

Securing Your Last Line of Defense

Backup Environment Access Considerations

The threat of cyber crime is everywhere, and too often, the perpetrators succeed. Even the most security-hardened organizations can fall prey. If it happens to you, you'll have to rely on backups to restore your precious data. As such, backup is your last line of defense against a cyber attack.

That's why we've created this series on how to assess your vulnerability and make sure your backup environment is impenetrable. Each installment will identify a key area to assess, explore why it should matter to you, provide questions to help you start your assessment, and identify key technologies that can close the gaps.

To get started, we'll talk about access to the backup environment. Let's get into it!

Why Does This Matter?

Creating backups is a vital part of any data protection strategy, but it's equally important to safeguard those backups against unauthorized access and cyber attacks. Without strong controls in place, your backups — intended as a safeguard — can quickly become a liability.

Unauthorized access to backups can have far-reaching consequences, including data breaches, financial loss, and regulatory penalties. In fact, cyber criminals increasingly target backup systems, knowing they hold the keys to an organization's ability to recover from an attack. Successful intrusions can result in:

- **Data breaches:** Exposing sensitive information and damaging your organization's reputation.
- **Compromised backups:** Preventing recovery by encrypting or deleting data, leaving businesses with few options but to pay a ransom.
- **Regulatory noncompliance:** Impeding implementation of strict data protection measures, including secure backups, to meet regulations such as GDPR, HIPAA, and PCI DSS.

The Change Healthcare ransomware attack is a striking example of the devastating real-world consequences of poor backup access controls. Attackers infiltrated the backup environment due to weak authentication measures: a user account without multifactor authentication. The attack delayed critical health care services, exposed sensitive records of more than 190 million individuals, and forced the company's parent organization to pay a \$22 million ransom. Worse still, the attack eroded public trust and drew scrutiny from regulators investigating whether proper safeguards were in place.

Assessing Your Own Backup Access Security

As cyber threats continue to evolve and become increasingly sophisticated, it is more important than ever to prioritize the security of your backup environment. By asking the right questions and implementing advanced security measures, you can significantly enhance resilience against data loss, ransomware attacks, and regulatory noncompliance.

Are you asking the right questions about your backup environment?

To get an accurate picture of how secure it really is, here are three examples of things you should be asking during your evaluation:

1. Do you employ multifactor authentication to ensure that access is limited to authorized personnel only?
2. Does your backup product eliminate OpenSSH access and ensure no direct access to backup server components or data?
3. Is your environment designed with Zero Access® architecture, restricting access to critical systems and data?

Answering these questions can reveal gaps in your backup security posture, helping you to prioritize improvements. For more questions, you can download our free assessment questionnaire.

Addressing Security Gaps and Mitigating Your Risk

Securing your backup environment is an essential part of protecting your organization's data and maintaining business continuity. Why leave it to chance?

The Cobalt Iron Compass® SaaS platform tackles common vulnerabilities, empowering organizations to reduce risks and fortify their backup environments. The platform employs a variety of tools and strategies to enhance backup environment security.

- **Zero Access architecture:** Eliminates direct access to backup server hardware, software components, and backup data.
- **Robust Authentication:** Uses multifactor authentication, adding an extra layer of security to prevent unauthorized access even if credentials are compromised.
- **Operational automation:** Reduces human access to backups, minimizing vulnerabilities and simplifying operations.
- **Isolated security zones:** Establishes multiple, fault-tolerant security zones to protect your backup infrastructure.

These features align with best practices for backup security, offering a proactive defense against unauthorized access and malicious threats.

Fortifying Your Data Protection Strategy

Backup systems should be the cornerstone of your organization's cybersecurity strategy, not the weak link. Using a proven platform to ensure robust access controls, automate operations, and implement advanced architectures, you can transform your backups from a target into a trusted recovery solution.

Interested in learning more about securing your backup environment? [Download the Backup Environment Security Vulnerability Questionnaire](#) to assess your current posture and discover steps you can take to achieve more robust protection. Or, get in touch to [schedule a free backup security consultation](#) with experts from Cobalt Iron.