A Business Value White Paper, sponsored by Microsoft Azure

IDC

The Business Value of Azure Site Recovery and Azure Backup

RESEARCH BY:

Harsh Singh
Senior Research Analyst,
Business Value Strategy Practice, IDC

Phil Goodwin
Research Vice President, Infrastructure Systems, Platforms and Technologies Group, IDC

February 2022 | IDC Doc. #US48616721

Navigating this White Paper

Click on titles or page numbers to navigate to each section.

BUSINESS VALUE HIGHLIGHTS

Click on highlights below to navigate to related content within this white paper.

370%
five-year ROI

8 months
to payback

46%
reduced total cost of operations

97%
reduced lost end-user productivity from data loss

48%
faster backups

80%
reduction in average data recovery time

100%
successful backup reliability

20%
more efficient data protection and data recovery teams

93%
reduction in unplanned downtime

18%
more efficient IT infrastructure teams

13%
more productive application developers

Executive Summary

IDC research shows that more than 90% of organizations utilize the public cloud for some data protection capabilities. Moreover, we forecast that by 2025, 55% of organizations will have migrated their data protection systems to a cloud-centric model to centrally manage core, edge, and cloud data protection from the cloud. Certainly, organizations will have applications deployed on core, edge, and cloud, but as more applications and data are deployed in the cloud, the balance of resources will tip to the cloud. These cloud data protection deployments (of which many will be "as a service") will have the breadth and capability to manage data protection across private and public cloud repositories.

Our research finds that cloud data protection as-a-service (DPaaS) solutions are proliferating rapidly. DPaaS includes backup as a service (BaaS), disaster recovery as a service (DRaaS), and archive as a service (AaaS). We forecast this market will grow from $10.5 billion in 2021 worldwide to $18.4 billion in 2025 (19.1% compound annual growth rate (CAGR)), representing the fastest-growing segment of the broader data protection market.

Providers of DPaaS solutions, both managed service providers (SPs) and cloud service providers have likewise proliferated. The result is thousands of competing companies and solutions, making differentiation difficult and a challenge for IT buyers to determine the correct solution for their situation. Vendor claims and counterclaims may be difficult to verify, raising the risk of a poor choice. Thus, independent empirical data about solutions is at a premium.

In this spirit, Microsoft engaged IDC to conduct an independent business value study of its Azure Site Recovery and Backup. IDC conducted interviews with a variety of organizations that had adopted Microsoft Azure Site Recovery and Backup as their primary backup and disaster recovery platform. This solution has been designed to cost-effectively and reliably

deploy and manage replication, failover, provisioning of backup resources, and recovery processes to ensure that business-critical applications continue running during planned and unplanned outages and disruptions in business continuity.

Based on a series of in-depth interviews, IDC found that participating organizations realized significant IT and business benefits from Azure Site Recovery and Backup through:

- **Reduced planned and unplanned downtime,** thereby increasing end-user productivity and lowering business risk
- **Optimized overall performance, speed, and reliability** of backup and data recovery (BDR) operations
- **The provision of a more cost-effective structure** for backup and data recovery hardware and software and staff operations
- **Improved productivity** of IT infrastructure, backup and data recovery, and application development teams

Situation Overview

The data management landscape has become increasingly diverse, fragmented and, in many cases, siloed. Our research also finds that data is increasing at a 35–43% CAGR, depending upon company size, industry, and other factors. This means that data volumes are doubling roughly every three years for most organizations. Presently, 50% of data is in the core, 22% in the cloud, 19% at the edge, and 9% in other locations. However, the cloud and edge have the fastest growth rates. In addition, we forecast that 80% of new application deployments will be in the cloud or at the edge, driving further data growth in these areas.

Data becomes siloed for a number of reasons: data location, data type, applications, data owners, data governance, and other factors. As a result, organizations are compelled to adopt multiple data protection strategies and solutions to address the various scenarios. Organizations commonly have three to four different backup solutions that create redundant toolsets and IT skill challenges as well as unnecessary costs of purchase, maintenance, and labor.

By adopting a cloud-based data protection strategy, IT organizations can get out in front of evolving data protection challenges. Data is growing fastest in the cloud and DPaaS solutions are properly positioned to protect both cloud-native applications and SaaS applications directly and efficiently. These solutions offer the advantage of on-demand resources, consumption-based pricing, and the ability to tier between on-premises and cloud bidirectionally with encrypted and immutable repositories as an option to address ransomware. DPaaS solutions also remove the need for IT organizations to directly manage and update infrastructure resources, freeing up the IT team to tackle more strategic activities.

Azure Site Recovery and Azure Backup

Azure Site Recovery and Azure Backup offer IT organizations the breadth of daily backup and recovery requirements and disaster recovery. Although available separately, these solutions combine to offer as-a-service convenience for cloud and on-premises requirements.

Azure Backup offers a range of backup functionality, including:

- **Centralized management for on-premises and cloud backup jobs** using Backup Center
- **Support for a wide range of workloads,** including virtual environments, SQL Server, SAP HANA, Azure files, Azure Database, and PostgreSQL.
- **Automatic configuration of backup jobs on production virtual machines** (VMs) using Azure Automanage
- **Encrypted backups** using 256-bit advanced encryption standard (AES) custom managed keys
- **Database consistent snapshots for Oracle and MySQL** on Linux VMs in Azure
- **Managed costs with the Optimize tab in Backup reports,** using the pricing backup estimator and resources across Azure
- **Compliance on a wide range of certification standards,** such as HIPAA, HITRUST, FedRAMP, and SOC

Azure Site Recovery extends data protection into DR with the following capabilities:

- **On-demand infrastructure** to fully restore application environments to a production state
- **Recovery of onsite workloads** to the cloud or cloud workload in the cloud
- **Compliance** with ISO 27001
- **Combine with high-availability configurations** for maximum application uptime

Both Azure Backup and Azure Site Recovery are automatically updated with new Azure capabilities as they become available.

The Business Value of Azure Site Recovery and Azure Backup

Study Demographics

IDC conducted research that explored the value and benefits of using Azure Site Recovery and Backup to optimize backup and data recovery operations. The project included eight interviews with organizations that were using the Azure platform. Interviewed managers all had experience with and knowledge about Azure's benefits and were asked a variety of quantitative and qualitative questions about the solution on their IT/BDR operations, core businesses, and costs.

Table 1 presents study demographics. The organizations that IDC interviewed had an average base of 37,919 employees and total average annual revenue of $8.0 billion, indicating the involvement of several large organizations. This workforce was supported by an IT staff of 6,819 supporting 630 business-critical applications on behalf of 36,669 end users. In terms of geographic distribution, four companies were based in the United States, with the remainder in the United Kingdom, India, and Singapore. In addition, a variety of vertical markets were represented, namely, the professional services, financial services, telecommunications, government, and information technology sectors.

TABLE 1

Firmographics of Interviewed Organizations

	Average	Median	Range
Number of employees	37,919	28,000	2,000 to 130,000
Number of IT staff	6,819	600	53 to 35,000
Number of IT users	36,669	28,000	2,000 to 130,000
Number of business applications	630	200	28 to 1,500
Organizational revenue	$8.1B	$3.3B	$470.0M to $20.0B
Industries	Professional services (2), financial services (2), telecommunication (2), government, information technology		
Countries	United States (4), United Kingdom (2), India, Singapore		

Source: IDC In-depth Interviews, August 2021

Selection and Use of Azure Site Recovery and Backup

The organizations that IDC interviewed described typical usage patterns for their IT environments, BDR operations, and Azure Site Recovery and Backup utilization. They also discussed the rationale behind their choice of Azure as an optimal means of enhancing their BDR infrastructure and operations. Study participants recognized the critical importance of protecting data to avoid being caught off guard when disruptive or catastrophic events occurred that had the potential to interrupt the continuity of their businesses.

Study participants cited a variety of reasons for choosing Azure Site Recovery and Backup. They recognized the need to ensure that their disaster recovery operations were using the best available technology and appreciated the need to migrate from high-maintenance legacy approaches. Increasing speed of recovery was emphasized as an obvious and critically important decision factor. Other important criteria centered on the need to significantly reduce the costs of existing on-premises BDR infrastructure that extended beyond a useful life cycle.

Study participants made detailed comments on these benefits:

- **Need to update disaster recovery infrastructure:**
  "Our primary applications are on Azure, and the remaining 20% are on premises because they run on older technology. To rewrite those systems to run in the cloud would require over two years of application changes, so we are still leaving these legacy applications on premises. The primary reason for the move is around our DR project because we were way behind from a resiliency standpoint with respect to disaster recovery and business continuity. Our key applications could no longer restore quickly enough to satisfy the business needs, and it was costing us money."

- **Reducing IT infrastructure footprint needed for BDR:**
  "Approximately two years ago we started the journey to eliminate a footprint in a colocation datacenter in Delaware. It was just becoming too costly from a hardware and leasing perspective. We decided it was much more cost-effective to move our recovery and backup to the cloud. That's when we went to Azure."

- **Minimizing downtime and data loss:**
  "The main purpose is to maintain the application availability and disaster recovery if an application or virtual server is down so that it will be available in some other zone and end users won't face any downtime. The business will run as normal and there will be no data loss."

- **Supporting customers and internal systems:**
  "We have two very specific use cases for Site Recovery. The first one is on a business level where we actually supply that as a service to our customers. Internally, we use it specifically for corporate systems and not customer-facing systems."

Table 2 provides a snapshot of the IT environments that are supported by Azure Site Recovery and Backup at the time of interviews. The overall IT footprint was substantial. The total number of virtual machines in active use across all organizations was 3,238 with 784 physical servers in play. Organizations were using these compute resources to provide 165 business applications to business end users and customers. The full array of computer resources was supported by 2,530TB dedicated for data repository and/or storage use. IDC calculated that 21% of these companies' revenue base was supported by Azure Site Recovery and Backup. Additional metrics are presented, and all numbers cited represent averages.

TABLE 2

Organizational Usage of Azure Site Recovery and Backup

	Average	Median
Number of Azure Backup systems	31	6
Number of TBs for Azure Backup systems	284	135
Number of datacenters	10	3
Number of TBs	2,530	421
Number of countries supported	13	5
Number of sites/branches	31	25
Number of Azure server instances	1,002	213
Number of applications	165	83
Number of internal users	9,516	6,150
Number of physical servers	784	200
Number of VMs	3,238	600
Percentage of revenue being supported	21%	13%

Source: IDC In-depth Interviews, August 2021

The Business Value and Quantified Benefits of Azure Site Recovery and Backup

IDC's research demonstrates the value for study participants in the decision to adopt Azure Site Recovery and Backup. Interviewed organizations reported an ability to improve the overall productivity and efficiency of their IT infrastructure, BDR, and application development teams, which served to reduce BDR management burden. Along with improvements in BDR features and functionality (such as multitiered layers of protection and better agility), the Azure platform served to optimize the performance, speed, and reliability of the BDR operations while providing a more cost-effective infrastructure and operation. In addition, reducing the incidence of planned and unplanned downtime led to better availability of services and applications for end users and customers, leading to improved productivity and customer satisfaction.

Study participants commented on these core benefits:

- **Reduced management burden:**

  "It's the redundancy and resiliency that the cloud gives us. If Azure gets attacked, it's their responsibility to get things back in business, spun up, and switched over to hot backup sites. This happens in the background automatically as part of our Azure fee. When my guys have to do all that with things on premises, it becomes an incredibly taxing endeavor that is very slow and cumbersome. It's better for me to pay one fee as a subscription and have someone else responsible."

- **Good customer satisfaction and easy integration:**

  "The first thing is customer satisfaction because the application is not down, so whatever is requested is submitted and there's no loss of data. There is also less load on IT maintenance, so we don't need extra manpower to set anything up. And the support costs also have been reduced by 45%."

- **Multitiered layers of protection:**

  "I would say [we get] flexibility and defensive depth with these layers of protection. We have different solutions and technologies that are meant to protect that information and replicate it so that it can be recovered at any time. One or many of those could be impacted, and that's why you have layered defense in place to make sure that if one fails, another is able to recover and provide that ability to get things back up and running quickly."

- **Improved agility:**

  "It would be the speed of recovery and the ability to bring up test DR environments quickly. Before, it would require this orchestration throughout the organization to schedule a test, schedule downtime, allocate equipment, provision it, and set it up. [Microsoft Azure's] got all that stuff all done already. So you just can call them up, send an email, or go through the portal and say, 'I need six Hyper-V VMs at this speed with this much storage or this much compute power, and this much network.' And, literally in 10–15 minutes, they could have it stood up. You could be testing these applications, and it doesn't impact anybody. You don't have to bring people in on weekends, so it's not as error-prone because people can make mistakes. Code changes could inadvertently be made. And you don't have to go through as much change management and approval."

Better Backup and Disaster Recovery Operations

IDC research has shown that many businesses are inadequately prepared for the advent of large-scale disruptions, which can have serious short- and long-term consequences for business continuity, financial results, and company reputation. When companies fail to invest in the best available technology to effectively respond to such events, they run the risk of unacceptably long recovery times, significant data losses, and costly business interruption

Given these realities, there is a strong need for IT organizations to optimize existing data protection and BDR profiles, especially with respect to the limitations of on-premises environments. With the goal of helping companies meet these challenges, recent advances in cloud-based data protection now offer an array of benefits such as improved economies of scale that make such approaches more accessible for small-and medium-sized businesses. By taking advantage of these cloud economics, IT organizations can benefit from offsite recovery capabilities that are highly automated, versatile, and efficient.

One such approach is Azure Site Recovery and Backup, a DRaaS native-cloud solution designed to protect workloads by providing disaster recovery failover from on-premises environments to the Azure cloud as well as offering Azure-to-Azure cloud recovery. The platform works for virtual infrastructure workloads, including Hyper-V or VMware, as well as physical workloads. Azure Site Recovery and Backup includes data replication, workload migration, and recovery orchestration functionality.

Study participants reported that the Azure platform was manifestly easier for IT to use and configure. Better ease of management could be traced to the automation of routine processes such as patching and updates, which alleviated staff workloads and enabled a shift of focus to higher-value tasks. Interviewed companies also called out reductions in planned and unplanned downtime as a key benefit. In the case of the former, this was because Azure allowed IT organizations to test DR failover without interrupting production workloads. The ability to shorten backup recovery windows was another important benefit called out.

Study participants commented on these and related benefits:

- **More layers of protection and improved data recovery:**
  "We have peace of mind knowing that we would be able to recover the impact from a possible ransomware attack. Because of layers we have built into the replication and recovery environment, there's a better chance we're going to be able to recover in a shorter period of time."

- **Freed up staff to work on higher-value work:**
  "We've got new levels of automation, so we don't have somebody running a utility to check for duplicate files. We've been able to shift people from low-value to higher-value work."

- **Reduced downtime:**
  "Azure offers 5–9s reliability. Our systems do as well but we do monthly downtime for backup and maintenance. One Saturday a month we'll be down, whereas Azure never seems to go down."

Interviewed companies reported that they were able to minimize the frequency and impact of unplanned downtime as a core benefit of Azure Site Recovery and Backup. For end users, business partners, and customers, this translated into an improved IT experience with less risk of being blindsided by outages involving key applications and services.

As shown in **Table 3**, Azure customers were able to reduce the impact of disruptive events by more than half (57%) on average. Further, when disruptions did occur, BDR teams were able to remediate them significantly faster (83%). These benefits combined for a productivity boost of 93%, resulting in an annual business value of $892,000 per organization.

TABLE 3
Unplanned Downtime Impact

	Before Azure Site Recovery and Backup	With Azure Site Recovery and Backup	Difference	Benefit
Frequency per year	15.4	6.6	8.8	57%
Mean time to resolve (hours)	3.3	0.6	2.7	83%
Lost productive time per employee (hours)	0.7	0.1	0.7	93%
FTE impact: Lost productivity due to unplanned outages	13.8	1	12.7	93%
Value of lost productivity per year	$963,000	$72,700	$892,000	93%

Source: IDC In-depth Interviews, August 2021

IDC then looked at the effectiveness of Azure Site Recovery and Backup in preventing data loss. Interviewed companies cited a number of positive benefits in this category. As one study participant noted: *"The biggest benefit is the integration … because mean time to resolve (MTTR) and the ability to troubleshoot becomes much easier. Also important is the confidence that we have about dealing with a crisis, particularly things like ransomware attacks. The ability to recover is greatly enhanced."*

IDC quantified impacts associated with data loss. As shown in **Table 4** (next page), after adoption, Azure Site Recovery and Backup helped interviewed companies substantially reduce the number of data losses occurring annually (83%). The same degree of improvement was experienced with respect to recovery time needed to restore lost or corrupted data. These two improvements combined to yield a BDR staff productivity boost of 97%. IDC calculated that this amounted to an annual business value of $976,000 per organization.

TABLE 4

Data Loss Impact

	Before Azure Site Recovery and Backup	With Azure Site Recovery and Backup	Difference	Benefit
Frequency per year	1.4	0.2	1.2	83%
Mean time to resolve (hours)	9.2	1.5	7.7	83%
Lost productive time per employee (hours)	0.7	0	0.7	97%
FTE impact: Lost productivity due to unplanned outages	14.3	0.4	13.9	97%
Value of lost productivity per year	$1.0M	$27,900	$976,000	97%

Source: IDC In-depth Interviews, August 2021

The Azure platform is designed to be simple to deploy and manage. Deployment is facilitated by replicating an Azure VM to a different Azure region directly from the portal. In addition, the platform is automatically updated with new features as soon as they are released. As one study participant noted: *"Now that we've got Site Recovery, we know it works. We test it twice a year and that's it. It's no longer an issue. We don't have to think about it or put any IT time or effort or manpower toward it, so we are quite happy with that. There are many other features, but we're quite happy with what works currently. It helped reduce some operational cost, and now it's easier to work with the systems."*

Study participants confirmed that IT staff responsible for BDR found the Azure platform easier to manage and use. **Table 5** (next page) quantifies these benefits and shows that study participants were able to capture substantial value from new team efficiencies, thereby helping minimize risk exposures. Interviewed companies saw a 20% improvement in overall team efficiency, which equates to about 6.2 full-time equivalents (FTEs) worth of time that can now be spent on strategic and other tasks. On an annual basis, this translated into FTE staff savings of $624,000.

TABLE 5
IT Data Protection and Data Recovery Staff Impact

	Before Azure Site Recovery and Backup	With Azure Site Recovery and Backup	Difference	Benefit
Management of data protection and data recovery (FTEs per organization per year)	31.2	25.0	6.2	20%
Staff time cost per year	$3.1M	$2.5M	$624,000	20%

Source: IDC In-depth Interviews, August 2021

IDC further drilled down on how the Azure platform impacted backup operations. Study participants consistently reported that Azure Backup's functionality helped their BDR teams run more backup operations and do so with greater efficiency. As one study participant noted: *"We don't have to keep up with the patching and latest and greatest with the strategy around it. We can just focus on business rather than having people monitor, track the backups, and make sure that everything works. … [It's] simplifying our engineering around it so we can focus more on overall digital transformation."*

As shown in **Table 6**, after adoption, the number of monthly backups performed increased 81% while successful completion of backup window targets saw a 39% improvement. Other improvements were seen in two additional metrics: **the average staff time needed to perform backups (48%) and backup reliability (6%).**

TABLE 6
Backup Metrics Impact

	Before Azure Backup	With Azure Backup	Difference	Benefit
Number of backups performed per month	38.6	70.0	31.4	81%
Data backup window targets (hours)	4.8	3.0	1.9	39%
Average staff time needed (hours)	3.0	1.6	1.4	48%
Backup reliability (backups that are successful)	94%	100%	6%	6%

Source: IDC In-depth Interviews, August 2021

IDC then evaluated Azure's impacts on recovery operations. Interviewed companies reported that the Azure platform helped their organizations perform data recovery tasks more efficiently. As shown in **Table 7**, after adoption, companies experienced an 80% improvement in two key metrics: **average data recovery window** and **average staff time needed per data recovery effort.**

TABLE 7

Data Recovery Impacts

	Before Azure Backup	With Azure Backup	Difference	Benefit
Average data recovery window (hours)	4.0	0.8	3.2	80%
Average staff time needed per data recovery effort (hours)	2.5	0.5	2.0	80%

Source: IDC In-depth Interviews, August 2021

From the perspective of IT infrastructure teams, Azure Site Recovery and Backup was easier to manage as organizations saw value in shifting workloads away from their on-premises setup to Azure cloud. As shown in **Table 8**, interviewed companies saw a 18% FTE-based productivity boost leading to an annual business value of $859,000.

TABLE 8

IT Infrastructure Management Staff Impact

	Before Azure Site Recovery and Backup	With Azure Site Recovery and Backup	Difference	Benefit
IT infrastructure management (FTEs per organization per year)	48.3	39.7	8.6	18%
Staff time cost per year	$4.8M	$3.9M	$859,000	18%

Source: IDC In-depth Interviews, August 2021

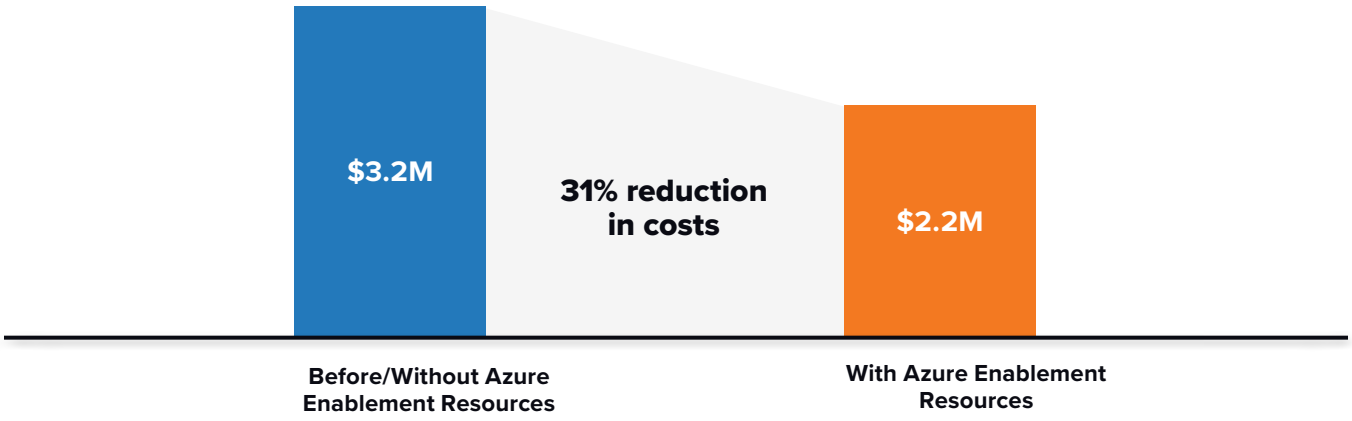
Cost-Effective Data Protection and Backup Operations

In addition to the operational benefits previously described, interviewed companies reported that Azure provided a cost-effective approach to BDR systems functionality in terms of hardware/software capex and opex. Study participants reported that in addition to staff-related cost savings, the use of cloud-based infrastructure eliminated the need to invest in higher-maintenance on-premises solutions. IDC evaluated infrastructure savings for interviewed companies and compared cost data against typical alternatives. These calculations are presented in **Figure 1**, showing a 31% reduction in costs.

FIGURE 1

IT Infrastructure Savings

Cost of Azure Site Recovery and Backup/other infrastructure ($M)



Source: IDC In-depth Interviews, August 2021

IDC then drilled down further on cost benefits by evaluating the following factors:

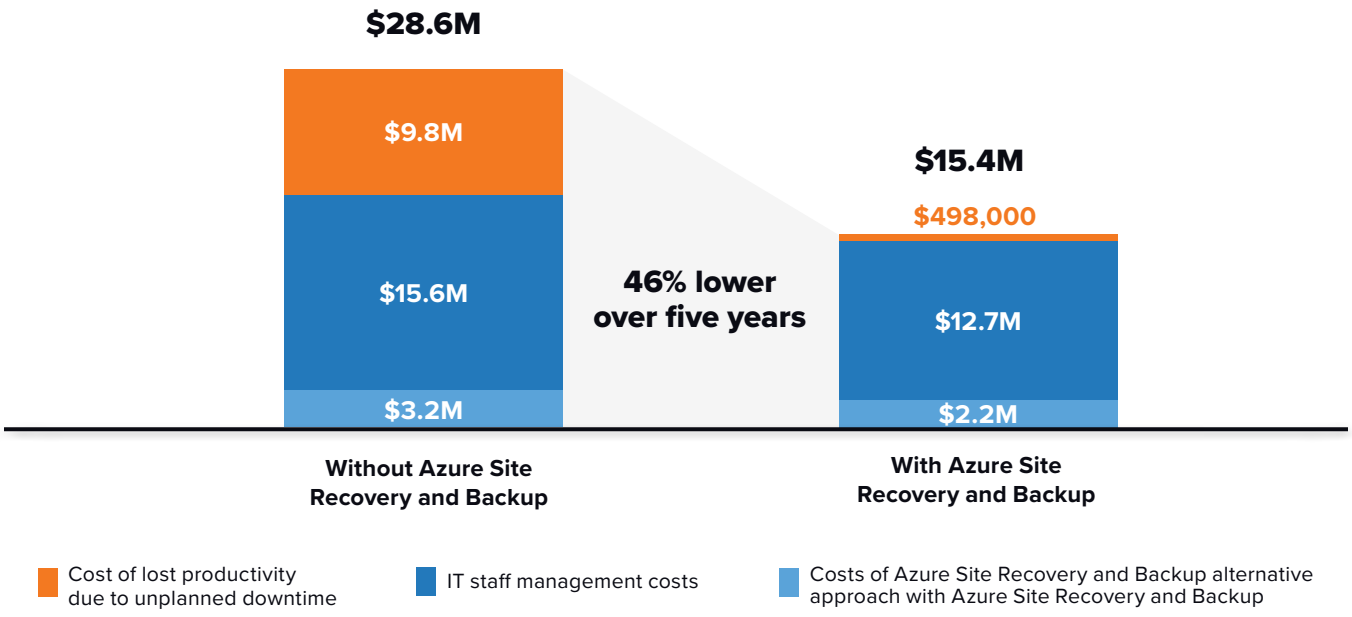
- The cost of lost productivity due to unplanned downtime
- IT staff management expenses
- The cost of the Azure platform versus alternative solutions

Taking these factors into account, **Figure 2** (next page) projects the five-year cost of operations compared against legacy or alternative solutions. Total costs are projected to be 46% lower after the deployment of Azure Site Recovery and Backup.

FIGURE 2

Five-Year Cost of Operations

($M)



Source: IDC In-depth Interviews, August 2021

The Business Impact of Azure Site Recovery and Backup

Improving BDR operations had both direct and indirect impacts on the business operations of interviewed companies. Study participants reported that they were able to optimize key aspects of their business by improving recovery agility, which made a substantive contribution to improving the performance of business-critical applications. They noted the benefits of better time to market and improved reputation with their external stakeholders. Application development life cycles were also improved in part because teams were able to generate their own test data and had a better road map to development, security and operations (DevSecOps) implementation. Others noted that end users benefitted from increased flexibility as the result of automatic updates and cited easier customization involving international regulations.

Study participants commented on these and related benefits:

- **Time to market and improved reputation:**

"It would be speed to market. For example, we're currently moving all our customer-facing systems to integration with Azure AD, and you protect your whole Active Directory ecosystem with the tools to recover from a catastrophic failure. The commercial benefit is peace of mind because it lowers our liability insurance by 10%. This lowered risk has a knock-on effect to getting funding, and it also helps with our government contracts. It's these little things that people don't consider that have a bigger effect."

- **End users benefit from increased flexibility:**
  "It provides better collaboration efficiency and flexibility of work practices. Everyone gets better access to automatic updates."

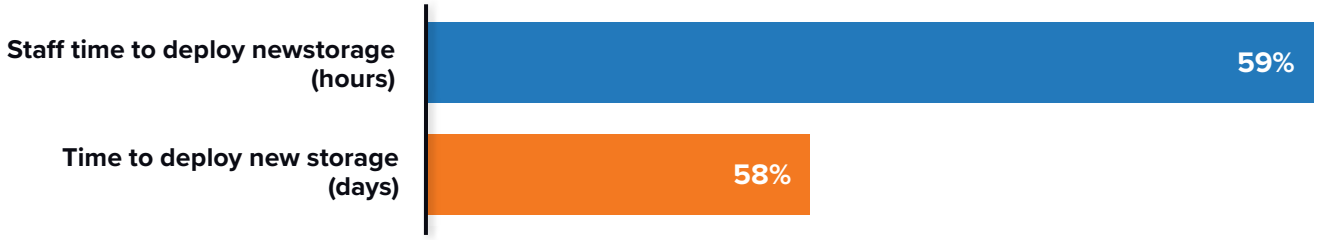
- **Easy to customize international regulations:**
  "There are multiple laws for having various kinds of encryption in different countries or jurisdictions, so it's a major advantage where data privacy is very rigid for standing up your own datacenter. For example, in Luxembourg, you can't move data outside the country. For primary backup centers, we have separate instances of our applications that run in Luxembourg. But if we have to stay in our own apps, we have our own infrastructure there to do primary backup, and we can't do that. This is where we use Azure because they are already in-country."

Another key area was agility. Greater agility enabled higher-value application development and ensured that IT organizations were able to better respond to fluctuations in business demand. In particular, they noted the importance of improved agility in deploying storage resources, which means that users have the resources they need to access more quickly. **Figure 3** presents data on how, after deployment, IT teams were able to deploy BDR-related storage resources quickly and easily. These teams were able to deploy new storage capacity 59% faster. In addition, the overall time required to deploy new storage was reduced by 58%.

FIGURE 3

Backup and Recovery Storage Agility Impact

(% improvement)



Source: IDC In-depth Interviews, August 2021

With respect to development, progress toward DevOps implementation and meeting requirements for accelerated application delivery are key aspects of digital transformation. IDC evaluated how Azure Site Recovery and Backup impacted this core business function. Study participants reported that, after adoption, their application development teams were more efficient. This gave business users increased confidence in the infrastructure support they needed to effectively work on projects. Commenting on how application development life cycles saw improvement, one study participant noted: *"Through the CI/CD (continuous integration and continuous deployment) pipeline, developers are actually able to do things. I've introduced DaaS so they can effectively fill in the form and create a data contract. Based on permission, they can get access to data through all of these things, whether it's legacy or current data. That has been one of the biggest uplifts to life cycles and time for development because now they can generate their own test data. Again, it's not an individual thing. Rather, it's a whole series of things we've done to move to the DevSecOps world, full stack development, and other things."*

Table 9 quantifies these improvements. Average productivity for application development and DevOps teams increased 13% annually after adoption of Azure Site Recovery and Backup. On average, these teams of 134.4 FTEs were able to support the work of an additional 17.8 FTEs without having to add those resources. Over time, this resulted in an average annual productivity-based business value of $1.8 million per organization.

TABLE 9

Development Staff Impact

	Before Azure Site Recovery and Backup	With Azure Site Recovery and Backup	Difference	Benefit
FTEs per year per organization	134.4	152.1	17.8	13%
Value of development team per year per organization (based on FTEs)	$13.4M	$15.2M	$1.8M	13%

Source: IDC In-depth Interviews, August 2021

ROI Summary

Table 10 presents IDC's return on investment (ROI) analysis for study participants' use of Azure Site Recovery and Backup. IDC projects that interviewed companies will achieve five-year discounted benefits worth an average of $16.7 million per organization ($156,800 per 100 users) through improved BDR operations, better application development, and robust cost savings. These benefits compare with total five-year discounted costs of $3.6 million per organization ($33,400 per 100 users). These levels of benefits and investment costs are projected to result in an average five-year ROI of 370% with a break-even point occurring in approximately eight months.

TABLE 10

Five-Year ROI Analysis

	Per Organization	Per 100 Users
Benefit (discounted)	$16.7M	$156,800
Investment (discounted)	$3.6M	$33,400
Net present value	$13.1M	$123,400
ROI (NPV/investment)	370%	370%
Payback	8.1 months	8.1 months
Discount factor	12%	12%

Source: IDC In-depth Interviews, August 2021

Challenges/Opportunities

Cloud-based data protection is an active, rapidly growing market that has attracted entrants from nearly every corner: independent software vendors (ISVs) developing data replication and protection software, cloud service providers and managed service providers that integrate software into solutions, and, of course, major cloud providers. The result is incredibly intense competition that leads to greater innovation and downward pricing pressure.

No company of any size is immune from these challenges. Microsoft certainly has scale, market recognition, and technical capabilities that immediately make it an important market force. Nevertheless, even a company with its capabilities cannot be all things to all people, and Microsoft must thus focus on the value that it can provide as a cloud platform provider without allowing itself to be spread too thin in its attempt to deliver too much.

Moreover, given that it cannot be all things, Microsoft must continue to partner with ISVs and enable cloud SPs and managed SPs to deliver complementary solutions. These partnerships create an ecosystem around Azure that is attractive to new customers and partners alike. In other words, Microsoft must balance the needs of the ecosystem while still delivering compelling and competitive solutions. Fortunately, there is a great deal of room for differentiation and innovation in which many organizations can operate successfully and profitably, all to the benefit of the IT consumer.

Conclusion

IT organizations are rapidly adopting cloud-centric data protection, including disaster recovery and archiving. This shift is illustrated by the rapid growth of these market segments. Organizations are deploying these solutions to address core, cloud, and edge data protection requirements from a central, cloud-based management perspective. Centralizing backup operations can help provide consistent, reliable data protection across the data estate as well as enterprisewide data management policies. Cloud-based data management platforms can also reduce labor costs and leverage on-demand cloud resources to optimize budgets and valuable human resources.

With literally thousands of DPaaS providers in the market, IT buyers have the challenge of determining which solution is the right one for them. Microsoft, as a first-party provider of DPaaS solutions on the Azure platform, has positioned itself to meet many of the broader data protection requirements of enterprises. Azure Site Recovery and Backup is designed to provide the data protection platform for virtual infrastructure, unstructured data, and structured file systems. These products offer high standards for data security and sensitive information.

Our research from this study revealed that utilizing Azure Site Recovery and Backup has provided significant business value to Microsoft Azure customers.

These include:

- **93% reduction in man-hours** lost to unplanned downtime
- **20% improvement** in time devoted to data protection operations
- **39% reduction** in the backup window
- **80% faster** data restores
- **46% lower** cost of data protection operations over five years

A simultaneous improvement in operations and reduction in cost is exactly what organizations look for when modernizing data protection operations and that is exactly what we found regarding the customers interviewed for this study.

Appendix

Methodology

IDC's standard Business Value/ROI methodology was utilized for this project. This methodology is based on gathering data from organizations currently using Azure Site Recovery and Backup as the foundation for the model.

Based on interviews with organizations using Azure Site Recovery and Backup, IDC performed a three-step process to calculate the ROI and payback period:

1. **Gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of using Azure Site Recovery and Backup.** In this study, the benefits included security staff time efficiencies,development productivity gains, reduced costs associated with risk, and higher revenue.
2. **Created a complete investment (five-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using Azure Site Recovery and Backup and can include additional costs related to migrations, planning, consulting, and staff or user training.
3. **Calculated the ROI and payback period.** IDC conducted a depreciated cash flow analysis of the benefits and investments for the organizations' use of Azure Site Recovery and Backup over a five-year period. ROI is the ratio of the net present value (NPV) and the discounted investment. The payback period is the point at which cumulative benefits equal the initial investment.

IDC bases the payback period and ROI calculations on a number of assumptions, which are summarized as follows:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and manager productivity savings. For purposes of this analysis, based on the geographic locations of the interviewed organizations, IDC has used assumptions of an average fully loaded salary of $100,000 per year for IT staff members and an average fully loaded salary of $70,000 per year for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).
- The net present value of the three-year savings is calculated by subtracting the amount that would have been realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.
- Because IT solutions require a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC prorates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

Note: All numbers in this document may not be exact due to rounding.

About the Analysts

Harsh Singh

Senior Research Analyst, Business Value Strategy Practice, IDC

Harsh V. Singh is a Senior Research Analyst for the Business Value Strategy Practice, responsible for developing return-on-investment and cost-savings analysis on enterprise technological products. Harsh's work covers various solutions that include datacenter hardware, enterprise software, and cloud-based products and services. Harsh's research focuses on the financial and operational impact these products have on organizations that deploy and adopt them.

More about Harsh Singh

Phil Goodwin

Research Vice President, Infrastructure Systems, Platforms and Technologies Group, IDC

Phil Goodwin provides detailed insight and analysis on evolving industry trends, vendor performance, and the impact of new technology adoption. He is responsible for producing and delivering timely, in-depth market research with a specific focus on cloud-based and on-premises data protection, business continuity and disaster recovery, and data availability. Phil takes a holistic view of these markets, and covers risk analysis, service level requirements and cost/benefit calculations in his research.

More about Phil Goodwin

Message from the Sponsor

The Azure Backup and Azure Site Recovery services provide simple, secure, and cost-effective solutions to back up your data and recover it from the Microsoft Azure cloud. It's critical to protect your workloads from ransomware with a multi-layered security approach using role-based accessed control, multi-user authentication, and redundant storage. Additionally, Azure Backup and Azure Site Recovery protect a diverse set of workloads: on-premises VMs, Azure VMs, Azure File Shares, Azure Blobs, and more.

Get started here

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell, and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC @idc @idc idc.com