Realtime publishers

Protecting Client Data in the Cloud:
A Channel Perspective

The Essentials Series

Selling Cloud Data Protection: Converting Potential Customers

sponsored by

EVault®
A Seagate Company

Ed Tittel

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Selling Cloud Data Protection: Converting Potential Customers

Lots of vendors offer cloud services to their customer base, and lots of resellers are wondering how to sell them. If you've already evolved your business model to include cloud data protection, your next step is converting customers. Use the information in this article as a springboard to help you gain new customers and to convert existing customers over to cloud services.

Data Is Highly Secure and Accessible in the Cloud

Of all the cloud services available, from remote server management to wide area network (WAN) management and optimization, data protection and disaster recovery are some of the most security-conscious. An organization that entrusts its data to an unseen storage device or array that's hundreds or thousands of miles away needs guarantees that its data is highly secure in transit and in storage. High availability also factors heavily into the quality of these services. After all, what's the value of a data protection or disaster recovery service if customers can't access their data or the solution when they're needed? Cloud-related data protection and disaster recovery services have come a long way, so you can assure potential customers that they're highly secure and accessible for a number of very good reasons.

Data Lives in a Secure Data Center

In data protection that accesses the cloud, whether data goes directly from disk to cloud or disk to disk to cloud (meaning it's stored on a device or appliance before being transmitted to remote storage), the ultimate location is usually a secure data center. A first-rate vendor always uses several geographically-dispersed, top-tier, Statement on Auditing Standards (SAS) 70 Type II- and ISO-certified data centers as the foundation for its cloud infrastructure and for redundancy.

The data is encrypted at the customer site using a strong encryption method such as NIST 128-bit or 256-bit Advanced Encryption Standard (AES). The connection between the customer site and the data center is encrypted, so data is secure in transit. Finally, data is stored in the data center in encrypted form. Only the customer has the key to decrypt their data.

De-Duplication and Compression = Storage Space Savings

Another process that takes place before transmission is de-duplication. The backup software identifies matching blocks across all files at a site and eliminates duplicates. This does not impact the backup window or performance; however, it can reclaim a large percentage of storage space. For example, depending on the type of data being backed up, de-duplication can squeeze 80 terabytes (TB) of data down to 12TB for storage purposes, saving the customer a lot of money and allowing you to handle more data.

Data Security Meets Compliance Requirements

Customers may need to comply with one or more government regulations, such as HIPAA, SOX, GLBA, or PCI DSS. A cloud data protection solution should meet or exceed such regulatory requirements to help customers maintain compliance. Remember, the customer may hand over IT functions to a cloud provider, but the customer continues to assume liability for the accuracy and security of its clients' data. For example, a company that maintains healthcare-related records contracts with a provider to handle remote data backup. If a data breach occurs and patient data falls into unauthorized hands, the records company remains liable and accountable according to applicable laws.

Also, by basing a data protection solution on standards such as CoBIT, ITIL, NIST, and ISO, customers can be better assured that a vendor or service provider has done due diligence when it comes to protecting data in and out of the cloud. If the provider is compliant, the reseller can establish a trust relationship with the end users.

The Alphabet Soup of Regulations and Standards

Here's a key to acronyms for regulations and standards mentioned in this article: Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX) Act, Gramm-Leach-Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI DSS), Control Objectives for Information and related Technology (CoBIT), Information Technology Infrastructure Library (ITIL), National Institute of Standards and Technology (NIST), and International Organization for Standardization (ISO). ISO is actually not an acronym in this case; it comes from the Greek iso, which means equal.

The Cloud Relieves Traditional Backup Limitations

Switching to a cloud data protection solution mitigates the drawbacks of on-premise backup processes:

- Slow and potentially risky manual transport for unencrypted backup tapes offsite
- No automatic access to offsite storage; only tape rotation or offsite network duplication provides redundancy needed for data protection and disaster recovery

Consider tape, or even disk-to-disk backup. Although backup speeds are relatively fast, especially with the latest media and drives, the amount of data to be backed up continues to increase, which jeopardizes the backup window or causes a less-than-stellar user experience.

For tape, a company needs to assign a person to load, eject, and transport tapes offsite for safe storage, and to retrieve one or more tapes to perform a restore. Recovery time is slow, especially if multiple tapes must be used to restore to a complete backup, and tape backups tend to be unreliable. Some experts estimate that a whopping 15 percent of tape recoveries fail. For disk-to-disk backup, burgeoning storage volumes often dictate tape as an archival medium, which simply re-introduces tape's weaknesses later in the storage life cycle.

For example, compare tape with the advantages of a cloud-based/cloud-connected backup solution:

- Ready 24/7 access to and from multiple sites
- Automated processing and offsite safety
- High-speed access at any location
- Expanded scope of storage savings across multiple sites
- Replication to multiple locations
- Ability to react quickly to many types of data loss or disaster
- Ability to recover data wherever and whenever it's needed

Clearly, data protection in the cloud is superior to tape backups for most computing environments, and provides valuable redundancy and offsite storage to complement disk-to-disk backup. Because the wave of the future is digital in almost every aspect of business, organizations will naturally flock to online data protection as an important backup solution.

Covers Multiple Platforms and Multiple Sites

A few more limitations of traditional backup methods are that they tend to be capital and labor intensive (customers own the media, the drives, and the software and must provide staffing and support to operate it). Adding the cloud to this mix enables organizations to trade off capital expenditures against monthly subscription or service costs and per-gigabyte storage fees. In addition, sending data into the cloud also incurs WAN utilization charges for bandwidth, and customers may need to trade data transfer performance against bandwidth costs (and availability).

In addition, an all-encompassing solution can protect multiple customer sites located across campus, across town, or in different states. These sites may be managed through a single console under the service provider's control. This can reduce staffing requirements and related personnel costs.

Channel Partners Handle Pain Points

With you, the channel partner, acting as the provider for the data protection solution your customer is "leasing," you also bear the weight of many of the challenges associated with protecting that organization's data. This can be a major selling point for customers. For the reasonable cost of an online data protection service, a customer can shift the pain points involved in maintaining software and hardware for data backups to a trusted third party.

Installation and Integration with Existing Technologies

Because cloud services are still relatively new to many customers, they don't understand how their current environment can work with or within a cloud environment. They may want to shift functions such as data protection to a third party but really don't know how. Integration is a key service a channel partner can offer customers who want to transition to a cloud-related data protection solution, either on a mostly do-it-yourself (DIY) subscription basis or as a fully managed service.

Service Level Agreements Guarantee Performance

Although the channel partner has a service level agreement (SLA) with its customers, the partner may also have an SLA with its vendor. The vendor SLA should have comprehensive terms and conditions that meet your needs and not simply a one-size-fits-all type of agreement. The strength of the SLA you sign with your vendor sets the stage for the type of service levels you can guarantee to your customers.

Customer Costs Move from CapEx to OpEx

The beauty of an online data protection solution, from a bean counter's point of view, is budget-ability. These types of solutions generally involve low or no startup fees (depending on the type of service and vendor) and predictable, monthly recurring costs—in most cases, a clean shift from unpredictable capital expenses and operating expenses to fixed operating expenses. Though online data protection costs go up as data volume increases, such increases can be tracked and predicted with reasonable accuracy.

Take Advantage of ROI Tools and Calculators

One important tool for analyzing and positioning backup and disaster recovery services in the cloud is a special-purpose ROI calculator. The Web is replete with such tools but they all encompass similar numerical components, in turn driven by costs of various approaches to handling backup and recovery. The key to using such a calculator, which is easy enough to build inside any spreadsheet program, is to capture the costs of two or more comparable solutions so that they can be compared over a common time period. The usual time period is three to five years, given standard depreciation schedules for capital assets.

> **Note**
>
> To find a free downloadable or online ROI calculator, search for "ROI calculator," "ROI calculator for backup and recovery," or "ROI calculator for disaster recovery."

Educating prospective buyers about how to compare costs for current systems and approaches vis-à-vis those for backup and recovery services can be a convincing experience in establishing and demonstrating the value of the service packages and options that resellers can provide to their customers. On the one hand, assessing costs for current systems invariably involves accounting for media or storage costs (for tape versus disk-based backup systems), and for the servers or other devices involved in making backups and providing file or image repositories from which restore operations may proceed. These costs include capital expenditures for hardware and the acquisition of software; they also include recurring costs for ongoing hardware and software maintenance and upkeep. Usually, those costs are dwarfed by the labor costs involved in initial setup, configuration, and deployment, followed by the regular effort expended in making and managing backups, and in performing restores when they're needed.

On the other hand, assessing costs for backup-as-a-service offerings involves explaining any upfront or startup costs necessary to adopt a service offering. The key component for recurring costs in this "service scenario" involves monthly subscription and service fees generally assessed on a per-site or per-server basis, along with storage-related costs associated with the amount of compressed and de-duplicated data that will be stored locally on appliances and in the cloud. Where service costs for restores and perhaps disaster recovery implementations also come into play, it's important to ensure customers understand all those components and the potential and likely cost scenarios. It's also important to stress the need for Internet bandwidth to move data for backups and restores, and to set customer expectations for the kinds of WAN links, communications charges, and related equipment or service charges involved in making the connections necessary for backup services to work properly and acceptably.

As customers work through the cost comparison process and learn to understand the returns on the investments involved, they will become more comfortable with transitioning to a backup service model. They will also appreciate the sometimes substantial benefits that such a switch can carry to their bottom line.

Summary

Customers who prefer a hands-on approach to data protection might be reluctant to switch to cloud-related services for data protection, and understandably so. Yet early adopters and technology movers will embrace the technology and ask what's coming next. The best approach to sales is to immerse yourself in the facts about cloud data protection—what it can deliver and what it cannot. Although your customers and prospects will vary, your role as trusted advisor should remain steady.