

Data survival is foundational to any data recovery. Cybercriminals try to destroy it. Cybervaults can help ensure it.

How Cybervaults Can Ensure Absolute Data Survival and Enable Full Recovery

November 2025

Written by: Phil Goodwin, Research Vice President, Infrastructure Software Platforms, Worldwide Infrastructure Research, and Johnny Yu, Research Manager, Infrastructure Software Platforms, Worldwide Infrastructure Research

Introduction

Every day, organizations perform data recoveries from their backup systems. Most of these are "garden variety" recoveries, perhaps due to simple human error or other minor events. Other recoveries are more complex, perhaps as a result of hardware failures (servers, storage, or network disruptions), software errors, and so forth. Thus recoveries can involve as little as a single file or complete systems with hundreds of terabytes (TBs).

At the largest and most complex end of the scale, disaster recovery (DR) and cyber-recovery (CR) are often the most complicated recovery scenarios that IT organizations will face. The extent of the recovery can be significant, such as involving more than one datacenter, on premises or in the cloud. All such recovery situations occur under high stress and time pressure. Having access to known, clean backup copies can reduce this stress and enable organizations to recover rapidly.

IDC's research has found that fewer than one-third of organizations are able to fully recover from a cyber-attack without data loss and without paying the ransom. Moreover, about half of the attacks involve an attempt to delete, corrupt, or otherwise compromise the backup systems. If successful in these attacks on backups, the attacker is virtually assured of collecting a ransom when victims have no other options. Unfortunately, this tactic is successful about half of the time. Doing the math, this means one in four attack victims has no path to recovery using their own systems.

Cybervaults have emerged as a valuable tool to ensure data survival in the face of any attack or data loss scenario. Due to their typical deployment offsite, they protect data from natural disasters, fires, floods, or other events that make access to the datacenter impossible. They also give any organization a significant advantage in defeating ransomers.

The three core tenets of cyber-recovery are: ensuring data survival, ensuring data integrity, and ensuring rapid recovery. Cybervaults address the first two and facilitate the third. With a cybervault, recovery operations can begin faster when there's a guaranteed safe, clean, and accurate copy of data to recover from.

AT A GLANCE

KEY STATS

- » Fewer than one-third (31%) of organizations can fully recover from a cyberattack without paying the ransom.
- » In about half of all cyberattacks, the data backup systems are targeted first to render recovery impossible; attackers are successful in about half of these attempts.

WHAT'S IMPORTANT

When properly configured, offsite cybervaults are the best way to ensure data survival for both disaster recovery and cyber-recovery.

Unfortunately, too many IT teams are not familiar with the advantages of cybervaults and therefore don't utilize them. In fact, some are not aware of the necessity of storing data offsite. This paper discusses the advantages and imperatives of cybervault deployment.

Definition

A cybervault is a repository for backup data that incorporates encryption, immutability, and an air-gapped architecture to make data destruction or compromise nearly impossible.

Benefits

Organizations can implement cybervaults with hardware-specific systems, such as purpose-built backup appliances on premises. Alternatively, and perhaps more commonly, they can be implemented in the cloud utilizing hyperscaler resources. In detail:

- » Implementation of on-premises systems can require complicated configurations. Unless implemented with datacenter-to-datacenter replication, it may not satisfy offsite repository requirements. However, on-premises implementations may be necessary when data cannot be moved offsite.
- » IDC's research shows that more than 90% of organizations use a hybrid cloud (on premises to cloud) architecture for data protection. Therefore, implementing a cloud-based cybervault is normally a relatively painless extension of current capabilities.
- » The cybervault exists in an environment completely separated from production environments and the organization itself, adding another layer of defense.

Many organizations are familiar with a 3-2-1 backup strategy, which specifies three copies of data, on two different types of media, with one offline copy. This has been the best practice strategy for more than two decades. However, with the common use of cloud and increasing cyberthreats, a newer and more up-to-date 3-2-1-1-0 improves this strategy. The second "1" refers to an offsite copy, and the "0" refers to verified zero errors in the backup.

Cybervaults address the new components of the backup strategy: The second "1" would be an offsite vault to ensure data survival, with the "0" referring to the immutability of the data in that vault. Combined, these two ensure the backup data in the cybervault is recoverable and authentic.

Key cybervault functionality includes the following:

- » **Immutability:** Immutability ensures that data in the vault cannot be modified or deleted. This is essential for ensuring the integrity and survival of data.
- » **Encryption:** Data encryption ensures that data is useless, even if it is stolen. This is especially important because IDC's research has found increased occurrences of data exfiltration as a ransomware strategy. Encryption also thwarts threats from internal sources.
- » **Two-factor/two-person authentication:** Two-factor authentication helps to reduce the risk of individual credentials being used to gain system access. Two-person authentication requires two people to collude to illegally access systems, which reduces the incidence of insider attacks.

- » **Air gap:** An air gap is both a physical separation of data from its access and a separation of the control path and data path (i.e., different credentials to access each).
- » **Offsite location:** Unless mandated by data governance requirements, organizations should use an offsite location for vaulting. Offsite storage is especially important for disaster recovery scenarios.
- » **Maintenance of service-level requirements:** Cybervaults, by virtue of data integrity and availability, can contribute to maintaining the recovery point objective (RPO) and recovery time objective (RTO) service-level requirements of the organization.
- » **Data governance and sovereignty:** Properly configured data vaults support and maintain data governance and sovereignty requirements.

Considering Veeam Data Cloud Vault

Veeam Data Cloud Vault (Veeam Vault) is the company's fully managed, secure cloud storage resource. It includes durable storage, which leverages object storage and provides synchronous replication with 12 nines of availability. As a fully managed solution, IT administrators do not need to worry about configurations, compatibilities, integrations, or daily management and maintenance. Veeam Vault is integrated with Veeam Data Platform and Veeam Kasten, serving as a secure target for backups of traditional and modern workloads on premises and in the cloud.

Veeam Vault is based on a zero trust architecture to limit the ability of threat actors to access sensitive systems. It is immutable by default to prevent any attempts to modify or delete backups, whether maliciously or accidentally. It encrypts data to protect sensitive information and defeat data exfiltration attacks.

Veeam Vault can help organizations achieve the backup strategies described previously. At minimum, the copy of data within Veeam Vault fulfills the 3-2-1 requirements because it can be one of the three different copies, be one of the two different types of media, and be stored offline. However, by its nature, Veeam Vault also fulfills the full 3-2-1-1-0 strategy because the backup data is offsite, and its zero trust architecture and immutable storage enable verification of zero-error data stores.

Veeam Vault is available on Azure Marketplace or one of the thousands of Veeam channel and service provider partners. Pricing is based on a flat, per-TB rate and intended to be all-inclusive of implementation, system management, updates, and support.

Challenges

While Azure offers a worldwide datacenter presence and is one of the leading cloud providers, some organizations will have a preference for a different cloud hyperscaler. In some cases, they will want to replicate data across hyperscalers for added data safety or regulatory reasons. As Veeam considers future expansion of Veeam Data Cloud, adding support for more hyperscalers will be a necessary priority to meet these demands.

IT teams should also be aware that just because data is copied to the cloud, that doesn't mean it's air gapped. Organizations must ensure their processes support a physical separation of the data path and data control using separate credentials. It is also wise to protect the data copies with two-factor authentication and/or two-person authentication.

Organizations should also consider replicating cloud repositories to other zones or regions in the event of a cloud outage. These replicas should be configured to satisfy data sovereignty and governance requirements.

Conclusion

We are absolutely certain data survival is foundational to any data recovery. Having at least one offsite copy can be critical for disaster recovery and cyber-recovery. However, an offsite copy alone is not enough. That copy must be invulnerable to both external and insider attacks.

Cybervaults have emerged as an essential protection against attacks on data, whether that attack is on the data itself or through data exfiltration. While organizations must continue to follow normal data protection best practices, cybervaults add an extra layer of protection that is the last, best chance of data survival and recovery. Organizations without a cybervault open themselves to substantial business risk. Cloud-based, fully managed cybervaults can mitigate this risk, both simply and with cloud economics.

Cybervaults add an extra layer of protection that is the last, best chance of data survival and recovery.

About the Analysts



Phil Goodwin, Research Vice President, Infrastructure Software Platforms, Worldwide Infrastructure Research

Phil Goodwin is research vice president within IDC's Worldwide Infrastructure Research organization and global research lead for the Infrastructure Software Platforms practice. He leads a team of analysts that provide detailed insights and analyses on evolving infrastructure software trends, vendor performance, and the impact of new technology adoption. Mr. Goodwin's own research focuses on multicloud data management, data logistics, on-premises and cloud-based data protection as a service, cyber-protection and -recovery, and recovery orchestration.



Johnny Yu, Research Manager, Infrastructure Software Platforms, Worldwide Infrastructure Research

Johnny Yu is research manager within IDC's Worldwide Infrastructure Research organization and part of the Infrastructure Software Platforms practice. His coverage includes storage software; data replication, protection, and archiving software; storage device management; and container data management. Johnny focuses on cost optimization, storage and data security, and service quality as companies bridge their infrastructure between on premises and cloud.

MESSAGE FROM THE SPONSOR

Veeam is the #1 global leader in data resilience, delivering business continuity without compromise.

Veeam Vault is our storage-as-a-service solution, purpose-built to receive your Veeam Data Platform backups and your Kubernetes stateful data via Veeam Kasten backups, helping you achieve the 3-2-1-1-0 rule with ease. Veeam Vault is fully managed and pre-secured, allowing you to eliminate the headaches of managing infrastructure and unpredictable cloud cost models.

With Veeam Vault, you can ensure your backups maintain data integrity, are always compliant, and ready for fast disaster recovery. With predictable, all-inclusive pricing, you can gain confidence in your data resilience posture without wasteful spending. And unlike DIY or boutique cloud alternatives, Veeam Vault is pre-secured and has zero management needs.

You can find more information on Veeam Vault and how it helps you achieve data resilience on [our product page](#).



The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2025 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)