BACKBLAZE & VEEAM PRESENT

Innovations

LEARNING SERIES

The Definitive Guide To Immutable Cloud Storage with Veeam and Backblaze B2 Cloud Storage

How Simple Solutions Can Ensure Maximum Recoverability

Melissa Palmer

Backblaze | veeam

POWERED BY ActualTech MEDIA

The Definitive Guide To Immutable Cloud Storage with Veeam and Backblaze B2 Cloud Storage

By Melissa Palmer

TABLE OF CONTENTS

Copyright © 2023 by Future US LLC
Full 7th Floor, 130 West 42nd Street, New York, NY 10036

www.actualtechmedia.com

Publisher's Acknowledgements

DIRECTOR OF CONTENT DELIVERY
Wendy Hernandez

CREATIVE DIRECTOR
Olivia Thomson

SENIOR DIRECTOR OF CONTENT
Katie Mohr

WITH SPECIAL CONTRIBUTIONS FROM BACKBLAZE
Anna Hobbs-Maddox, Sr. Partner Marketing Manager
Kari Rivas, Sr. Product Marketing Manager

ABOUT THE AUTHOR

Melissa Palmer is a technologist and content creator specializing in many areas of data centers, cloud, and information security. She is a VMware Certified Design Expert and previously worked for and with vendors for over a decade in roles such as Systems Engineer, Technical Marketing Engineer, Product Marketing Manager, and Office of the CTO.

She is a consultant focused on solving some of the toughest problems IT environments face daily including ransomware and security threats.

Introduction

In today's rapidly evolving digital landscape, organizations face an unprecedented array of threats that underscore the critical importance of business resilience. An alarming rise in ransomware attacks has revealed that many organizations have inadequate data protection strategies and disaster recovery plans. To remain resilient, businesses must be proactive in adopting robust strategies that prioritize protection and recovery.

Organizations must invest in comprehensive data protection solutions that embody cutting-edge tools for backup, disaster recovery, and modern data protection across various workloads.

This comprehensive guide explains the various facets of business resilience, including data protection and disaster recovery challenges. It also explores how the cloud has become an important tool for a more robust and agile response to cyberthreats.

The Need for Business Resilience Today

Business resilience refers to an organization's ability to rapidly adapt and respond to disruptions while maintaining continuous business operations, safeguarding people and assets, and upholding its brand and reputation. It is about creating a robust system that allows the business to endure shocks and bounce back quickly from a crisis, thereby minimizing disruption to its services.

In the current business climate, business resilience is one of an organization's most important focal points. This centrality of resilience stems from the staggering rise in ransomware attacks in recent years. According to Veeam's 2023 Data Protection Trends report, over 85% of organizations suffered a ransomware attack in the past year, and of those attacked, only 55% of the data was able to be recovered on average. These statistics have left organizations scrambling to implement business resilience plans.

Planning a Strategy with Protection and Recovery in Mind

The path to a winning business resiliency strategy is to start planning backups and disaster recovery immediately. Historically, backup and disaster recovery have not been the most popular areas for IT planning. Many organizations that now have a gap in data protection simply accepted the risk of disaster in the past.

In reaction to ransomware, the paradigm has shifted. The question is no longer whether an organization is struck by a security threat or data disaster, but when. The old data protection and disaster recovery strategies no longer work, and steps need to be taken today to ensure resilience tomorrow.

Being ready for the threat of a ransomware attack also prepares organizations for more traditional disasters such as natural disasters, system failures, or hardware malfunctions. By having robust data protection and recovery systems in place, organizations are capable of quickly restoring operations and minimizing downtime, even in the face of unexpected incidents. This preparation results in resilient infrastructure that can withstand a multitude of disruptive events, an area that many organizations have lacked in for some time.

⚠ **Many organizations face a "Reality Gap" when it comes to recovering from a cyber event or other type of disaster.**

According to the Veeam 2023 Data Protection Trends Report, 79% of organizations realize they have gaps in their data protection service-level agreements (SLAs), and 82% of organizations admit they have a gap in their ability to protect their data in the first place.

This new reality calls for a proactive approach to business resilience. Organizations must invest in comprehensive data protection solutions that embody cutting-edge tools for backup, disaster recovery, and modern data protection across various workloads.

In addition, businesses should cultivate a culture of cybersecurity awareness and implement robust policies to minimize the risk of ransomware attacks. By taking these steps today, organizations can build a strong foundation for data protection and disaster recovery, ensuring business continuity and safeguarding their assets in an ever-evolving digital landscape.

Common Data Protection and Recovery Challenges

If organizations aren't prepared for a disaster recovery event it's because they haven't found solutions to some of the most common data protection problems plaguing IT environments. The problems are not new, but the impact of a failure to protect backup and recovery systems is much greater than in the past.

Ensuring Data Is Protected Before an Attack

In today's environments, data is everywhere, from on-premises to the cloud. It's important for organizations to have visibility into their data wherever it may be, so they can properly protect it.

After organizations have identified their data, they also need to understand its location, along with its role in business continuity. It's essential to determine Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for each data set to guide an effective backup strategy. RTOs and RPOs help decide the frequency of backups to meet the business's recovery needs.

Backups need to be stored in an immutable fashion, so malicious actors cannot modify or delete them.

Setting up the backup process according to RTOs and RPOs involves secure, reliable storage that's preferably offsite or in the cloud to ensure maximum recoverability in the event of an on-premises disaster.

Today, malicious actors can spend time inside an environment undetected to learn how things work before sabotaging backup systems and encrypting and exfiltrating data. Immutability is a response to this threat. Backups need to be stored in an immutable fashion, so malicious actors cannot modify or delete them.

The Price of Protection

Budgets are not increasing, and neither is the number of staff on hand to manage the data protection environment. Costs in hardware and facilities are also multiplying, making it difficult to ensure that a data protection environment is truly able to protect and recover in a way that meets business requirements.

When putting a business resilience plan into place, many organizations will realize they aren't properly protecting their data. They might find large amounts of unprotected data, while other data may not be protected in the way that will meet recovery objectives.

To address these challenges and constraints, organizations can explore cost-effective cloud-based solutions, automation, and managed services to optimize their data protection and recovery strategies. By prioritizing data protection and employing innovative solutions, businesses can build a robust resilience plan that safeguards their critical assets and ensures continuity in the face of evolving threats.

Every Recovery Is Different

No matter how prepared an organization is, no one can know for sure what will happen when a cyberattack unfolds. This is why it is so important to have data in multiple recovery locations ahead of time and make sure recovery has been tested in each and every one.

It's only after the attack has been identified and the incident response process has begun that organizations will know which recovery plan to execute. Testing is crucial to ensure that all issues are found and fixed before recovery.

It's essential to continuously assess and update the organization's cybersecurity measures, adapting to new threats and refining recovery plans accordingly. By adopting a comprehensive and proactive approach to cyber resilience, organizations can minimize downtime, protect valuable data, and maintain their reputation in the face of ever-evolving cyber threats.

Employing the Cloud

While ransomware and the cyber climate of today have shifted the scale and likelihood of a disaster, the cloud has modernized protection and recovery strategies in several different ways.

Using the Cloud for Cyber Resilience

Using the cloud in some form is a must for every cyber resilience plan. Having backups waiting in the cloud, along with the ability to recover to the cloud, is an essential pillar of any disaster recovery strategy.

According to Veeam's 2023 Data Protection Trends Report, the adoption of cloud-powered disaster recovery has been growing in recent years, as illustrated in **Figure 1**.

Which of the following is your organization's primary method of business continuity and disaster recovery (BC/DR) today? In two years time?

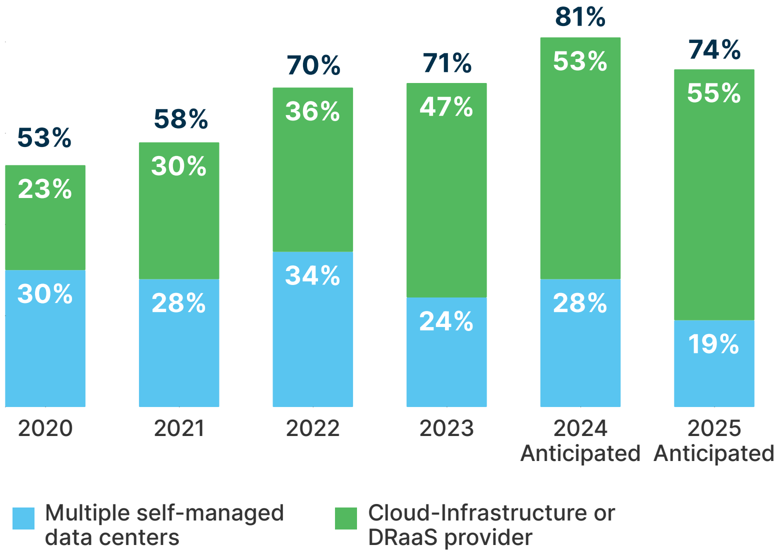

Figure 1: Cloud-powered disaster recovery 2020 to 2025

This trend has been increasing for a number of reasons. Perhaps the leading reason is that many organizations simply never had the on-premises capabilities to do a site-level recovery.

In many cases, it's no longer practical from a time, cost, or personnel perspective to build out complete recovery capabilities on-premises. This leaves the cloud to be a great alternative, especially since there are so many ways to consume the cloud for recovery.

Cloud-based recovery solutions can provide scalability, flexibility, and cost-effectiveness, allowing organizations to adapt their resilience strategies to ever-changing threats and business needs while maintaining the highest levels of data protection and operational continuity.

Cloud Challenges

Although the cloud is an essential part of any cyber resilience plan, it’s not without its own set of challenges. First and foremost is cost, including but not limited to storage, egress fees, and other incremental charges like the cost of support. It’s essential for organizations to determine these costs before starting to move backup data to the cloud, so that they can avoid a surprise bill.

There are also softer costs associated with the cloud, such as the cost of operations and of training administrators and architects on the cloud environments that are to be leveraged.

How Backblaze and Veeam Solve Backup, Disaster Recovery, and Business Resilience Challenges

Modern solutions are needed to solve today’s backup, disaster recovery, and business resilience challenges. Solutions need to be ultra-flexible to enable organizations to recover from a cyber event at a moment’s notice.

Solving Business Problems

Backblaze and Veeam are uniquely poised to solve modern business resilience problems, from ensuring all data is protected to meeting business recovery objectives. Veeam's data protection solution pairs perfectly with Backblaze B2 Cloud Storage to provide a backup repository protecting all workloads.

To understand why Backblaze B2 is so well suited to protecting and recovering data, it is important to understand Veeam's methodology to data protection.

At the heart of this methodology is Veeam's 3-2-1-1-0 rule, which becomes simple and cost effective to implement with B2. You can see what this looks like in **Figure 2**.

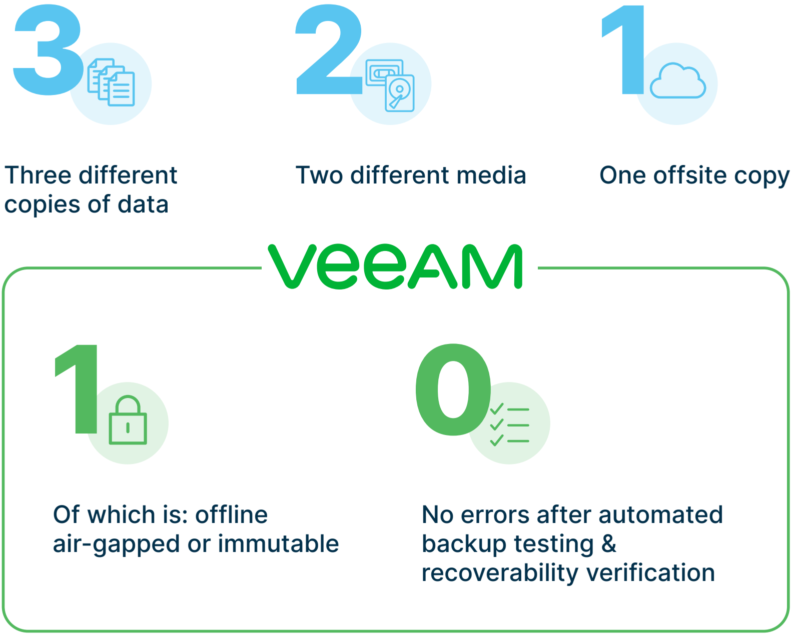
3
Three different copies of data
2
Two different media
1
One offsite copy
veeAM
1
Of which is: offline air-gapped or immutable
0
No errors after automated backup testing & recoverability verification

Figure 2: The 3-2-1-1-0 rule explained

This rule is simple to follow, and prepares organizations to recover data at a moment's notice to any location. The rule calls for 3 copies of backup data stored on 2 different media types, with 1 being offsite. In the age of ransomware, the last 1 and 0 become very important. These components break down to 1 copy being stored offline, air-gapped, or immutable, with 0 errors after recovery testing from backups.

Backblaze makes it simple to follow this rule, and strengthens the rule further by making it easy to locate the offsite copy of data geographically distant from the production location and to enable immutability on the backup, which has become a popular model for Backblaze customers.

EXECUTIVE CORNER

AcenTek Case Study

AcenTek, a Midwest-based telecom company, prioritizes protecting and managing critical data for its rural customers. To enhance its data backup strategy, the company adopted a 3-2-1 approach: 3 copies of data on 2 different media, with an off-site copy in a different geographic region. AcenTek chose Backblaze B2, an enterprise-grade, S3-compatible object storage solution, to complement its existing setup on Veeam.

Backblaze met AcenTek's performance and security requirements and satisfied its cybersecurity insurance provider's off-site data storage mandate. The new infrastructure enhances AcenTek's resilience to potential data loss while satisfying SLA obligations to customers.

Cost remains one of the biggest factors in plans for data protection and disaster recovery. Backblaze helps to reduce costs dramatically with B2 Cloud Storage. B2 Cloud Storage is always hot storage at cold storage price points. It is one-fifth the cost of the big, hyperscale public cloud solutions as a backup target. This means organizations no longer need to cut corners on things like retention periods or versioning. B2 Cloud Storage allows immediate access and, unlike diversified cloud providers, doesn’t charge egress fees between many partner integrations, which are important factors when it comes to recovery planning.

Backblaze and Veeam are uniquely poised to solve modern business resilience problems, from ensuring all data is protected to meeting business recovery objectives.

B2 Cloud Storage is also object-lock-capable, making it easy to have an offsite immutable copy of your backup data that cybercriminals cannot delete or modify. With security in mind, B2 Cloud Storage also provides protective features such as server-side encryption and multifactor authentication. Backblaze data centers are SOC-2 compliant, able to store customer data securely and with the utmost care.

While security by design and cost reduction are two important components to a modern business resilience plan, Backblaze

B2 also shines in many other areas. It's simple and easy to use, offering storage in a set-it-and-forget-it style. Most customers can set up B2 Cloud Storage within minutes on their own, and Backblaze teams provide super-fast support when needed. This nicely complements Veeam's similar simple-to-use, software-defined model.

When a ransomware attack does happen, Backblaze and Veeam are able to provide a unique solution to allow customers to recover under any scenario. Cloud Instant Business Recovery with Continuity Centers offers on-demand, multi-cloud disaster recovery as a service. This solution provides flexibility and cost effectiveness when you are planning for and recovering from a ransomware attack.

Tackling contemporary backup, disaster recovery, and business resilience challenges requires the implementation of advanced, flexible solutions that enable organizations to bounce back from cyber incidents swiftly. Backblaze and Veeam have established themselves as frontrunners in addressing these challenges, providing comprehensive data protection, and meeting a wide range of recovery objectives.

The powerful synergy between Veeam's data protection approach and Backblaze B2 cloud storage allows seamless implementation of Veeam's 3-2-1-1-0 rule for robust data protection.

In the face of ransomware attacks, Backblaze and Veeam's combined solution offers unparalleled flexibility and cost-effectiveness for recovery planning. Their joint capability to provide instant recovery in any cloud environment and multi-cloud disaster recovery demonstrate the strength of their collaboration in delivering a resilient, secure, and accessible data protection solution for organizations of all sizes.

The Time Is Now

In this guide, we've looked at how critical data protection, disaster recovery, and business resilience is for any organization. The paradigm has shifted for organizations due to the increase in cyber threats, especially ransomware attacks.

By adopting proactive strategies, organizations can be sure they are able to recover under any scenario to any location. This type of preparation does not come without challenges, especially when it comes to data protection gaps, cost constraints, and operational overhead. The cloud has become a vital part of any organization's business resilience strategy.

The partnership between Backblaze and Veeam is a powerful solution to these challenges and enables organizations to meet their recovery objectives no matter what the disaster scenario is.

Thanks for reading, and remember, the time is now to protect your data so you can recover it after a disaster. Get started today with Veeam and Backblaze. Have more questions? Be sure to connect with a Veeam Backup Specialist.

About Backblaze

Backblaze makes it astonishingly easy to store, use, and protect data. The Backblaze Storage Cloud provides a foundation for businesses, developers, IT professionals, and individuals to build applications, host content, manage media, back up and archive data, and more. With over two billion gigabytes of data storage under management, the company currently works with more than 500,000 customers in over 175 countries. Founded in 2007, the company is based in San Mateo, CA. For more information, please go to www.backblaze.com.

About Veeam

Established in 2006, Veeam initially aimed to streamline virtual machine backups and rapidly emerged as an industry leader. The company remains dedicated to driving innovation in the sector, empowering you to take ownership of, manage, and secure your data across the hybrid cloud. Veeam offers cutting-edge data protection solutions, including backup, disaster recovery, and advanced data protection software for virtual, cloud-native, SaaS, Kubernetes, and physical workloads.

About ActualTech Media

ActualTech Media, a Future company, is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.