Achieving Cyber Resilience — Backup Security — L2

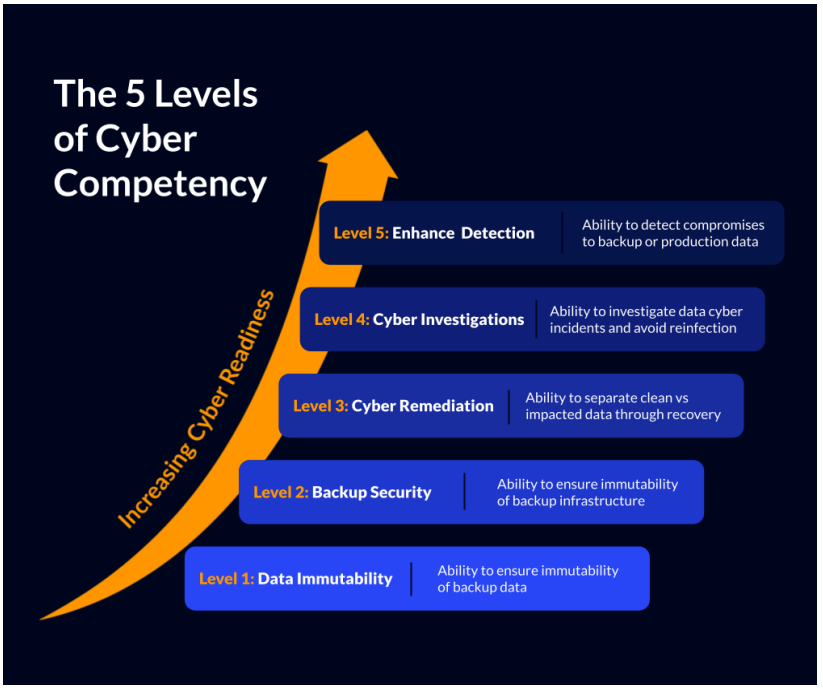
Ability to Ensure Immutability of Backup Infrastructure

While immutable backups are crucial, they alone don't provide full cyber resilience. If an attack impacts both production and backup servers, recovery could still be jeopardized. The next level of the maturity model focuses on securing not just backup data, but the entire backup infrastructure. This means implementing robust security measures to protect backup systems, ensuring that they are isolated, monitored, and resilient against threats—much like your primary servers.

Safeguarding Access: It's vital to enforce strong root access controls and use multi-factor authentication (MFA) for backup systems to prevent unauthorized access and reduce the risk of compromise. By addressing these challenges, you're laying the groundwork for the next phase, where comprehensive investigation and proactive monitoring become essential. This will ensure that your systems are not only recovered but also fortified against future threats.

Druva Can Lead You to Cyber Remediation

After securing your backup infrastructure, focus on effective cyber remediation to ensure a clean recovery with minimal data loss. Quick recovery is crucial, so organizations need a tested recovery plan for efficiency. This ensures you can recover quickly while maintaining data integrity. This **clean recovery** capability is vital for restoring operations after an attack without compromising security. However, securing a clean recovery environment is just part of the process.



As your organization masters clean data recovery, you'll be poised for the next phase: **investigating data breaches** and preventing **reinfection**. This will involve delving into cyber incidents to piece together what happened, ensure compliance, and ensure that your recovery remains intact.

Key questions for your team:

- Do you have a strategy to identify clean data and avoid reintroducing threats?
- How do you manage rollback processes for deleted backups?
- How do you identify the safest restore point to minimize data loss?

Strengthen Cyber Resilience with Druva

Druva's Data Security Cloud provides a robust, cloud-native platform that addresses critical gaps in incident response and recovery workflows. 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.