druva

Business Brief

SIMPLIFIED DATA PROTECTION FOR REMOTE & BRANCH OFFICES

MAKING THE BUSINESS CASE FOR ROBO DATA BACKUP IN THE CLOUD

Q118-CON-10739

Explosive Growth: The Enterprise Data Issue

In today's hyper-connected business landscape, enterprise data is growing at an exponential rate—40%-to-60% every year, according to CIO.com. With more data comes an increased risk of exposure as a result of litigation and compliance audits. This explosion of information places enormous pressure on companies to more efficiently archive, retrieve, and manage their data. Any company with remote or branch offices (ROBO) requires a data protection solution with the flexibility to support the differing needs of both central and distributed sites.

"Primary and secondary storage requirements are growing at around 40% year-over-year."

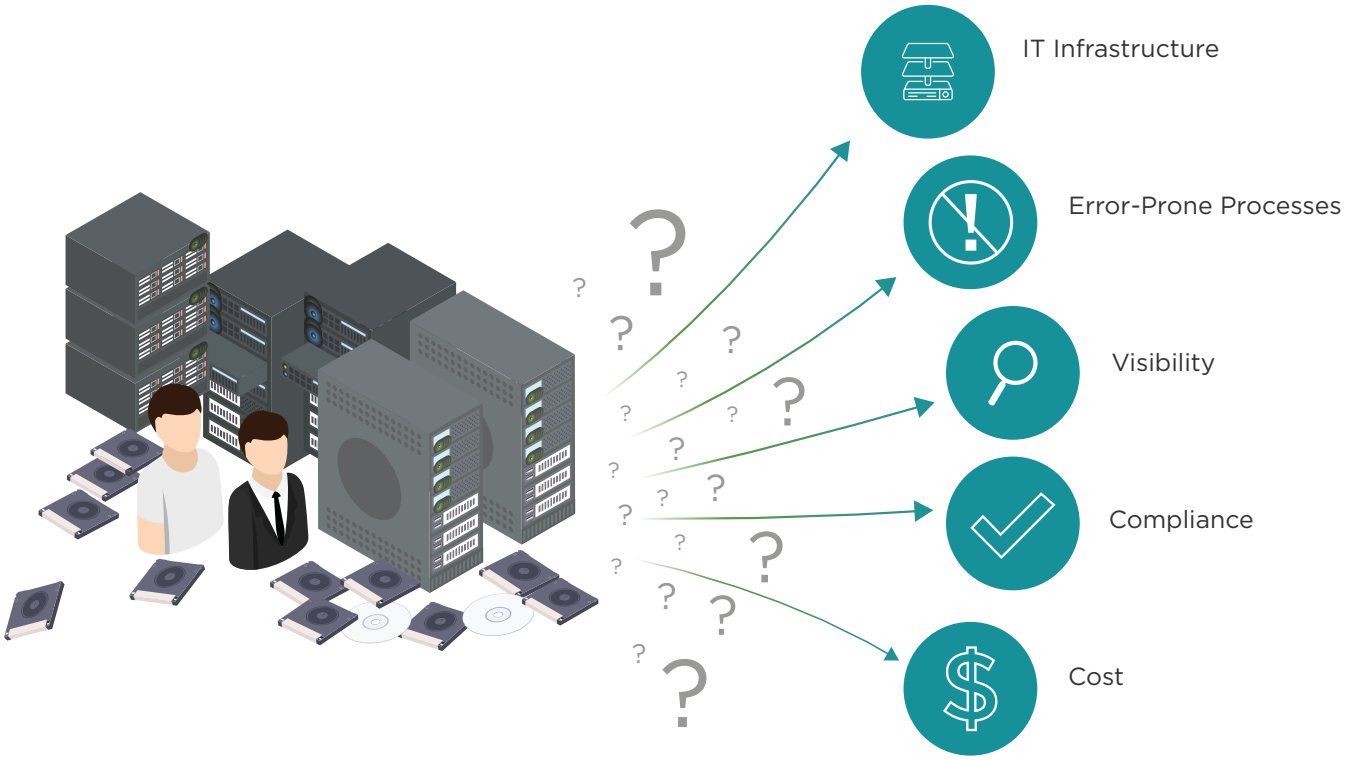
–ESG, Plan for Hybrid Data Protection Media January 2016

Most recently, today's economic realities have forced companies of all sizes to reevaluate their IT environments. They must find ways to do more with less: following new regulations while cutting costs without sacrificing service levels. Fortunately, IT departments now have more choices than ever when selecting a data protection strategy for their remote environments. This includes cloud storage and other service options, which provide distinct advantages over traditional approaches.

Business Critical ROBO Data: The Challenges

For many organizations, their remote and branch offices are like the Wild West: lawless and largely unregulated. While the enterprise may have a well-defined set of policies and procedures in place for server data protection, they are often not effectively enforced at every location. Instead, teams are left to develop their own strategies using whatever tools are available to them.

For example, whereas a primary data center typically has dedicated backup and recovery administrators, ROBOs often do not. Instead, someone in the ROBO, who is most likely not part of the IT function, typically handles data backup as a secondary responsibility. In a recent ESG analyst study, nearly three-quarters of respondents reported that only 20% of their ROBO locations have dedicated IT staff. The all-too-common result? Inadequate backup procedures inevitably leading to data corruption and/or loss. These lapses can result in serious financial consequences stemming from regulatory fines, litigation missteps, and failed audits.



ROBO sites face many unique challenges that make traditional data protection approaches difficult, if not impossible, to implement, such as:

- **IT infrastructure and Resources:** ROBOs are often hampered by network and computing limitations as well as a lack of trained IT staff. These challenges are compounded by regional data privacy restrictions requiring organizations to have the ability to manage their data dynamically. These complexities can lead to insufficient IT services being provisioned—in a recent ESG study, for instance, 37% of respondents reported local data backup as a significant ROBO challenge.

- **Manual Error-Prone Processes:** Backup processes in ROBO environments usually lack automation and depend on tape shipment or other manual, off-site methods. This can lead to backups occurring infrequently or not at all, putting ROBO data at an increased risk of loss.

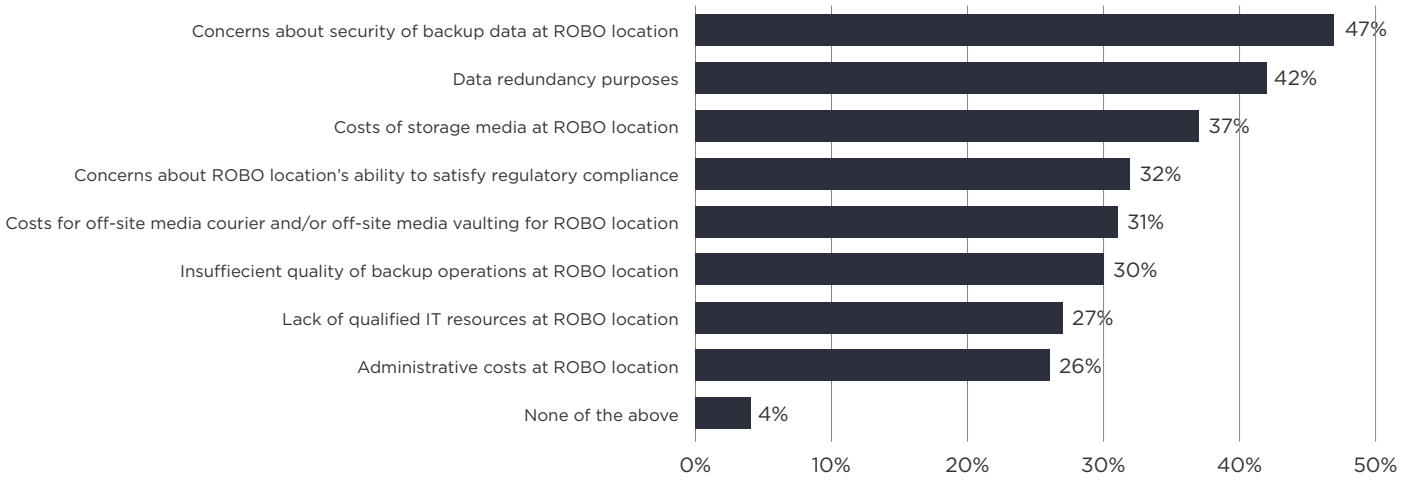
- **Lack of Visibility into SLAs:** Manual processes, combined with lack of sufficient infrastructure, make it difficult or impossible for IT to have visibility into service resiliency as well as recovery time objective (RTO) and recovery point objective RPO guarantees. And if you can't see it, how can you manage it?

- **Cost:** Respondents in the ESG survey also cited cost-related issues as one of the many challenges related to running services locally at ROBO sites. Decentralizing the IT infrastructure, services, and management expands the overall cost of ownership for backup services, which also increases with each ROBO location. As a result, companies often underprovision remote sites, leaving them poorly equipped to meet their individual data protection needs.

Business Critical ROBO Data: The Risks

Legacy solutions have proven woefully inadequate at meeting enterprise ROBO needs, especially given the new legal and regulatory landscape. According to the Norton Rose Fulbright 2015 Annual Litigation Trends Survey, 37% of large organizations reported having 20 or more pending lawsuits, and 42% of companies overall reported having more than six lawsuits filed within the last year. In total, 26% of companies surveyed have cases that exceed $20 million. These legacy solutions don't provide the visibility and manageability necessary for organizations to adequately comply with regulations requiring data to be retained for a set period of time, or that is subject to legal requests. Without these capabilities, critical data is inadvertently lost or mishandled—exposing a company to compliance risks and potentially resulting in ruinous litigation.

Why Organizations Are Moving ROBO Backup to Third-Party Cloud Services



Traditional methods that employ a mix of on-prem infrastructure, disk hardware, and tapes are prone to failure and represent a serious risk to ROBO data. Luckily, these obstacles are easily overcome by leveraging cloud.

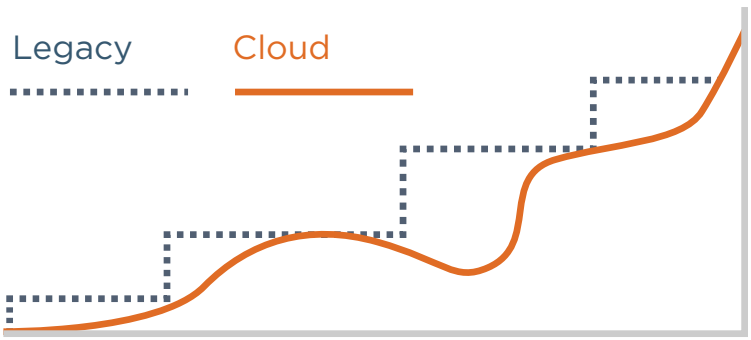
Disk—is still the predominant media type for storing secondary and tertiary data. However, disk is an extremely expensive medium for storage at the required scale, leaving many organizations unable to afford the redundant infrastructure necessary to ensure data integrity and resiliency. This substandard approach to archiving leaves organizations vulnerable to lost and corrupted data, non-compliance, and other issues.

Tape—like disk, tape often fails to meet compliance and other data governance needs. Due to long-term retention policies, a growing number of systems and sites, and a wildly impractical "hold-everything-just-in-case" mindset, companies often manage thousands, or even hundreds of thousands, of aged tapes in libraries and offsite locations. At this scale, retrieving and restoring legacy data from mountains of tape is slow, cumbersome, and a major burden for companies facing time-sensitive compliance or legal demands. In addition, boundless data retention can lead to serious legal exposure if information is asked for during litigation and no solution exists to automate deletion based on standard retention policies.

Solution: Centralized Cloud Backup for ROBO

The first step in addressing this growing concern is assessing your current environment to determine how your organization can best leverage cloud options to improve your ROBO data protection. With a cloud-native solution, there is no expensive hardware to provision, which virtually eliminates capital expenditures (CAPEX). In addition, the cloud can provide global data deduplication and smart WAN bandwidth allocation to dramatically lower the enterprise data footprint and enable massive operating expenditures (OPEX) savings.

Pay Only for What You Use



- As data grows, the savings grow compared to overprovisioned legacy hardware
- Scale storage on demand, removing time-consuming and costly procurement cycles

"By 2019, the percentage of enterprises using the cloud as a backup destination will double, up from 11% at the beginning of 2016."

–Gartner, Market Guide for Data Center Backup October, 2016

A cloud solution simplifies the process by enabling you to backup straight to the cloud, providing a seamless way to manage all your backup and archives centrally. Cloud removes the traditional bottlenecks of compute and scale, delivering a high-performance experience and enabling organizations to achieve the highest level of data throughput possible to meet their RPO and RTO targets.

Improving Business Agility and Reduce Cost

Data backup and archiving is no longer an option for today's enterprise. The exponential growth of mission-critical business data and the corresponding legal requirements for its retention make it essential that every company has a robust plan in place for the safe storage of server data. The proliferation of remote and branch offices only makes this need more acute.

Gain Visibility & Streamlined Management: Leverage a single pane of glass to manage and monitor all your global server backup and DR policies, removing the burden of complex storage, compute, and networking management—and significantly reducing costs.

Self-Service Backup & Recovery: A cloud-native solution enables different site admins to perform self-service backups and recovery of their own data set, without infrastructure interdependencies.

Improved Business Agility: A unified cloud management approach enables fast response times in the case of failover for disaster recovery with RTO in minutes, or can allow you to replicate and move VMs across regions.

What's Next?

By leveraging a unique and scalable cloud-native storage architecture, organizations have overcome these outdated and overtaxed models and have achieved the search, retrieval and management functionality and speeds required by the modern, decentralized enterprise.

To explore more scalable approaches to data protection that leverage the power of the public cloud to offer a comprehensive ROBO data protection solution, visit our ROBO Solutions Page.

About Druva

Druva is the leader in cloud data protection and information management, leveraging the public cloud to offer a single pane of glass to protect, preserve and discover information—dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations and protects over 25 PB of data. Learn more at http://www.druva.com and join the conversation at twitter.com/druvainc.

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44.(0)20.3150.1722
APJ: +919886120215
sales@druva.com
www.druva.com