

Achieving Cyber Resilience – Data Immutability – L1

Ability to Ensure Immutability of Backup Data

Backups are the last line of defense in cyber incident recovery, which is why it's crucial to ensure that backup copies are both immutable and stored in air-gapped locations. Data immutability guarantees the availability and integrity of your backups, forming the bedrock of your organization's cyber resilience. With secure, immutable backups in place, organizations can confidently assure recovery when it matters most.

To further strengthen recovery efforts, follow the 3-2-1 backup rule: maintain three copies of your data on two different media types, with one copy stored off-site. This approach ensures both data availability and integrity, safeguarding against potential loss. Reliable access to backups is essential for effective recovery, and adhering to the 3-2-1 rule positions your organization for success in future recovery stages.

Once your backup systems are secure and isolated, you'll be better prepared for clean data recovery, minimizing the risk of reintroducing threats into your environment. This critical step helps ensure your recovery process is both thorough and effective, protecting against future vulnerabilities.

Druva Can Lead You to Cyber Resilience

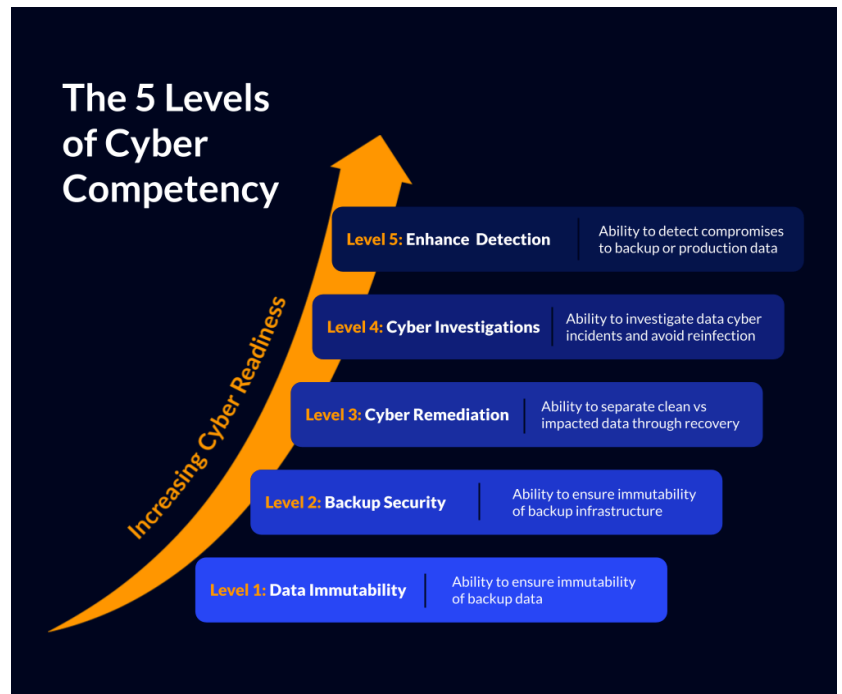
While backup immutability is essential, it isn't enough for full cyber resilience. If an attack affects both production and backup servers, recovery can be compromised. The second level of the maturity model emphasizes securing not just backup data, but also the backup infrastructure. This ensures that your backup systems are **well-secured and isolated**, reducing the risk of failure in the event of a cyberattack. This is critical for **quick recovery**—without it, an attack that compromises both production and backup environments could significantly delay recovery efforts.

By addressing these questions, you establish a secure, resilient foundation for recovery:

- Is your backup infrastructure isolated from production systems?
- Is your backup environment continuously monitored for security?
- How do you manage root access and MFA for backup systems?

Strengthen Cyber Resilience with Druva

Druva's Data Security Cloud provides a robust, cloud-native platform that addresses critical gaps to make your organization cyber resilient. Built on secure AWS infrastructure and using a zero-trust security model, it delivers comprehensive protection to help organizations advance through every level of cyber competency.



druva Sales: +1-800-375-0160 | sales@druva.com

Americas: +1-800-375-0160
 Europe: +44 (0) 20-3750-9440
 India: +91 (0) 20 6726-3300

Japan: japan-sales@druva.com
 Singapore: asean-sales@druva.com
 Australia: anz-sales@druva.com

Druva is the leading provider of data security solutions, empowering customers to secure and recover their data from all threats. The Druva Data Security Cloud is a fully managed SaaS solution offering air-gapped and immutable data protection across cloud, on-premises, and edge environments. By centralizing data protection, Druva enhances traditional security measures and enables faster incident response, effective cyber remediation, and robust data governance. Trusted by over 6,000 customers, including 65 of the Fortune 500, Druva safeguards business data in an increasingly interconnected world. Visit druva.com and follow us on [LinkedIn](#), [Twitter](#), and [Facebook](#).