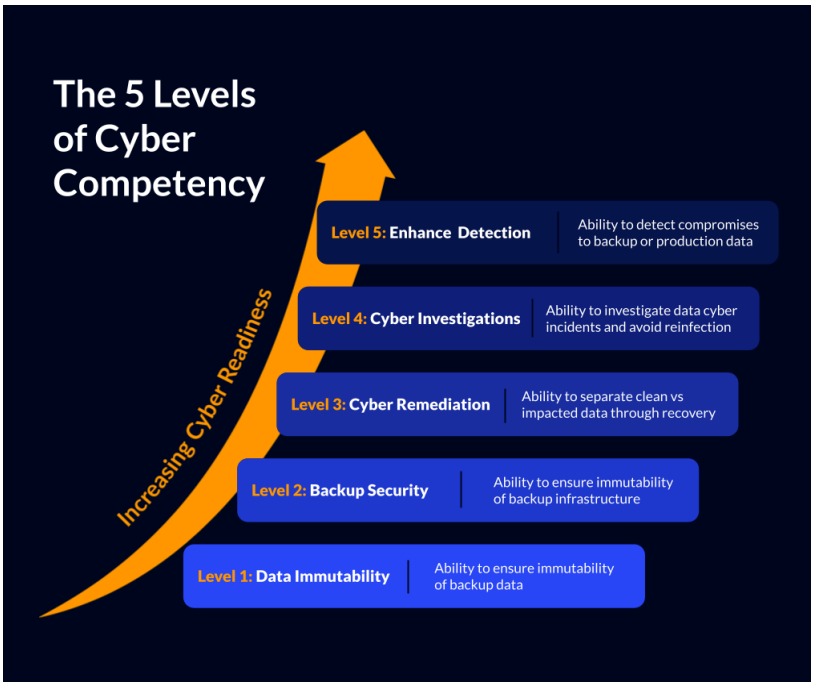
Achieving Cyber Resilience — Enhance Detection — L5

Ability to Detect Compromises to Backup or Production Data

After strengthening your cyber investigation capabilities, the next focus should be on enhancing threat detection, particularly around backups. Attackers often target backups by deleting, encrypting, or altering retention policies to obstruct recovery efforts. Detecting these threats early is key to reducing dwell time and limiting the damage caused by attacks. It's essential to implement robust methods for identifying compromises in both backup and production data to improve overall threat detection and reduce potential risks.

Detecting Compromises: Organizations must develop strategies to detect compromises in both backup and production data. When attacks encrypt primary data, Security Operations Center (SOC) teams may lack crucial insights into the scope and timeline of the threat. At Level 5, you're not only ensuring the integrity and security of your backup systems, but you're also safeguarding your entire data ecosystem. This level of preparedness minimizes risks, limits damage, and ensures your systems are always primed for a quick, clean recovery. This establishes a strong foundation for a continuous, proactive security strategy moving forward.



Druva Can Lead You to Cyber Remediation

Reaching **Level 5** means your organization has a mature, proactive cybersecurity strategy, with advanced tools and processes in place to not only recover from cyber incidents efficiently but also to detect and prevent attacks before they cause significant harm.

Key capabilities include:

- **Early Detection of Compromises**: Sophisticated monitoring tools that detect suspicious activities in both backup and production environments, including unauthorized changes or encryption of data.
- **Proactive Threat Hunting**: Using backups and other security data to continuously search for **Indicators of Compromise (IOCs)**, even before an incident is fully identified.
- **Minimizing Dwell Time**: By detecting threats early, your team can respond faster, reducing the time attackers have to linger in your systems and limiting the impact of the attack.
- **Integrated Threat Detection Across Environments**: Monitoring and alerting systems are integrated to ensure that any signs of a breach in either production or backup systems are flagged immediately, enabling rapid action to contain the attack.

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.