FLEXENTIAL

Managed cyber-resilient recovery infrastructure

Protect recovery data and preserve validated recovery capability with Flexential Backup-as-a-Service (BaaS)

When ransomware, credential compromise, infrastructure failure, or operational disruption affects production, recovery infrastructure becomes a critical operational dependency. Attackers target backup repositories, identity systems, and administrative credentials because compromised recovery options increase disruption and extortion leverage. Recovery readiness therefore depends on more than completed backup jobs. It requires recovery data and supporting controls that remain protected, reliable, and operationally usable when production systems are compromised.

Flexential Backup-as-a-Service (BaaS) provides managed, cyber-resilient recovery infrastructure designed to protect recovery data, validate recoverability, and maintain reliable recovery capability. It combines immutable architecture, logical isolation, independent administration, governance controls, recoverability validation, and 24x7 managed operations across cloud, colocation, and hybrid IT environments.

Key recovery challenges

Organizations face increasing recovery risks that extend beyond backup creation:

- Backup repositories are targeted during ransomware and cyber extortion events
- Successful backup jobs do not prove that recovery data remains recoverable
- Compromised credentials and administrative accounts can expose recovery infrastructure
- Recovery processes may depend on systems, identities, or services that are unavailable during an incident
- Governance, compliance, and cyber insurance initiatives increasingly require immutable, and validated recoverable data
- Internal teams often lack the capacity required to continuously operate, monitor, and validate a hardened recovery environment

Why recovery readiness matters

Recovery capability increasingly determines whether organizations experience manageable disruption or prolonged operational, financial, and business impacts.

- Ransomware was involved in 48% of breaches analyzed, up from 44% the prior year
  - Verizon 2026
- 89% of ransomware victims had their backup repositories targeted
  - Veeam 2025
- 76% of organizations suffering a material cyberattack exceeded their RTO, with recovery taking, on average, nearly 2× longer than planned
  - Cohesity 2026
- Only 28% of ransomware-affected organizations fully recovered all affected data
  - Veeam 2026
- Average ransomware recovery costs reached $2.51 million for U.S. organizations, excluding the ransom payment
  - IBM 2026

Recovery and resiliency outcomes

Flexential BaaS helps organizations reduce the risk of extended operational disruptions:

- **Preserve reliable and validated recovery capability** during ransomware, cyber incidents, and operational disruptions
- **Reduce attacker leverage** by protecting data and recovery infrastructure from tampering, compromise, and unauthorized deletion
- **Improve confidence that recovery points remain usable and available when recovery is required**
- **Strengthen governance** through controlled administrative actions and documented operational processes
- **Support availability, resilience, cyber insurance, audit, and compliance initiatives** through validation, retention, and recovery testing capabilities
- **Reduce the operational effort** required to operate, monitor, and maintain recovery infrastructure
- **Establish consistent recovery readiness** across distributed hybrid IT environments

Cyber-resilient recovery architecture

Flexential BaaS addresses four requirements for dependable recovery: backup survivability, recoverability validation, recovery governance, and continuous managed operations. Together, these controls protect the recovery environment, validate the integrity and usability of recovery data, govern high-risk administrative actions, and support trusted recovery capability when production systems, identities, or administrative credentials are compromised.

Capability	Key features	Operational function	Business and operational outcomes
Backup survivability	Immutable backup architecture, logical air-gap separation, dual-domain isolation, independent backup control plane, protected administrative access model, and encryption in transit and at rest.	Protects recovery data and administration from ransomware, credential compromise, unauthorized changes, and destructive actions.	Maintains reliable recovery capability when production environments, credentials, or operational systems are compromised.
Recoverability validation	Daily CRC validation checks, automated data verification, restore testing capabilities, recoverability validation, and recovery readiness support.	Validates recovery data integrity and supports testing to confirm that data remains usable and recoverable.	Improves confidence that validated recovery points are usable when restoration begins.
Recovery governance	Dual-administrator deletion approval, multifactor administrative controls, policy-driven retention, documented change management, optional customer deletion restrictions, and authorization controls for destructive actions.	Governs administrative actions, retention, change activity, and destructive operations across recovery assets.	Reduces risk exposure to credential compromise, accidental deletion, malicious actions, and uncontrolled changes.
Managed operations	24x7 monitoring and management, self-service recovery options, cloud, colocation, and hybrid IT support, flexible retention policies, scalable protection architecture, and no ingress or egress fees.	Provides continuous monitoring and management across distributed recovery environments with flexible protection and recovery options.	Reduces operational burden and supports consistent recovery readiness across hybrid IT environments.

Why Flexential and our NIST CSF 2.0-aligned Cyber Resiliency portfolio

Most organizations already have backup software. The challenge is maintaining a recovery environment and data that stays protected, reliable, and usable when production systems or administrative access are disrupted.

Flexential brings infrastructure, security controls, recoverability validation, and 24x7 operational management together in one managed service, helping teams protect recovery assets, reduce operational risk, and maintain recovery readiness.

Learn more about Flexential Backup-as-a-Service. Flexential BaaS is part of the Flexential NIST CSF 2.0-aligned Cyber Resiliency Portfolio to successfully identify, protect, recover, and govern your IT assets.