them to the right destination—clean backups are secured in your Safe Vault, while infected ones are quarantined for analysis.

1. **Backup Created:** AWS Backup writes the recovery point to your default vault.
2. **Automated Scan:** Elastio scans it using detection engines that look for signs of encryption, corruption, and malicious behavior.
3. **Clean Backups Promoted:** When a scan confirms a backup is clean, it's automatically copied to your Safe Vault (e.g., LAG/Bunker), becoming part of your verified, provable recovery set.
4. **Infected Backups Quarantined:** When a scan confirms a backup is clean, it's automatically copied to your Safe Vault (e.g., LAG/Bunker), becoming part of your verified, provable recovery set.
5. **Forensic Analysis:** Your IR or Security team can safely access quarantined data to trace root cause, timeline, and attacker behavior—without risk to production.

By combining Elastio with AWS, Elastio transforms recovery from a potential weak link into a security control you can count on.