IDC PERSPECTIVE

Why a Backup Strategy for Microsoft Office 365 is Essential for Security, Compliance, and Business Continuity

Archana Venkatraman

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Backup Strategy for Microsoft O365 is Essential for Security, Compliance, and Business Continuity

Email and collaboration is the most mature business process, and it is the most adopted software-as-a-service (SaaS) solution. This makes Microsoft Office 365 (O365) the center of business productivity, and ensuring data protection of O365 is imperative for security, compliance, and business continuity. A lack of O365 backup plan is a risky data strategy.

Key Takeaways

- 6 in 10 O365 users IDC spoke with at an event do not have a data protection plan for their O365 estates or rely on Microsoft's native capabilities.
- Microsoft's shared responsibility in O365 is limited to infrastructure — ensuring uptime, cloud service availability, basic retention, and physical and logical infrastructure security.
- While the data owner is ultimately responsible for data security, privacy, compliance, and recovery, enterprise-grade backup of O365 can give businesses the confidence to recover from security breaches, compliance exposure, and data loss.

Recommended Actions

- Make O365 backup a key priority.
- Ensure strategic and methodical adoption of the O365 suite with a backup environment to mitigate risks from SaaS lock-in.
- Be in complete control of business data, and lay the foundation to become data-driven.
- Consider enterprise-grade data protection and recovery features, automation, security, and integration between the O365 environment and your existing data protection environment when investing in backup solutions.

Source: IDC, 2019

May 2019, IDC #EUR145096519

SITUATION OVERVIEW

In the era of digital transformation, cloud – particularly SaaS – is considered as a breath of fresh air around user interface. It offers easier collaboration and is considered as transformative.

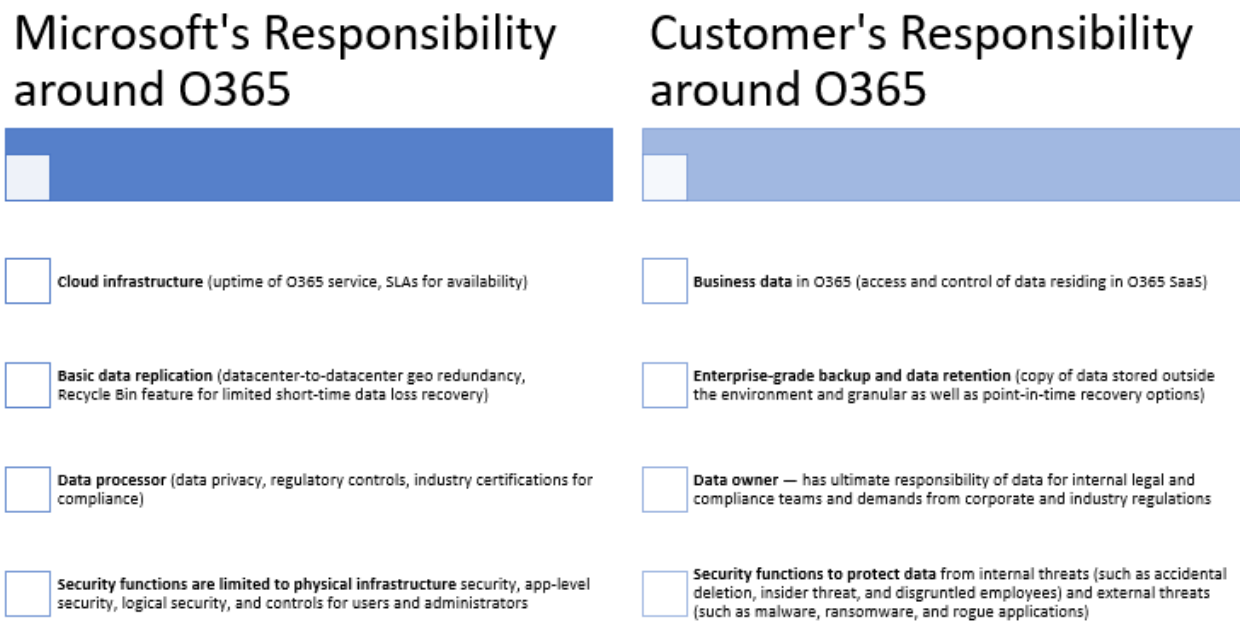
IDC research finds that email and collaboration is the most mature business process within SaaS, and it is the most adopted at 61%. As one of the most popular SaaS products, Microsoft Office 365 adoption is accelerating, and its use is expanding beyond Exchange to more services including SharePoint, OneDrive, and Teams. While O365 is fast becoming the center of business productivity, a backup and recovery strategy is just an afterthought. 6 in 10 users of O365 IDC spoke with at an event do not have a data protection plan for their O365 estates or rely on Microsoft's native capabilities. In conversations with O365 users, IDC observes that many users confuse Microsoft's availability SLAs to backup strategies, while others don't see the need to think of backup for cloud because it is "different" technology.

Regardless of whether the data is on-premise or in cloud infrastructure/SaaS such as O365, ultimate responsibility of data protection lies with the customer or the data owner – you. Adopting O365 without enterprise-grade backup is a risky strategy.

The first step is to understand the responsibilities of Microsoft and O365 user organizations. Figure 2 illustrates how Microsoft's basic responsibility is limited to infrastructure levels – infrastructure availability, security, and access controls – while all data responsibilities are on the user to ensure data security, privacy, and retention.

FIGURE 2

O365 Vendor-Customer Shared Responsibility at a Glance



Source: IDC, 2019

Given Microsoft's responsibility and supporting technology is limited to infrastructure levels, organizations are exposing themselves to the following risks if they are without third-party backup plans:

- **Data loss and security breaches**. O365 is no exception to security breaches — it is vulnerable to internal threats (e.g., accidental deletion of data, actions by disgruntled employees, or access from ex-employees) as well as external threats (e.g., malware or ransomware). According to IDC research in 2018, 69% of organizations have suffered successful malware attacks within 12 months, 39% of which involved ransomware. Malware attacks are a reality today, and SaaS tools are no exception. Almost half (49%) of organizations have suffered from an unrecoverable data event in the past three years. An enterprise-grade backup strategy can give enterprises an option to recover from security breaches by using granular recovery.
- **Retention and regulatory compliance exposures**. Microsoft offers a 90-day retention policy that does not meet the more stringent data retention regulations for certain industries such as financial services, healthcare, retail, and government. Having a third-party backup can help organizations set their own retention policies according to their business needs and remain compliant with European data regulations.
- **Lack of data control in hybrid deployments**. Full oversight and control of data is a boardroom priority and a first step toward becoming data-driven. Without backup, organizations do not have an exit strategy or freedom from SaaS lock-in because they are not in complete control of their data.

In addition, many customers have a blend of on-premise and SaaS in which they adopt Exchange online, but they are yet to migrate SharePoint to SaaS. In other cases, if there are mergers or acquisitions, different teams on different versions of email and collaboration suites can make data protection more challenging in hybrid deployments without unified backup. Having a unified data protection for hybrid environment can ease the adoption of O365.

ADVICE FOR THE TECHNOLOGY BUYER

Without data protection extended to SaaS, enterprises are exposing O365 data to compliance issues, data loss, security vulnerabilities, and business continuity risks. In addition, integrating SaaS into enterprise data protection can help unify data management and develop a foundation to become data-driven.

Backup for fast-growing SaaS such as O365 is no longer an option — it is imperative for security and data control. Many data protection vendors have started offering backup for O365 environments and are fast-expanding to add more O365 services. When investing, organizations need to ensure that the backup solution they choose offers:

- **Flexibility and choice**. The business should have the freedom to use existing on-premise capacity for O365 backup or leverage another cloud for cloud backup.
- **Features**. It should provide incremental backups, granular recovery, automation, and policy-based retention capabilities.
- **Breadth of service**. The solution should be capable of managing and protecting hybrid deployments and ease the full adoption of SaaS.
- **Complementarity to O365.** It should have deep integration with O365 and the customer's existing data protection environment.
- **Innovation**. There should be additional security features such as access control, SaaS usage metrics, and multifactor authentication for additional security.
- **Scale.** Ability to scale up or down without capex as business and data demand changes and as SaaS is rolled out more widely within a company.

LEARN MORE

Related Research

- *European Data Replication and Protection Software and Services Market Shares, 1H18: Cloud Services Get an Edge* (IDC #EMEA44902219, March 2019)
- *What AWS's Launch of its Own Backup Solution for Hybrid Cloud Means for the Data Protection Market* (IDC #EMEA44901319, March 2019)
- *New Commvault CEO: Sanjay Mirchandani Takes the Helm* (IDC #IcUS44862419, February 2019)

Synopsis

This IDC Perspective assesses how data protection dynamics in SaaS change, particularly as services such as Microsoft Office 365 adoption accelerates, and its use expands beyond Exchange to other services that include SharePoint, OneDrive, and Teams to become key to business productivity.

"While O365 is fast becoming the center of business productivity, a backup and recovery strategy is an afterthought. Relying on Microsoft's native backup capabilities and infrastructure-level uptime features is a risky strategy because regardless of where the data is, it is the company's responsibility," said Archana Venkatraman, research manager, IDC European Datacenter. "Without an enterprise-grade backup strategy for O365, enterprises are exposing themselves to risks such as ransomware, accidental loss of data, lack of data control, compliance exposures, and threats to business continuity."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com