Data protection is a business imperative, but SMB technology teams cannot give data protection needs enough focus. This is where managed service providers can add tremendous business value with the right solutions.

Cloud Business Continuity and Disaster Recovery: Providing Peace of Mind to Small and Medium-Sized Businesses

November 2021

Written by: Shari Lava, Research Director, Automation within the AI and Automation Group

Introduction

In the past 18 months, small and medium-sized businesses (SMBs) have made dramatic changes to their technical environments, including their infrastructure and application mix, as they responded to the pandemic and the challenges of digitizing quickly. Before the emergence of COVID-19, SMBs were increasingly open to the idea of the cloud but were lagging enterprises in making cloud investments. That has changed, with cloud adoption growing significantly among SMBs. But the mix of new technology and legacy technology is creating challenges for SMBs, translating into business opportunities for managed service providers (SPs).

New technology being adopted by SMBs is putting significant pressure on the already constrained IT resources these businesses might have. According to IDC's *Worldwide Small and Medium Business Survey* from October 2020, only 43.6% of small businesses (those with fewer than 100 employees) have even one full-time person in IT. And those that do have IT resources on staff are still struggling with competing priorities while needing to upskill/reskill these employees to new technology, as those resources must be generalists overseeing a wide variety of technologies. Implementing this new technology has become a business imperative that SMBs can't accomplish without the help of technology partners.

With the change in technology deployment approach, most SMBs have reported outdated and limited skill sets in IT as being among the largest technology barriers to meeting business objectives, particularly for in-demand skills such as security. In addition, 41.1% of SMBs indicated that having too many reactive needs is preventing them from achieving strategic priorities, meaning that only tactical and reactive approaches are being used for data protection.

While data protection is a business imperative, technology teams cannot give these needs enough focus, which might mean they think they are adequately protected by simply having public cloud services. This is where managed SPs can add tremendous business value with the right solutions. SMBs that have even a single IT employee are more likely to use service providers to help manage the parts of the technology environment that don't require the precious organizational knowledge that full-time IT employees tend to have. Managed SPs should capitalize by getting cloud certified, ramping up on cloud offerings, and providing differentiated services and support.

AT A GLANCE

WHAT'S IMPORTANT

» 36% of all SMB IT spending is being dedicated to cloud services in 2021.

» Only 43.6% of small businesses (those with fewer than 100 employees) have even one full-time person in IT.

» Most SMBs are using multiple tools to manage their environments, increasing complexity, requirements, and administration burden.

The State of Data Protection and Backup

Most SMBs understand neither the link between data backup/protection, disaster recovery and emerging cyberthreats even if they do have IT staff nor their obligations in their cloud providers' shared responsibility model. Too many SMBs assume their cloud providers are delivering data backup and protection services as part of the utility service they purchase. This is frequently not the case, leaving SMBs vulnerable to data loss as a result of error or bad actors. Further, even when the provider does have some backup protection baked in, the service-level agreements (SLAs) for data recovery and restoration will often still lead to some data loss for SMBs. With threats increasing while SMB users are also getting used to new technologies, the risks to business continuity multiply.

The types of technologies that SMBs are using to protect business data are also increasingly complex, with most SMBs using multiple methods in their hybrid environments (see Figure 1). This complexity increases the risk of overburdening stretched resources, where staff must learn, maintain, and verify multiple tools, including in some environments that are unfamiliar. The use of multiple tools also leads to higher and unpredictable costs for SMB customers, which can be a barrier to adopting more robust tools.

FIGURE 1: *Top Choices for Data Backup, Data Protection, and Disaster Recovery*
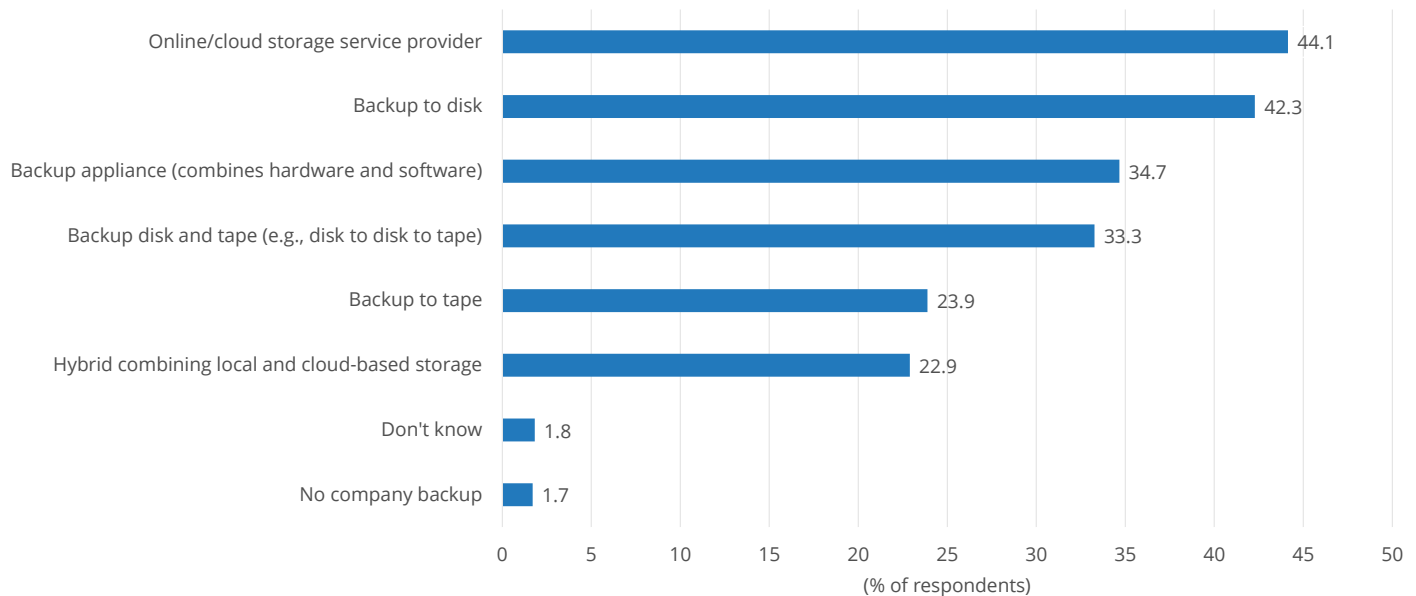
n = 2,493

Source: IDC's Worldwide Small and Medium Business Survey, October 2020

Managed SPs that can streamline both the management and the toolset of data protection can provide SMBs with reliable and differentiated services that can protect business value while reducing complexity.

Definitions

IDC provides the following definitions as a baseline for understanding the cloud-based business continuity market and the paper's content:

» **Public cloud:** Computing that is based on a service composition model and on-demand delivery of IT resources via the internet with pay-as-you-go pricing (It is like a utility because it is a computing environment where unrelated customers can acquire technology such as compute power, storage, databases, applications, and other services on an as-needed basis.)

» **Hybrid infrastructure:** The integration and orchestration between a private environment including on-premises and private cloud and one or more public clouds

» **IaaS:** Servers, system management, and security services delivered via a public or private cloud

» **PaaS:** Application development/deployment and middleware delivered via a public or private cloud services model

» **Data protection:** The act of safeguarding critical business data and making it available in all circumstances (Safeguarding includes using governance and technology tools to protect data from privacy and security threats as well as ensure data integrity is not compromised. Having a robust data protection plan for key business data is typically a key component of a disaster recovery and business continuity plan.)

» **Data backup:** The act of making backup copies of key business data to ensure data can be recovered and the business can resume normal activities (Data backup is a key part of any data protection plan and must include a plan for all application, user, and system data in the hybrid infrastructure world in which many SMBs are currently operating.)

» **Business continuity and disaster recovery (BCDR):** A plan typically developed by a business to ensure that if key systems become unavailable by accident, through disaster, or through security threats, the business has a plan to reestablish itself, complete with business systems and data that can be executed quickly to help the business recover (A strong BCDR plan not only will provide a playbook for IT resources to restore the business technology operating environment but also will be tested frequently to ensure the plan is up to date.)

» **Small and medium-sized business (SMB):** Any business in any industry with 1–999 full-time employees, not including the business owner (A small business is defined as a business with 1–99 employees, and a medium-sized business is defined as a business with 100–999 employees.)

» **Workloads:** The types of processing that consume IT computing resources, including applications, databases, and other user requests

Key Trends

Several trends are impacting the need for SMBs to seek new service provider support, including cloud adoption, rising cyberthreats, and vulnerabilities in the SMB technology architecture.

In 2020, cloud services — including SaaS, PaaS, and IaaS — became the single largest spend category in the IT budget, overtaking hardware and traditional software for the first time. That trend is expected to continue in 2021, with 36% of all SMB IT spend being dedicated to cloud services. What's more, the smallest and largest SMBs are adopting cloud the most, whereas those with 50–499 employees are still adopting more cloud than hardware and traditional software but also have more on-premises investments that are not yet ready for migration.

At the same time, the frequency of cyberthreats is increasing, and while many SMBs are becoming more aware of these threats, many wrongfully assume that their business is not a large enough target for bad actors. There are several reasons this is not the case. First, as the number of bad actors increases, so too does the risk to businesses of all sizes. Also, many businesses are not aware that bad actors can also use technology to automate and scale their cyberattacks to hit multiple targets with a high level of sophistication. While most SMBs have purchased protection for email and network device security, many have not safeguarded against other threats that can leave them exposed, particularly to ransomware.

In fact, recent IDC research indicates that while ransomware is among the top security concerns of SMBs, only 9.8% of small businesses and 13.5% of medium-sized businesses are planning to implement protection. Managed SPs are uniquely positioned to provide solutions and services to support a comprehensive data backup, protection, and recovery plan. This includes everything from educating SMBs about threats to their business to building and executing the BCDR plan.

To provide a service that can be reliable for the SMB customer while scaling to accommodate the business needs of the provider, managed SPs need effective, multicustomer solutions with the flexibility to manage individual customer environments at scale and monitor operations across customers.

Benefits of Cloud Data Backup and Protection Solutions for Managed SPs

Cloud data protection and backup technology that is specifically designed for managed service providers, which must be able to frequently see environment health at both the macro level and the micro level, can benefit managed SP customers in the following areas:

- » **Predictable pricing:** Managed SPs need to be able to anticipate their cost to serve to correctly price their own solutions and services to customers to achieve a fair price. Not all data protection solutions for the cloud can do this without requiring the managed SP to estimate public cloud costs or unexpected charges. In fact, many data backup solutions come at unpredictable price points, and final price is determined by amount of data, tests conducted, and egress charges for data restore.

- » **Solution designed specifically for managed SPs:** Data protection solutions designed for a single customer's environment can be much more difficult for a managed SP to use, particularly if multiple solutions are needed to serve various customers. This increases the cost to serve each customer and can make it more difficult to monitor customers at that macro level.

- » **Workloads that are backed up hourly:** Customers need more robust and frequent backup capabilities than what many legacy backup solutions provide. Managed SPs must adopt solutions that will minimize the potential data loss for their customers if they are to provide strong business value to the SMB when an event occurs.

- » **Immutable architecture:** To minimize threats and disruption, managed SPs need to utilize tools that are much less vulnerable to attacks, as bad actors will target managed SPs because they can, in effect, target multiple customers at the same time. Enhanced tenant security controls are solutions designed to exclusively protect managed SP environments and secure individual tenants with an extra level of security controls and encrypted disks per client tenant for more business value.

- » **Simple restore process:** When data loss does occur, customers of a managed SP want the peace of mind that systems, data, and applications can be restored quickly. Managed SPs need to use tools that simplify the restore process, even in public cloud environments.

»   **Single pane of glass for hybrid environments:** Most SMBs are still operating in hybrid environments and will be for the foreseeable future. They do not want to manage multiple service providers and solutions; they would rather work with a service provider that can protect their infrastructure no matter where it resides. Managed SPs that use tools that can do this will be able to differentiate themselves.

»   **Screenshot verification:** One of the biggest concerns SMBs have with using service providers for data protection/backup is to know the backups are being done correctly. Managed SPs should make use of tools that can simplify this process so that SMBs can have confidence in their services.

»   **Total cost of ownership:** Managed SPs need tools that can allow them to scale operations while retaining as much revenue as possible. Tools that are specifically made for managed SPs can provide a lower total cost of ownership, which can maximize revenue and at the same time provide competitive pricing to the SMB.

To enable these types of benefits, managed SPs must modernize product portfolios to be able to offer clients the scalability and efficiency of the public cloud and create new revenue opportunities for the business.

Considering Datto

Datto is a provider of global cloud-based software and security solutions purpose built for delivery by managed SPs. The company's Unified Continuity, Networking, and Business Management solutions are intended to drive cyber-resilience, efficiency, and growth for managed SPs. Delivered via an integrated platform, Datto's solutions are designed to help the company's global ecosystem of managed SP partners serve over 1 million businesses around the world. The solutions are meant to defend against costly downtime and data loss in servers, virtual machines, and cloud applications, or anywhere data resides, by providing proactive dynamic detection and prevention to fast, flexible recovery from cyberincidents. Datto also has a strong partnership with Microsoft, a key technology partner of many managed SPs with a technology footprint in many SMBs.

Datto Continuity for Microsoft Azure is a BCDR solution that is built exclusively for managed SPs and provides the ability to customize protection and streamline recovery for critical business infrastructure residing in Microsoft Azure. It is intended to allow managed SPs to efficiently manage on-premises and cloud backups from a single dashboard while protecting managed SP customers from ransomware and other security threats using encrypted discs and an immutable cloud architecture.

Datto Continuity for Microsoft Azure is replicated every hour to the secure Datto Cloud. Offering daily backup verification and optimal recovery time objective (RTO) and recovery point objective (RPO) performance, the solution makes it simpler for managed SPs to deliver reliable business continuity services — at a predictable cost — without the need to piece together individual technologies or depend solely on Microsoft. The solution includes access to technical experts, saving time and eliminating confusion when an issue occurs.

Datto has received a considerable amount of recognition in the industry for its rapid growth, product excellence, and superior technical support, including the following:

»   2021 MSP Innovation Awards: Best backup/continuity offering (won in the United Kingdom and North America)

»   2021 CRN Annual Report Card Survey: Top grades in data protection and management

»   2021 CRN Partner Program Guide: 5-star data storage and backup vendor

Challenges

The public cloud market has grown extensively since the pandemic, with many cloud vendors increasing their mindshare and market share with SMBs. Microsoft's Azure Cloud services is one of the top 3 choices among SMBs, which is particularly important given Datto's partnership. But more and more, SMBs are operating in hybrid environments that include a combination of on-premises and cloud workloads, meaning they need to ensure that workloads in multiple locations are secure and recoverable.

The data protection market is also an established market, with many competitors refactoring their offerings for a cloud-first world. According to Datto, it serves more than 16,000 managed SPs today. Leveraging this strong focus, Datto will need to continue to build mindshare and partnerships with managed SPs to maintain and build on its reputation as a trusted cloud BCDR provider.

SMBs, which are the end customers of many managed SPs, are not always clear that the data backups provided by cloud vendors are not as comprehensive as their own on-premises backups might be. Managed SPs are often on the front lines to educate SMBs about the business risks they face as well as the increase in both the number and the dynamic nature of threats.

Conclusion

Given the enduring need for better access to company resources, the unprecedented growth in cloud adoption by SMBs, and the scarcity of technical skills within SMBs, IDC believes the cloud data protection/backup market and managed services offerings will continue to grow. To the extent that Datto can provide managed SPs with tools that are scalable and optimized to help them address the challenges of SMBs as described in this paper, the company has a significant opportunity for success.

About the Analyst

Shari Lava, *Research Director, Automation within the AI and Automation Group*

Shari Lava is Research Director, Automation within the AI and Automation Group. Ms. Lava's core research coverage includes the fast-changing automation and API management software space. Based on her background in enterprise applications and data integration, Ms. Lava's research also includes an emphasis on understanding the market and adoption of these key technologies that are integral to business productivity and success. She is based in Toronto, Canada.

MESSAGE FROM THE SPONSOR

About Datto

Datto Continuity for Microsoft Azure provides MSPs with a premium level, business continuity, and disaster recovery solution for the critical workloads residing in Microsoft Azure. With the Datto Continuity for Microsoft Azure solution, MSPs can feel confident that their clients' cloud data is backed up and recoverable within minutes.

»   To learn more about Datto Continuity for Microsoft Azure, visit www.datto.com/azure

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.