CYBERLENCE

CYBERLENCE IN ACTION

Adaptive Application Recovery

Backups protect data. They don't restore operations. 84% of C-suite leaders report experiencing a cyber incident in the past three years — 39% of breached organizations reported ransomware, up from 34% the year before — and only 42% of them say they've fully recovered: operations normal, obligations met, trust restored. Recovery runbooks are static: built for the application you had and the incident you'd already seen, so when either changes, teams fall back to trial and error.

CONTINUOUS RECOVERY VALIDATION

Recovery That's Proven Before You Need It

Cyberlence treats recovery the same way it treats production — continuously discovering, protecting, and testing every application, not just the one that made it into last year's DR plan.

CYBERLENCE SOLUTION

One Recovery Capability. Every Scenario.

Cyberlence continuously discovers your application, protects it to your RTO and RPO targets, and validates recovery with non-disruptive testing — the same loop for a DR test, a ransomware recovery, a forensic investigation, or a live failover. No manual runbooks, no once-a-quarter fire drill.

CONTINUOUS READINESS, NOT ANNUAL DRILLS

Discovery and protection run continuously in the background, so recovery is validated constantly — not proven for the first time when an incident hits.

RECOVER WITH PROOF, NOT PROMISES

Every recovery logs its trigger, duration, and RTO/RPO achieved — evidence produced by recovering, not assembled afterward for an auditor.

CUSTOMER BENEFIT

What Your Team Gets

Fast, Automated Recovery: Recovery orchestrated to meet your RTO and RPO targets, executed human-in-the-loop or fully automated — your choice.

Application Recovery, Not Component Recovery: Cyberlence restores the full business service — app, data, and dependencies together — not just the database or VM that traditional backups protect.

Measurable Resilience: A recovery readiness score, tracked continuously and ordered by business criticality — evidence for the board, not a claim.

Turn resilience from a once-a-year audit exercise into a continuously validated business capability.

Sources: [1] EY, 2025 Cybersecurity Study: Bridging the C-suite Disconnect. [2] IBM, Cost of a Data Breach Report, 2026.

© 2026 Cyberlence. All rights reserved.