Top 4 ways to secure your data for clean, reliable recovery

Data is vulnerable to countless threats, from cyberattacks and hardware failures to natural disasters. A robust, multilayered backup strategy protects your data, ensures business continuity, reduces the risk of data loss, and strengthens your overall security posture.

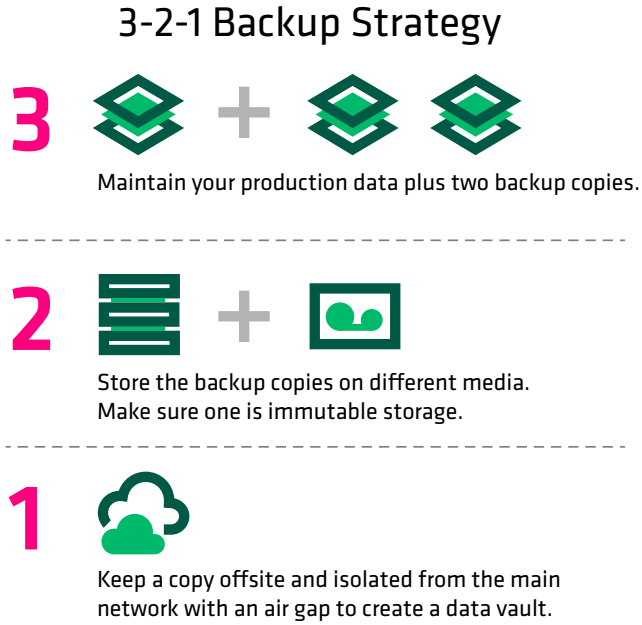
Here are four security posture measures that help ensure your data is always clean and recoverable.

1. Implement access control and authentication

- **Ensure only authorized users can access your data.** Adding an extra layer of security is essential in protecting against both internal and external threats. Enabling multifactor authentication (MFA) everywhere is an effective means of protecting against these threats, along with maintaining your existing identity and access management policies.
- **Limit access and permissions based on user roles.** Apply role-based access control (RBAC) to provide limited, granular access and permissions for the users in your backup environment based on their specific role. This helps ensure that each person has only the minimum access privileges required to fulfill their responsibilities.

2. Prioritize data protection and integrity

- **Implement an immutable data vault.** To keep your data safe from tampering, consider using Cohesity NetBackup Flex Appliance or Cohesity FortKnox for secure and tamper-resistant immutable storage on-premises or in the cloud.
- Implement a 3-2-1 backup strategy for critical workloads. Maintaining three copies of data on two different media, with at least one copy stored offsite on immutable and indelible storage, provides data redundancy and helps ensure your data is always recoverable.
- Prevent data exfiltration with strong encryption. Protect data from unauthorized access during transmission and storage. To prevent unauthorized access and data theft, use strong encryption for all your data, whether it's stored on-premises or in the cloud.



3. Take advantage of security monitoring and detection

- Use automation for intelligent detection of user threats. Our adaptive risk engine continuously monitors user behavior for suspicious activities. Upon detecting anomalies or other suspicious user actions, the platform will autonomously initiate security actions—such as multifactor authentication—to lock down access to backup data.

- Accelerate threat identification and response. Cohesity provides rapid threat hunting capabilities that proactively search for indicators of compromise and respond to threats. We also offer a complete blast radius analysis of affected areas across the entire environment—up to 93% faster than traditional malware scanning.

4. Harden your system configuration

- **Create a Digital Jump Bag.**™ A Digital Jump Bag is a protected and trusted repository that provides rapid access to the tools needed for remote acquisition and analysis. It contains the tools, software, configuration files, and documentation needed to respond to an incident in a vaulted immutable store—beyond the reach of adversaries.
- **Reduce network exposure**. Implement Network Access Controls to restrict network access to backup systems and data and prevent unauthorized access. Easily segment your network and create a Clean Room environment to enhance security and help minimize the impact of any potential security breaches.
- **Implement Clean Room data recovery**. Create a separate, secure environment for forensic and recovery operations to minimize the risk of contamination.
- **Keep all systems and software updated**. Regularly update software and install security patches to take advantage of new features and improved security measures.

Share these guidelines with your team and encourage them to implement these crucial steps to protect your organization's data and strengthen your security posture.

For blueprints and best practices for architecting a backup environment for your organization, read *Modern data security and management topologies: A guide for IT leaders*.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

9100085-001-EN 6-2025