druva

White paper

You need to simplify remote office backup —and here's why

Q320-20084

Introduction

Cloud backup and recovery has modernized data protection for enterprises of all sizes, including remote and branch offices (ROBOs). It has become a compelling value proposition for every company looking to prevent potentially catastrophic data loss, from the smallest offices to regional headquarters and everything in-between. Cloud backup and recovery is the obvious solution for mid-to-large enterprises with hefty resources, yet it's also very useful for typically unprotected smaller offices with limited budgets.

But, maybe your organization hasn't fully strategized an effective cloud backup and recovery plan for remote and branch offices. Not sure where to start? As an initial step, it's important to think about the following challenges and craft a strategic plan on how to resolve them:

- Remote and branch offices struggle with the challenges of effective backup and recovery.
- Smaller locations often lack dedicated IT resources to achieve and manage comprehensive data protection protocols.
- Larger offices typically lack the storage scalability and security needed to protect endpoints, data centers, and cloud workloads enterprise-wide.

This paper outlines the benefits of cloud-based backup and recovery for remote and branch offices, relevant uses cases, and best practices to consider as you implement a third-party cloud backup solution. You'll be ready to tackle remote and branch office backup challenges in no time.

Cloud backup and recovery benefits for ROBO

Cloud backup and recovery lets companies reduce data protection costs, minimize downtime, and enable central IT to manage backup and recovery remotely for ROBO sites. According to Aberdeen Group, "The use of a cloud-based backup and restore solution reduces the total cost of lost productivity for enterprise users in ROBO scenarios by more than 95%, as compared to the use of traditional on-premises approaches."

> *"The use of a cloud-based backup and restore solution reduces the total cost of lost productivity for enterprise users in ROBO scenarios by* ***more than 95%.***
>
> — Aberdeen Group

Many cloud backup vendors offer up-to-the-minute snapshots of virtual machines, applications, and changed data. Some offer backup and recovery capabilities for business-critical SaaS applications such as Microsoft Office 365. Others also offer data management features such as analytics, eDiscovery, and regulatory compliance. This is all done while eliminating on-premises hardware and software infrastructure, greatly simplifying backup administration.

The wide-ranging benefits of cloud data protection for ROBO environments include:

- **Lower TCO:** To accurately calculate the costs of using and maintaining an IT investment over time (TCO), you have to combine both direct and indirect expenses. Hardware, software, operations, and administration costs are usually easy to quantify. But figuring out indirect costs is trickier, especially in ROBO environments. Initial hardware investments typically represent a fraction of their TCO. The missing percentage is the technical support, maintenance, and other labor costs over time. Cloud data protection doesn't require on-premises infrastructure.

- **Ransomware protection:** Every year, ROBOs worldwide lose billions of dollars worth of data and lost productivity to a man-made disaster: ransomware. That's why it's critical for your organization to be prepared and protect from ransomware entering the network from vulnerable ROBOs without local IT. According to a recent report by Aberdeen Research, an enterprise with 1,000 workers, each with a laptop, handling collectively 10TB of data, is likely to lose nearly $480K from a successful ransomware attack. Plus, there's a 10% chance it'll lose more than $2.5M.

  However, after setting up a cloud backup and recovery solution, the likely loss goes down to about $54K. The loss from a 10% worst-case attack goes down to $200K. That means a solution that lets you easily back up all of your enterprise data in the cloud, and restore it quickly, can reduce the impact of a ransomware attack by more than 90%.

- **Centralize backup storage:** ROBOs have data that they simply can't do without and if it's lost for any reason, they need it restored immediately. Cloud storage provides a single backup repository for central offices, as well as ROBOs, for legal hold and eDiscovery.

Cloud or cloud-native SaaS?

When you're thinking about the various backup solutions for remote and branch offices, there is a significant difference between backup vendors that offer cloud vs. cloud-native backup and recovery, usually centered around how the product was originally architected. Cloud is generally an adaptation of a traditional, on-premises solution that simply adds cloud storage as an option. It's typically a fully customer-managed product that includes software and hardware.

> *"Cloud-native solutions are 'born in the cloud.' They're designed from the start as services that require minimal IT overhead and fully leverage cloud service provider systems and microservices.*

On the other hand, cloud-native solutions are "born in the cloud." They're designed from the start as services that require minimal IT overhead and fully leverage cloud service provider systems and microservices, without requiring onsite hardware or maintenance. That's why you should evaluate your vendor's technology and ensure your organization is receiving the most optimal and modern approach to cloud backup services.

Use cases

With its low cost and ease-of-use, cloud backup and recovery works well with wide-ranging data protection scenarios. This section describes several ROBO use cases.

Self-service backups and restore

Self-service backup and restore is ideal for smaller locations given the low likelihood of dedicated staff for managing backups. In fact, for ROBOs, self-service cloud backup and recovery is practically an operational requirement to ensure that business operations continue in a timely fashion after a data loss.

Archiving

The cloud's vast scalability and end-user management choices make it an obvious choice for archiving data enterprise-wide. End-users should evaluate entry costs and data access times when using cloud-storage services such Amazon Glacier and look for a vendor that uses policy-based auto-tiering to move data to cold storage. Amazon Glacier, for example, can take hours for retrieval so should be limited to storing cold, infrequently accessed data.

Central management

ROBO operations need comprehensive remote management features that let management tasks be completed over the network. Cloud-native backup solutions can manage backup and recovery from a centralized management console, enabling a headquarters-based IT group to configure and monitor backups and restores with no intervention from ROBO personnel.

> *Cloud backup and recovery works well with wide-ranging data protection scenarios, including remote and branch offices.*

Governance

Over the past years, corporate governance and compliance have become business-critical for most companies. The IRS requires financial data to be retained for at least seven years, and other regulations, such as FINRA and Sarbanes-Oxley, have even longer horizons. Regulations such as HIPPA have stringent requirements for securing personally identifiable information (PII), which means that companies need backup and recovery capability that supports strong encryption and data security. Considering stringent governance and compliance regulations, the cost of a robust backup and restore solution is easy to justify.

Best practices for implementing cloud backup and recovery

Here are the most important factors to keep in mind when implementing a comprehensive cloud backup and recovery solution for ROBO.

Planning

"Fail to plan, plan to fail." Always have a project plan in place to guide evaluation, procurement, implementation, and support of your cloud backup and recovery strategy for ROBO. Even an informal document is better than none at all. Outline who's responsible for the various aspects of a successful implementation, what happens when something goes wrong, and how and where users can get backup-and-recovery support.

Architecture

Cloud data protection can run on a variety of architectures, including direct to cloud, hybrid with caching, hybrid with storage, and local-appliance to cloud. But, there is only one appropriate option for ROBO—direct to cloud. With no local storage appliance, advantages include a lower cost-of-ownership and a simple architecture. Particularly for ROBOs, look for vendors that offer a centralized management console for all backup operations.

Trials

Testing all of your potential ROBO cloud backup solution choices thoroughly helps minimize surprises during the implementation and operational phases. IT should test each product's backup and restore procedures, and if you're implementing server backup and restore capabilities, be sure to include server and backup admins in the trial phases.

> *Particularly for remote and branch offices, look for vendors that offer a centralized management console for all backup operations.*

Encryption

Data security is just as important to your company's success as adequate backup, so be sure that the products you evaluate include appropriate encryption. This is an absolute necessity in industries that are subject to data security

and privacy regulations such as HIPAA, FINRA, and Sarbanes-Oxley. Be sure that the cloud solutions you evaluate include appropriate encryption levels (both in-transit and at-rest) and sufficient data security features to ensure compliance with all applicable regulations and company guidelines.

Support

Even the best cloud backup solution is worthless if the vendor is not available to provide help in a timely manner to the project manager or operational IT manager. Remote troubleshooting is critical for ROBO, and you should ensure that it's included in your vendor's support processes and expertise as you evaluate your options. Online knowledge bases and robust support portals are extremely useful, but you still need to be able to reach a real support agent quickly. Once you commit to a solution, you need to know that the company will be there to help when you need it.

Next steps

Cloud backup and recovery has gone from an expensive wish-list item to a budget-friendly, solution that's critical to your company's ongoing operations. If your company is not taking advantage of cloud backup and recovery for remote and branch offices, there is no time like right now to implement a suitable solution. The survival of your company could be at stake. If your company has a cloud backup and recovery strategy in place, you can still explore the cost-saving potential of cloud backup for remote and branch offices, or increase your cloud backup capabilities without increasing costs, or, in some cases, both.

> *"Explore the cost-saving potential of cloud backup and recovery.*

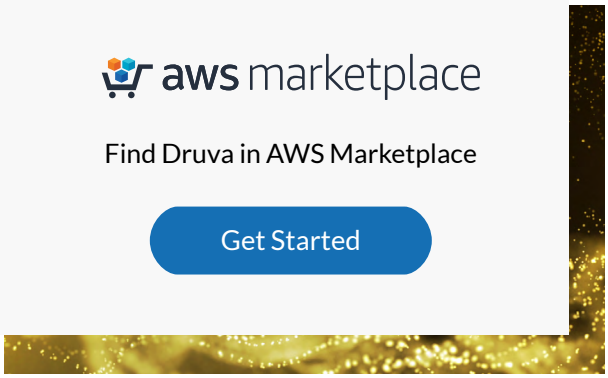
We recommend exploring the potential of cloud backup and recovery for remote and branch offices. Then look into determining how these capabilities can help you better protect your business-critical data. The question is no longer whether you can afford it, but rather, can you afford not to?

See how your remote and branch offices can benefit from a cloud-native backup solution—check out **druva.com/remote-office-cloud-backup/.**

aws marketplace

Find Druva in AWS Marketplace

Get Started



druva

Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit Druva and follow us @druvainc.

© Druva, Inc. | www.druva.com