us signal

Don’t Risk It All: The Case for Microsoft 365 Data Protection with a CSP

Table of Contents

Chapter 1: Introduction

Businesses worldwide trust and utilize the Microsoft 365 (M365) suite for their productivity and data modernization needs.

With M365 usage, massive amounts of data are collected and transferred every second of every day. To ensure business continuity and minimize the risk of data loss, organizations must prioritize protection for their M365 data.

Small and mid-market organizations face significant resource constraints regarding budget and personnel. These limitations can make it difficult to implement and maintain adequate data protection strategies, particularly for complex platforms like M365. Many organizations also lack the expertise or staffing to effectively manage M365 data protection, leaving them vulnerable to breaches, accidental data loss and other security incidents.

Working with a Microsoft Cloud Service Provider (CSP) helps overcome these challenges by providing access to experienced security professionals, specialized tools, technologies and scalable data protection solutions that adapt to evolving needs.

This e-book gives organizations a comprehensive understanding of the importance of data protection for their M365 data and how partnering with a CSP can ease the burden of achieving this goal.

"Microsoft 365 users generated more than 38 BILLION collaboration minutes in a single day and have over 345 MILLION paid seats"
- Satya Nadella, Microsoft CEO

Chapter 2: Who is Responsible for M365 Data Protection?

Who is Responsible for M365 Data Protection?

M365 data protection is a shared responsibility between Microsoft and the organization using the platform. Microsoft is responsible for the security and availability of the underlying infrastructure, including the servers, data centers and networks.

They also provide security features and tools within M365 to help organizations protect their data, such as encryption, threat detection and security monitoring. However, the organization using M365 is ultimately responsible for protecting its data and ensuring compliance with relevant regulations and industry standards. This obligation includes managing user access and permissions, securing data and employing appropriate security controls.

"We don't claim ownership of Your content. Your content remains YOUR CONTENT, and you are responsible for it."
- Microsoft Service License Agreement

Verify Your Backups

Businesses should implement a layered security approach that includes Microsoft's built-in security features combined with additional measures addressing specific security needs.

For instance, organizations should define and enforce access and permissions policies that prevent unauthorized access to sensitive data. They should also implement endpoint protection measures, such as antivirus software, firewalls and threat monitoring, to secure devices and networks against external threats.

Finally, a comprehensive backup and recovery plan that ensures the restoration of critical data in case of accidental deletion, hardware failure or cyberattack is a must.

- Regular backups must be performed to a secure, off-site location, and the recovery process must be tested to ensure effectiveness.

- Organizations should continuously monitor and evaluate their security posture to identify and mitigate potential vulnerabilities.

- Working with a CSP can help navigate these responsibilities and implement effective data protection measures.

A report by Gartner predicts that by 2025, 70% OF ORGANIZATIONS will rely on CSPs for M365 data protection, UP FROM 30% in 2020.

Chapter 3: Collaboration

Identity Management

Identity assessment is crucial to M365 data protection, ensuring only authorized users can access critical data and systems. Given the sensitivity of the data stored and processed in M365 applications, organizations must employ rigorous protections. Identity management is especially critical for small and mid-sized companies that may not have the resources to maintain a robustIT security infrastructure.

Azure Active Directory
Azure Active Directory (Azure AD) is one of the most powerful and widely- used cloud-based identity and access management solutions. Azure AD is a comprehensive tool to manage user identities, credentials and permissions effectively and securely. It offers a wide range of capabilities that enhance user security when accessing M365 applications, such as single sign-on (SSO) and multi-factor authentication (MFA), while also easing the burden on IT administrators through features like conditional access policies.

One of the most notable advantages of using Azure AD is the ability to centralize identity management. This centralization streamlines managing identities across multiple systems and applications, reducing the risk of security breaches from weak or stolen credentials. Azure AD also offers advanced security features such as conditional access, allowing organizations to set policies based on location, device type and user risk. By using conditional access, organizations can enforce strong authentication policies while ensuring users can access only the resources they need to do their jobs.

Why use a Microsoft CSP?

CSPs are critical in ensuring the successful setup and deployment of Azure AD so organizational IT staff can take full advantage of its centralized management capabilities. A CSP's engineers provide technical expertise and support to help navigate the complexities of identity management, while assisting in selecting suitable Azure AD and other licenses to meet an organization's unique identity and access management needs.

Furthermore, CSPs help integrate Azure AD with other M365 tools and applications, including those geared toward endpoint protection, while simplifying the security process and ensuring alignment with industry best practices.

Break the Glass Accounts
An emergency access account that provides authorized personnel with elevated privileges to access critical systems
or data when there is no other way to access them. These accounts are highly restricted and monitored, with access granted only to a few individuals who have undergone rigorous background checks and security training.

Chapter 4: Management

Multi-Factor Authentication

One of the most effective security measures against security breaches and cyber-attacks is multi-factor authentication (MFA).

MFA requires a user to verify their identity by providing two or more forms of authentication. Typically, this involves something the user knows (like a password) and something they have (like a code sent to their phone).

MFA provides an additional layer of security over passwords that prevents unauthorized data access, especially for organizations storing sensitive data such as financial records, personal information or trade secrets. The damage caused by illicit access to sensitive data can be catastrophic, with costs of both financial losses and reputational damage.

By implementing MFA, organizations can significantly reduce risk and protect themselves from the associated costs. Even if an attacker manages to stea a user's password, they will still be unable to access the user's data without providing additional authentication factors.

"Providing an extra barrier and layer of security that makes it incredibly difficult for attackers to get past, MFA CAN BLOCK OVER 99.9 % of account compromise attacks. With MFA knowing or cracking the password won't be enough to gain access."
– Microsoft

CSP + MFA = Enhanced Security

A CSP can help configure MFA for all users, providing the correct setup to ensure it works seamlessly with the organization's IT infrastructure and minimize user frustration. By leveraging this expertise, organizations can implement and maintain MFA effectively, reducing the risk of data breaches and cyberattacks.

A CSP can also provide ongoing support and maintenance, ensuring that MFA remains effective and up to date. This supervision includes keeping up with the latest security threats, updating configurations as necessary and guiding best practices to help organizations integrate MFA with other security tools and systems.

Chapter 5: Endpoint Protection

Endpoint protection is a critical component of data defense. Endpoints such as laptops, desktops and mobile devices are often the weakest link in an organization's security posture.

Attackers frequently target endpoints to gain access to sensitive data or systems, so it's essential to have a robust endpoint protection strategy. Microsoft offers two powerful tools for endpoint protection: Microsoft Defender for Endpoints and Microsoft Intune.

Microsoft Intune is a cloud-based mobile device management (MDM) and mobile application management (MAM) solution. It allows organizations to manage and secure mobile devices that access company data and applications. With Microsoft Intune, organizations can enforce security policies, such as requiring a passcode to access a device and remotely wiping devices if they are lost or stolen.

Additionally, businesses can manage and deploy applications to smartphones and tablets, allowing organizations to control use on company devices and ensure they are up to date and secure. Microsoft Intune integrates with other Microsoft tools, such as Azure Active Directory and Microsoft Endpoint Configuration Manager, to provide a comprehensive endpoint management solution.

Microsoft Defender for Endpoints is a protection platform with antivirus, anti-malware and other security features. It provides real-time protection against a wide range of threats, including viruses, spyware and ransomware.

The Microsoft Defender family of products also includes advanced features such as behavioral analysis and machine learning to detect and respond to emerging threats.

Defender for Endpoints can be combined with other Microsoft tools, such as Microsoft Defender for Cloud (formerly known as Azure Security Center) and Microsoft Cloud App Security, to provide a comprehensive security solution for organizations. Microsoft Defender for Cloud offers centralized security management and monitoring for an organization's Azure resources, including virtual machines and databases. Microsoft Cloud App Security helps organizations protect cloud applications and data by providing visibility into cloud usage and detecting threats such as unauthorized access and data leaks.

Better Protection from Start to Endpoints

A Microsoft CSP that offers endpoint protection services can help organizations evaluate their M365 configurations against best practices and identify security gaps. Additionally, an experienced CSP can assist with setting up, configuring, and managing endpoint protection to ensure better safety from start to endpoints.

It is important to note, Microsoft Defender is not one tool but a family of products and services, including:

- Microsoft 365 Defender
- Microsoft Defender for Cloud
- Microsoft Defender capabilities in Windows
- Microsoft Defender for IoT
- Microsoft Defender Threat Intelligence

Discovering which of these tools is right for your organization is one of the more challenging aspects of Microsoft data protection.

Chapter 6: Backup Solutions

M365 data is critical to an organization's operations and data loss can be catastrophic. With the rapidly increasing volume of data being created and stored in M365, organizations must protect this essential resource from accidental deletion, malware, ransomware and other threats.

Commvault Metallic Security

Commvault Metallic provides enterprise-grade protection for critical Microsoft 365 data with stringent security standards, privacy protocols, and zero-trust access controls to combat today's data loss threats.

With Metallic, organizations can rest assured that their data is protected with isolated, virtually air-gapped backups (backup data is stored separately from source data) and layered security, including GDPR compliance, at-rest and in-flight data encryption, role based, SSO, and SAML authentication controls and SOC2 and ISO 27001 certifications.

On average, small instances of data loss (fewer than 100 files) cost businesses between $18,000 TO $35,000, while large-scale incidents can cost up to $15.6 MILLION, according to a 2022 study by Verizon.

Metallic provides comprehensive backup and recovery services for M365 data and offers multiple features that protect M365 data, including:

1. Cloud-based Backup: A secure and scalable cloud-based solution 1 providing easy and efficient M365 data protection, eliminating the need for on-premises hardware or infrastructure.

2. Automatic Backup: Removes the need for manual backups, reducing the risk of human error.

3. Granular Recovery: Enables restoration of individual emails, files, folders or mailboxes. This feature ensures organizations can recover specific data quickly, minimizing the downtime necessary for a full restore.

4. Multiple Restore Options: Point-in-time restores allow data recoveryfrom a specific time, while cross-user restores enable data restorationto another user's account.

5. Compliance: Compliant with various industry standards, including NIST, CIS and HIPAA, allowing for the protection of M365 data while meeting regulatory requirements and providing e-discovery meeting Electronic Discovery Reference Model (EDRM) requirements.

The CSP Backup Advantage

Implementing an effective backup solution for M365 data can be challenging, so a CSP can help facilitate the process. By leveraging a provider's expertise, businesses can protect their data from accidental deletion, malware, ransomware and other threats.

In particular, a CSP can help businesses deploy the comprehensive M365 data backup and recovery services of Commvault Metallic. Benefits include managing and monitoring Commvault's Metallic portfolio and enhancing self-service management capabilities to boost storage configuration and backup efficiencies and minimize downtimes.

Digital Infrastructure Solutions Built for Your Business

US Signal, established in 2001, is a premier national digital infrastructure company that operates a fully owned fiber network to deliver a wide range of advanced digital solutions. Our offerings include robust cloud services, secure colocation facilities, high-performance connectivity, comprehensive hardware resale, and managed IT services, empowering businesses to enhance their operational efficiency through tailored network, data center, data protection, and cybersecurity solutions.