Key Considerations for Data Protection and Cloud on Your Digital Journey

How unified backup and cloud enable your digital transformation success

IDC ANALYZE THE FUTURE

An IDC InfoBrief, Sponsored by VERITAS The truth in information. Microsoft

February 2018

Digital Transformation (DX) is the Most Important Strategic Initiative for Small and Midsize Businesses* in 2018

- Digital transformation is a critical strategic initiative for all businesses to enable them to compete successfully in the long run and to stay relevant to their customers.
- The focus of digital transformation is often on business initiatives like customer service innovation, product innovation, or improving the way the business communicates with its customers, partners, and employees.
- Vital to the success of DX initiatives – and sometimes overlooked – is an assessment of the existing infrastructure within the business, to ensure that it can support the requirements of new digital initiatives. Infrastructure modernization is cited to be as important as business innovation for DX success.
- Two prerequisites for digital transformation success are a firm handle on the company's data to manage it, protect it, and create value from it, and the ability to take advantage of cloud services to provide the functionality, flexibility, and speed that the business requires. Cloud services enable small and midsize organizations to access world-class IT infrastructure and compete on equal terms with larger competitors.

This IDC InfoBrief will explore the role of cloud services in a modern IT strategy, and how to more effectively protect data in the cloud and with the cloud.

84% of small and midsize businesses are undertaking or starting a digital transformation initiative this year

Top 3 DX Initiatives of Small and Midsize Businesses

50% CUSTOMER SERVICE INNOVATION
– changing service concepts, service delivery systems, and customer support channels

39% PRODUCT (OR SERVICE) INNOVATION
– developing digital products or apps, embedding sensors, etc.

37% MARKETING INNOVATION
– changing how the organization engages and communicates with customers and prospects

IDC ANALYZE THE FUTURE

*IDC defines small and midsize businesses as organizations with 50–999 employees

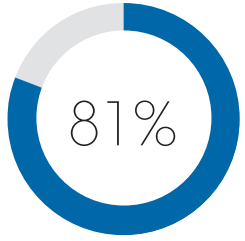
Source: IDC's 2017 Digital Transformation Survey, n = 423. Multiple answers possible.

Data Protection and Cloud are Key Enablers for Digital Transformation

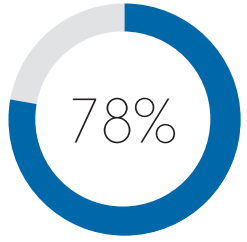
- **Modernizing IT is critical to digital transformation success.** A modern IT infrastructure is key to successful digital transformation – if IT is not refreshed regularly, it can end up holding the business back, but keeping up with IT developments is time consuming.
- **Cloud provides always up-to-date infrastructure and new functionality.** Getting your house in order by consolidating data and IT assets, and being open to adopting new technologies such as cloud services, can ease daily operations and free up time to focus on new things – helping to drive the business forward.
- **Protecting your data is key for digital transformation success.** Data is critical for business operations, customer service, and innovation. Protecting data is a major headache with security threats and regulations constantly changing. IDC research shows that improving data security, protection, and compliance, and driving successful technology refresh are top of the to-do list for small and midsize businesses. Using cloud services is emerging as a great way to deliver cutting-edge technology, but how do you get there?

At the point of technology refresh or new service development, ask yourself:

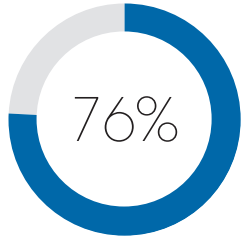
Do I really need to operate my own IT? Can my IT operate more securely and reliably than a cloud provider? Can I really keep pace with technology change? Do I protect my data well enough?



of small and midsize businesses are enhancing their disaster recovery plans with cloud-based solutions to be fit for the digital age



of small and midsize businesses are moving from local on-premise to cloud-based backup to modernize their IT estate



of small and midsize businesses are developing and executing an information governance strategy to support their digital transformation initiative

Source: IDC's 2017 Datacenter Survey, n = 640

Data Protection Challenges

- Getting your data under control is a critical challenge for small and midsize businesses, especially as business users choose IT tools and services to improve their own productivity, sometimes without involving IT and thus creating shadow IT and allowing data to grow and fragment unchecked.
- When it comes to data management, it is vital to get a handle on:
  - Knowing what data you actually have
  - Whether data resides in your own infrastructure or in the cloud, or in a customer's or partner's network
  - Who has access to it
  - How old it is
  - When it was last accessed
- Consolidation of data protection tools and processes is a key step for better, more efficient, and cost-effective data protection. If you can use the same data protection tools for all your present and future use cases, you only need to define the process and policy once and can execute it regardless of where your data resides (in the datacenter or at the remote/branch office, in the cloud, on desktops/laptops/mobile devices, in physical or virtual machines). This helps you solve the most common data protection challenges.
- Shortening the backup window is a challenge in the face of rapidly growing data volumes. Today's solutions can help to bring down the amount of data that needs to be backed up through global deduplication and enable you to meet challenging SLAs from your business users. Faster restore is equally important.
- Cloud is emerging as a preferred destination for data backup and as a disaster recovery service, as it provides cost-efficient long-term storage without the need for redundant infrastructure. For faster restore, SMBs tend to have a hybrid solution in place where the latest backup data is stored onsite for performance as well as in the cloud for redundancy and longevity.

Top 6 Data Protection Challenges

01 Protect data at a remote or branch office

02 Improve backup performance to shorten backup window

03 Protect virtual machine data

04 Reduce data protection cost (opex and capex)

05 Ensure that critical workloads are restored in minutes rather than hours

06 Implement a new disaster recovery solution/redesign a current one

Source: IDC's 2017 Datacenter Survey, n = 640

Why Cloud Makes Sense for Better Data Protection

- **Cloud solves a critical challenge for small and midsize businesses:**
  - How to have a state-of-the-art IT infrastructure without the deep IT skills that larger enterprises can afford.
- **Cost efficiencies.** Cloud comes as a complete package with all the services already integrated and available for a price. Enabling a service is as simple as subscribing and paying for it, rather than having to plan, procure, deploy, test, and operate hardware and software of your own. Cloud provides the ease of use to enable you to implement a modern IT setup, and this is true for data protection and backup.
- **Greater agility and flexibility.** In addition to the IT transformation benefits, cloud helps deliver digital transformation with new apps and service, as well as workplace transformation with better collaboration through easy communications and sharing.
- **No rip and replace required.** Cloud is complementary in a modern data protection setup, particularly for long-term storage, as a second site for disaster recovery and to enable data to be easily and reliably restored.
- **Lower operational and change management overhead.** Cloud services are upgraded regularly to provide the newest features, so you don't need to worry about planning and delivering technology refreshes quite so much anymore.

What is Cloud?

PRIVATE CLOUD: virtualized infrastructure accessible through a self-service portal

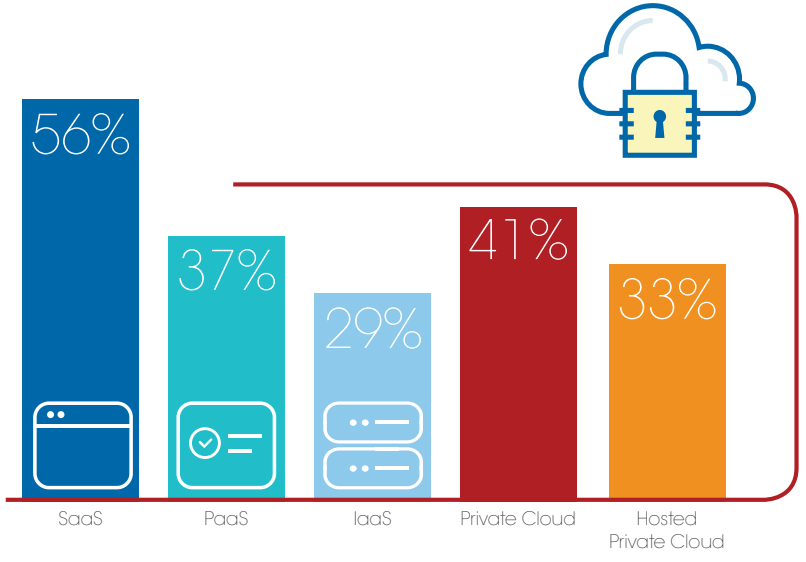
PUBLIC CLOUD: third-party-provided IT infrastructure and applications, running on shared multitenanted infrastructure, accessible through a self-service portal

HYBRID CLOUD: a hybrid cloud is a computing environment which combines a public cloud and a private cloud by allowing data and applications to be shared between them

Source: IDC's 2017 Datacenter Survey, n = 640

How to Use the Cloud for Data Protection

- Small and midsize businesses are using a range of cloud services, from on-premise private cloud, to hosting private clouds in third-party datacenters, to public cloud services such as SaaS, PaaS, and IaaS, with both SaaS and private cloud usage being over 40%.
- The next frontier for small and midsize businesses is to connect their various cloud services into a hybrid cloud architecture, where services cross multiple organization boundaries.
- The move to cloud does not mean that on-premise IT will disappear. Although some businesses will be able to run completely out of the cloud, many will use public cloud or hosted services alongside their own on-premise IT capabilities.



Three steps to the cloud …

1. **Assess your current infrastructure.** Where does your data reside: physical, virtual, or cloud infrastructure?
2. **Consolidate your current infrastructure as much as possible.** Focus on a unified backup regime to get all data under a single management and governance structure.
3. **Migrate relevant workloads to the cloud** but make sure that you can manage and protect on-premise and cloud data with the same solution.

Once in the cloud …

4. **Hybrid cloud and multicloud.** Once in the cloud, move workloads between different cloud providers based on cost, performance, and location or build an integrated hybrid cloud with elements of on-premise and cloud. Ensure that your data is protected, regardless of your cloud strategy.

IDC ANALYZE THE FUTURE

Source: IDC's 2017 Cloud Impact Survey, n = 801

Three Types of Cloud-Based Data Protection

Data protection **to** the cloud.

This is the most common model, where you use a public cloud infrastructure-as-a-service (IaaS) offering as your backup target, just like a backup appliance or storage system. You can interact with the cloud service as with any other secondary storage system. Small and midsize businesses often use a hybrid approach where they store the latest backup data on-premise for faster recovery and store older backup data for longer-term retention and disaster recovery in the cloud. Data protection to the cloud provides the benefit of providing an offline copy in addition to disk copy, which is particularly important in the face of a ransomware attack that encrypts your disks.

Data protection **in** the cloud.

If your business users are running applications in the cloud, you still need to make sure that the data from these applications is backed up, so you can restore the data in case of a service outage or issues with the data such as corruption, mistakes, or destruction. This is an often overlooked aspect. You can also use one cloud service as the backup location for another cloud service.

Data protection **from** the cloud.

Some businesses decide to back up cloud-based data back on-premise, so that they have a copy in case the cloud service provider discontinues the service, or they want to switch providers.

Security Challenge: Ransomware

- 2017 has seen several high-impact ransomware attacks including WannaCry and Petya and NotPetya. These have affected small and midsize businesses as well as large enterprises, and the effect is often devastating.
- Attempting to regain access to encrypted data is often not possible even if a company is willing to pay a ransom as the perpetrators' accounts or control servers are often disrupted. Or the ransomers may be incompetent and are unable to effectively provide decryption keys. Ultimately, a successful ransomware attack is likely to result in lost data.
- A very effective protection against this increasingly common attack is data protection through effective backup and restore capabilities. If data is attacked and compromised, you can rebuild affected machines or data stores with backed up data that is up to date or very close to it. In combining onsite data protection with a cloud copy of your data, you have an offline copy of your data in the cloud that will not be affected by the disk encryption attack. By doing so, the impact is minimized and the risk to business operations greatly reduced.

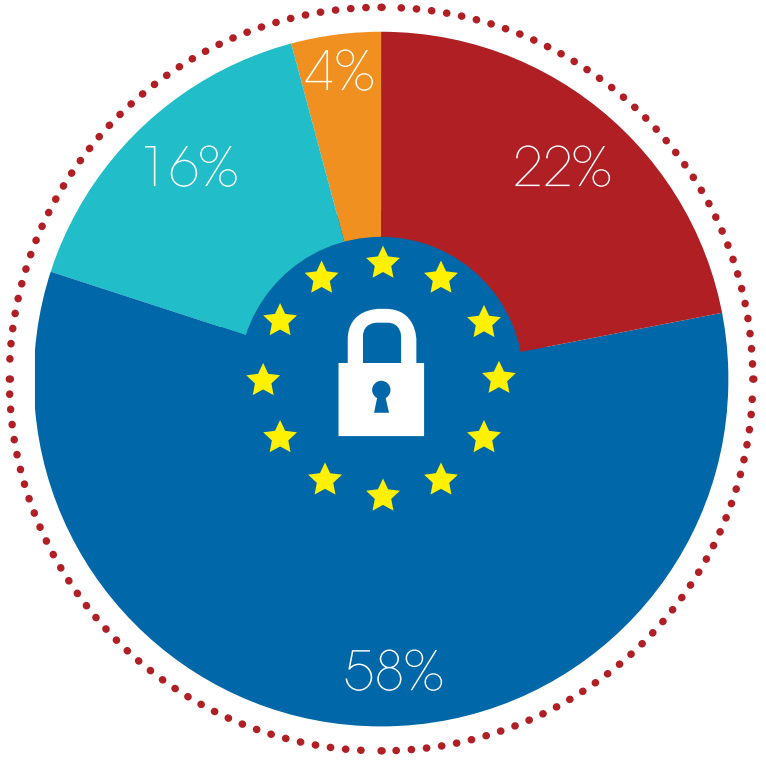
Shipping company Maersk says the NotPetya attack has cost it $300 million to recover.

A small hospital in California had to pay almost $20,000 for a decryption key to recover data as its inadequate backup solution meant data was too out of date to make recovery viable.

Source: IDC's 2017 Datacenter Survey, n = 640

The Privacy Challenge: GDPR and Other Regulations such as HIPAA and PDPC

- Small and midsize businesses are being challenged by the introduction of GDPR in May 2018:
  - **Only 22% have a firm grasp of GDPR requirements.**
  - **58% are only somewhat familiar.**
  - **GDPR applies globally for any company that holds data on European citizens.**
- Key requirements of GDPR are privacy protection of personal data of European data subjects, data protection by design and by default, data minimization, and an understanding of state-of-the-art technologies and processes.
- Small and midsize businesses must be aware that they can never delegate responsibility to a cloud service provider and that they are ultimately responsible for GDPR compliance.
- Due to a lack of understanding of detailed requirements and a push to pass GDPR audits, 56% of small and midsize businesses are reconsidering their use of cloud services. But with the right governance practices in place, cloud services can be used under GDPR and often provide better privacy protection than can be achieved on-premise due to CSPs' high levels of investment in shared security capabilities.
- Encryption is a key enabler for GDPR preparation as it allows companies to avoid having to disclose a breach if a device is lost or stolen.
- GDPR applies globally, to any organization doing business in Europe. GDPR is not the only regulation driving greater importance on managing personal identifiable information (PII). Other regulations such as HIPAA and PDPC could lead to similar possible issues.



Source: IDC's 2017 Cloud Impact Survey, n = 801

Six Considerations for Selecting the Right Cloud Vendor and Cloud Enabled Data Protection Solution

1. Can you extend your current IT infrastructure and skill sets into the cloud? Can you take advantage of hybrid cloud benefits with your current provider?
2. Does your data protection vendor have a long-term vision and roadmap for cloud-enabling its products?
3. Does the data protection and cloud vendor provide a global footprint, aligned with your growth and geo-expansion aspirations?
4. Security and compliance are paramount – especially for data in the cloud. What are the security and industry/regulatory compliance track records of your providers?
5. How does the cloud-enabled data-protection solution cost structure compare to an on-premise solution? Does your vendor provide tools to monitor and optimize your cloud costs?
6. Does your data protection vendor offer multicloud support? This may not be important today, but may become important down the line.

Best Practices for Data Protection in the Cloud

- **Visibility into the data.** Get an overview of all the data that needs protection, independent of where the data resides (on-premise, in physical and virtual environments, in a hosting facility, in partners' or suppliers' facilities, or in the cloud).
- **Business-driven policies.** Define retention policies based on the business criticality of the data and deploy these policies across on-premise and cloud-based assets.
- **No rip and replace.** Consider cloud-based data protection as complementary to, rather than a straight replacement of, on-premise data protection:
  - This is especially true for remote and branch offices and for desktop, laptop, and mobile device backup.
- **Unified platform.** Choose a data protection provider that can support you wherever you want to go: on-premise (physical, virtual, containers) and supports various clouds, so that you can maintain the same data protection regime regardless of the location of your data.
- **Lower your operational risk.** Choose a public cloud provider that supports the management tools that you are already familiar with.
- **Lower your operating cost.** Choose leading cloud and data protection vendors to benefit from lower cost and lower risk on your digital journey with a unified data protection offering that supports your business strategy.
- **Cost-efficient SLAs.** Choose a cloud provider that covers different service levels and storage tiers to get the right mix of price and performance for your backup needs.
- **Focus on security and compliance.** Choose a cloud provider that takes security seriously and invests in security staff, processes, and certifications.

How to Choose the Right Solution Provider, Vendor, and Cloud Partner for Cloud-Based Data Protection

- Conduct a competitive review of market offerings both for data protection solutions and cloud storage backends.
- Seek a partner that:
  - Has a strong focus on innovation, security, and leading technological developments in the market.
  - Provides regular forums to showcase the latest technology developments based on an understanding of how users behave.
  - Understands your business and can provide relevant data protection and cloud services to enable productivity and efficiency gains.
  - Discusses, advises, and provides market-leading solutions.