Realtime publishers

Protecting Client Data in the Cloud:
A Channel Perspective

The Essentials Series

What Are Cloud-Connected Data Protection Services About? Architectural Advice for Resellers

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

What Are Cloud-Connected Data Protection Services About? Architectural Advice for Resellers

Backup and data protection services that touch the cloud come in many forms, and offer an interesting mix of features and functions. Channel-oriented organizations, such as value-added resellers (VARs) and managed service providers (MSPs) looking to branch out, should understand how this technology and its overall delivery model work.

Data Protection Services and the Cloud

Generally speaking, the cloud refers to one or more data centers somewhere "out there" on the Internet, with services and storage accessible to authorized users or consumers of such things. Cloud-connected services (also referred to as "cloud-attached" or "hybrid") involve at least a modest local presence on a customer network, usually via resident software or a local appliance. Cloud-based services let customers back up multiple systems and applications using offsite solutions. Both of these offerings are designed to accomplish data protection, but each comes with its own pros, cons, and costs. Cloud-connected solutions can be attractive to customers because they include a local storage component that enables quick and easy local restore operations, which may not be available in purely cloud-based solutions. These offerings are structured to allow resellers to quickly deploy solutions to their customer base and ensure that customer data remains available and safe from disasters.

In a typical cloud-connected backup and recovery solution (see Figure 1), agents run on workstations and servers at a client site. During backup, the data is de-duplicated, compressed, and encrypted before transmission into the cloud. This conserves storage space and saves on expensive wide area network (WAN) bandwidth. Data is deposited into a storage vault at a data center—this is essentially the "cloud" in this model. Additional de-duplication may occur when data arrives at the storage vault as well. For redundancy purposes, data may also be replicated to multiple locations around the globe.

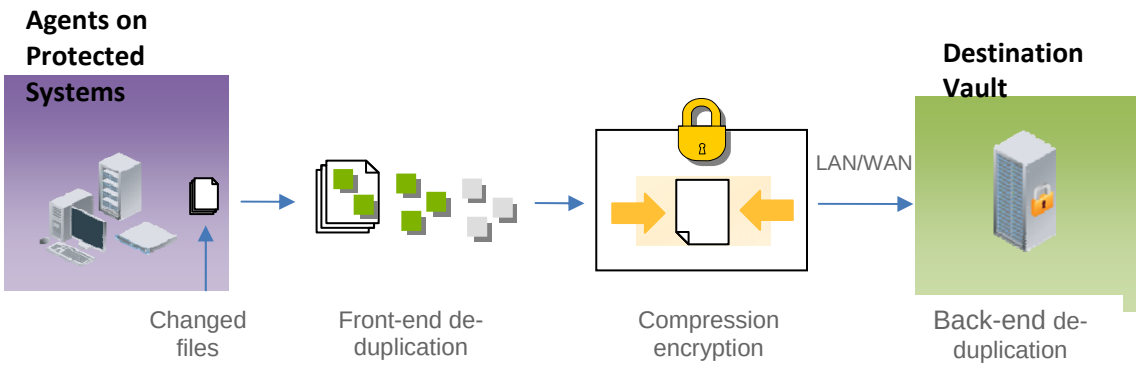

Figure 1: A cloud-connected backup and recovery model.

To obtain the full benefit of a cloud-connected deployment, involve a local disk-to-disk network copy, with subsequent LAN-to-WAN transfers of compressed and encrypted data to a vault somewhere in the cloud. Backup copies at the appliance level (disk-to-disk) are what support local restore or access operations, for added customer convenience. In addition, disk-to-disk-to-cloud data backup and recovery uses WAN-optimized connections for high-speed transfers and end-to-end encryption for security. Some vendors even offer single-pass restores for ease of use.

> **Note**
>
> Most vendors provide encryption for data in transit and stored data using the National Institute of Standards and Technology (NIST) 128-bit or the 256-bit Advanced Encryption Standard (AES).

A Look at Services and Products

Different technology vendors offer different ways for the channel to deliver cloud-related data protection services. Figure 2 shows several delivery methods that may involve software-as-a-service (SaaS), on-premise software, edge appliances, managed services, or various combinations of these elements.

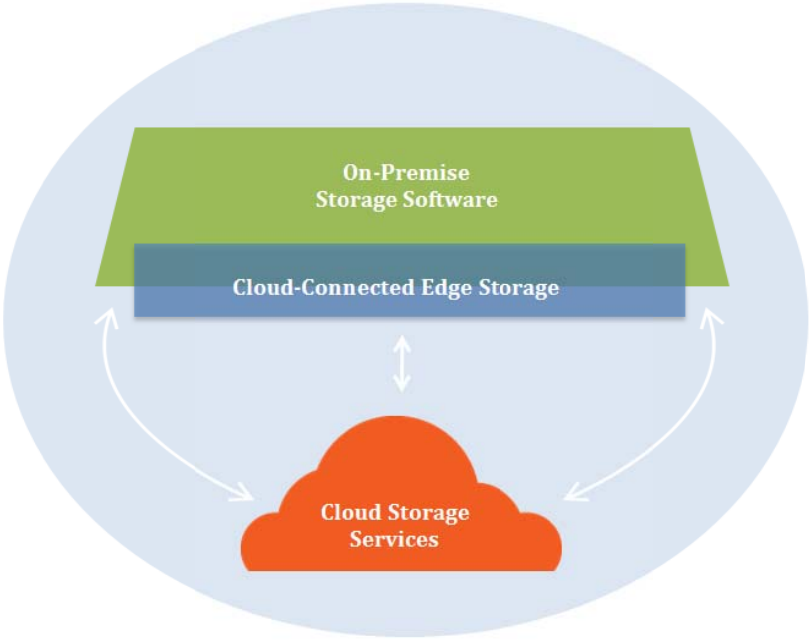

Figure 2: Cloud data protection delivery options.

- SaaS provides secure, efficient automated online backup and recovery. Connections are made over the Internet to cloud-based data center storage. SaaS includes an on-premise component that handles cloud communications on the customer's behalf, and provides backup and restore capability. Customers leave back-end vault management to the cloud vendor and will manage the agents themselves.
- On-premise software is local backup and recovery software. It consistently and continuously backs up open files onsite. Customers usually manage on-premise solutions themselves.
- Edge appliances provide complete on-premise data protection and can connect to cloud storage for redundancy. Here again, customers often manage their own edge appliances.
- Managed services allow resellers to administer a complete data protection solution on a customer's behalf; such offerings often include SaaS, edge appliances, and cloud storage services. Customers may pay more for such a full-service option but are then able to use onsite IT resources for higher-priority tasks and projects.

Collaboration Between Cloud Technology Vendors and Resellers

Within the "cloud," IT products and processes that traditionally operate onsite are offered remotely as services instead. This relatively new way of providing IT services is seeing explosive growth. In fact, managed services is the only technology space that grew during the recent recession. Everyone wants in, including telcos and technology vendors, some of whom are cutting out their channel partners and offering cloud services directly to their customers. This leaves many channel companies wondering how they'll remain competitive, or even how they'll remain in business.

But cloud-related business models actually offer new business opportunities for resellers wanting to become MSPs, or for companies wanting to expand their current portfolio of managed services. Who better to turn to for access to the cloud than a customer's trusted advisor—their local reseller? Customers find it easier to obtain cloud services from a trusted reseller rather than going directly to a big technology vendor, where they might not get the personalized service they're after. Many technology vendors still value the channel and see it as a necessary link between vendor and customer, and are finding ways to boost the partnership between themselves and their resellers so that everyone can thrive and succeed.

> "Forrester estimates that more than 60% of tech industry revenues are generated through channel partners, often by serving customers deemed otherwise unreachable by tech vendors."
>
> — Forrester Research (Source: Tim Harmon and Peter O'Neill. "Channel Models In The Era Of Cloud" whitepaper, November 3, 2010.)

Vendor-Partner-Customer Relationship Explained

In a cloud-based or cloud-connected data protection business model, channel partners can either resell the vendor's cloud service or they can provide online backup service themselves, while the technology vendor supplies hardware, software, and cloud replication services. Resellers fold the service into their portfolios, branding the service using their own service name followed by "powered by <vendor service or product>." Outright resale of cloud service involves less investment from resellers but also generates lower margins and profits. Creating and private branding their own services lets resellers achieve higher margins and profits but also involves higher investments in capital expenditures and human assets—so there are interesting tradeoffs involved all around.

One significant point to understand is that resellers continue to own the relationship with their customers, from sales to installation to maintenance to billing. The technology vendor may support the channel by providing hardware and software installation, training, and certification to partners. Some vendors even offer marketing development funds (MDFs) to help partners speed sales growth. Certain vendors also document best practices on running a cloud/SaaS business to help their partners develop and maintain key core competencies.

After installation, resellers provide first-level support to customers while the technology vendor backs them up with second-level support. This ensures that the customer receives reliable, dependable service and that the reseller can meet the stipulations of its service level agreements (SLAs). Finally, resellers bill customers for services provided while the technology vendor bills them in aggregate for all of their customers' access, subscriptions, and activities.

Costs and Margins Examined

When considering a shift to a cloud data protection business model, one of the primary barriers reported by channel partners is the high cost of building and maintaining the necessary IT infrastructure. However, entry costs to a cloud data protection business can be relatively tolerable, depending on the type of components or elements you choose to acquire (see Figure 3). And many partners can begin providing services to customers within weeks rather than months, reducing the return on investment (ROI) window.

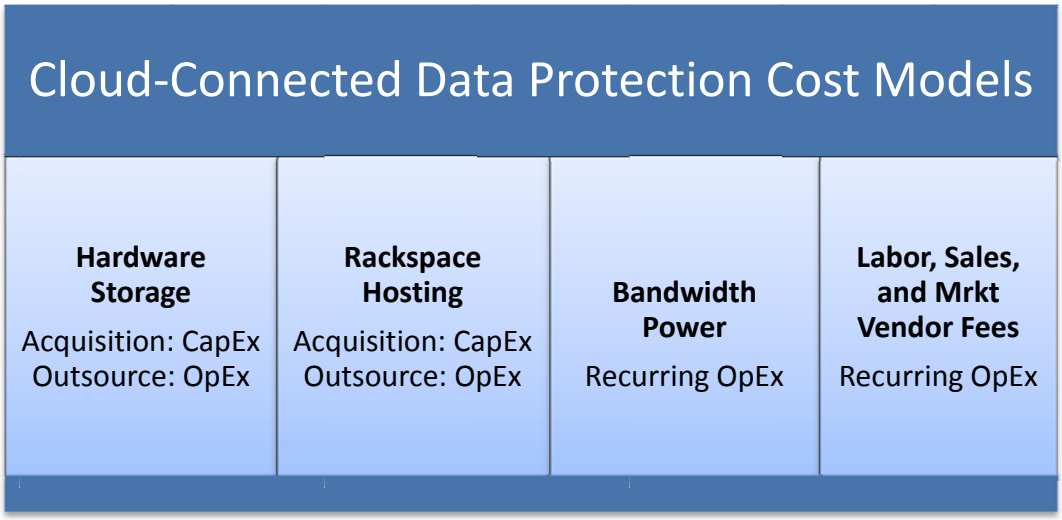

Figure 3: A comparison of cloud data protection cost models.

For resellers already doing business as MSPs that want to branch into backup and disaster recovery, or resellers intending to become MSPs, a range of investments and activities must be considered and decisions made as to buying and managing one's own assets versus outsourcing to make use of them.

For hardware and storage, resellers can decide if they want to operate their own infrastructures or outsource their infrastructures into the cloud. In the former case, resellers must take on construction or obtain access to a data center, then acquire the necessary network hardware (switches, routers, and load balancers), servers, and storage devices, all of which represent capital expenditures. Outsourcing means finding a provider for servers and storage, and arranging for SLAs to make sure the reseller's customers can obtain a satisfactory level of service. This trades CapEx for operating expenses instead.

Rackspace and hosting represent another approach to picking up the MSP role. Resellers can incur operational costs to move into a collocation facility or third-party data center, and lease rackspace which they then populate with their own equipment. Or they can contract with another third party to provide that equipment and operate it for them. The degree of hardware acquisition and ownership controls the tradeoffs between operational and capital expenditures in this kind of scenario.

Bandwidth and power represent classic consumption fees that will attach to any MSP scenario because resellers must use both electricity and Internet bandwidth to provide services to customers. This can involve substantial recurring costs, so resellers are well-advised to shop carefully for these services and to drive hard bargains for discounts.

As in any business, labor and overhead charges are important factors to consider in deciding whether to become an MSP. Labor can be a substantial portion of total costs and is likely to represent the majority of monthly recurring costs. Staffing for technical administration, customer installation and support, and general and administrative overhead must all be factored into this calculation. Sales and marketing costs are important, too, because the latter is needed to create customer awareness and drive demand, while the former is needed to service demand and maintain good working relationships. Finally, a reseller's chosen technology vendor will assess typical program fees: these include royalties or licensing fees, training charges, and installation and maintenance charges. Other items that can add costs are security, regulatory compliance measures, and disaster recovery efforts (including staff relocation to a hot site in the event of a disaster.

Summary

Cloud-related backup and data protection can be a lucrative offering for resellers, with surprisingly low entrance costs. Forming a partnership with the right technology vendor is key. It can make the difference between increasing the customer base and their loyalty versus sitting by the sidelines while competitors gain the industry spotlight and a market edge. In the next article in this series, find out how to expand a managed services portfolio by offering online data protection.