

Securing Your Last Line of Defense Backup Data Security

It's no exaggeration to say that a data breach could ruin your business — thus emphasizing the need for comprehensive security measures in backup strategies.

That's why we're bringing you this series about reducing your vulnerability. 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.

We've talked about considerations related to accessing your backup environment. Now let's talk backup data security.

Why Does This Matter?

You must treat your backup like the critical attack surface it is. Otherwise, it can't be the last line of defense or the recovery path you need when all your other data gets stolen or wiped away. A compromised backup is a useless backup.

Ransomware attacks targeting backups: Ransomware groups like Black Basta and BlackCat have exploited backup environments, encrypting both primary and backup data. If backups are poorly secured, attackers could plant malicious code during the compromise, which might execute if those backups get restored. Attacks on companies like Dish Network highlight the risks of insecure backup systems. And as recently as February, the [FBI issued a warning](#) about the Ghost ransomware campaign, which targets backups and exploits unpatched vulnerabilities in widely used software and firmware.

Data corruption and manipulation risks: Attackers targeting insecure backup environments might inject malicious payloads into the data. While such payloads would typically

require execution during a restoration or access process, the possibility underscores the need for securing backups with immutability and integrity checks.

The 2021 Kaseya VSA ransomware attack, orchestrated by the REvil group, is one example of a cyber attack involving malicious code executed from backup data. Exploiting a zero-day vulnerability in Kaseya's Virtual System Administrator software used by managed service providers, attackers deployed ransomware that infected both live data and backup files on thousands of downstream systems. The malware's ability to embed itself in backup workflows led to reinfection during recovery attempts, exacerbating the damage. This incident resulted in widespread data encryption, significant operational downtime, and substantial financial costs for affected businesses, with ransom demands ranging from tens of thousands to millions of dollars. The attack underscored the critical need for advanced malware detection in backup environments to prevent malicious code from spreading to backup files.

Consider this:

- Backups provide a false sense of security if they are not adequately protected.
- Malware in backup data can sabotage recovery efforts and prolong downtime.
- Failure to implement encryption of data leaves data exposed, putting the company at risk for regulatory fines, reputational damage, and litigation.

Assessing Your Own Backup Access Security

With so much at stake, how do you make sure your own backup environment will withstand an attack ... and bring your business back to life if need be? One way is to take a hard look at the characteristics of the backup data itself. Ask yourself the right questions about the backup data to determine just how secure it is, including:

1. Is your backup data inert (not actively used)?
2. Does your backup product perform data integrity checks on all data at ingest and recovery at both the block and file levels and during replication/copy events?
3. Is your backup data immutable, with additive ingest only to eliminate data overwrites, destruction, or mutation?

Inert data, integrity checks, and immutability are just a few ways to significantly reduce the risk of cyber criminals introducing malicious code into backup data or otherwise targeting it. Even if primary systems become compromised, you'll still have clean and unaltered backups available for recovery.

For more questions related to backup data security, you can download our free assessment questionnaire.

Addressing Security Gaps and Mitigating Your Risk

Armed with the information from your self-assessment, you can go about choosing a backup system that fits your situation.

The Cobalt Iron Compass® SaaS platform is engineered to resist attacks against backup data. It has features that let you answer yes to all the questions above, including:

- **Immutable storage:** Prevents data alteration.
- **Encryption at source, in flight, to storage, and at rest:** Protects data from unauthorized access by converting it into an unreadable format.
- **Data integrity checks at all phases of data protection:** Ensures data remains unaltered throughout its life cycle, from creation to storage and transmission.
- **Multiple, automatically managed copies of backup data:** Protects against data loss by maintaining multiple, up-to-date backups across diverse storage systems
- **Automated encryption key management and rotation:** Limits key exposure and ensures data remains protected.

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

Fortifying Your Data Protection Strategy

Secure backup data is crucial for cybersecurity because it provides a safety net against data loss from cyber attacks (not to mention system failures and human error).

Ready to learn 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.