Commvault

eBOOK

# Your Path to Microsoft 365 Ransomware Protection

Safeguarding Microsoft 365 data with cyber resilient data protection

# Introduction

Microsoft 365 has become the central driving force for borderless collaboration, increased productivity, and facilitating new remote workforce models. And with 345 million paid Microsoft 365 users and with an annual revenue over $2B, quarter-over-quarter growth, it's not going away anytime soon.[1, 2] But as more organizations standardize on Microsoft 365 to facilitate day-to-day operations, cybercriminals are following them there.

Unfortunately, bad actors understand how tightly today's organizations are tied to Microsoft 365—and the widespread impact a successful breach can have on operations. Employees, sub-contractors, and sometimes even trusted partners need access to emails, documents, file repositories, departmental workspaces, virtual meeting rooms, and more. Without access to critical Microsoft 365 data, many businesses would fail to collaborate and generate revenue. Without Microsoft 365, many organizations would fail to stay productive.

As cybercriminals turn their focus to exploiting SaaS applications, this eBook uncovers the risks in today's environment, explores cyber resilient considerations for Microsoft 365 data protection, and determines the best ways in which data protection-as-a-service can mitigate those concerns.

## SOPHISTICATION, FOCUS, VOLUME—AND IMPACT

Ransomware has proven to be a very lucrative business model for bad actors. The more lucrative it becomes for the cybercriminals, the more challenging it becomes for legitimate organizations to overcome the volume, sophistication, and impact of these attacks. And as today's businesses double-down on SaaS-based solutions, many ransomware gangs are following the data, setting their sights on exploiting invaluable SaaS apps, like Microsoft 365.

**236M+ attacks** were attempted in the first half of 2022.[3]

### Growing sophistication

Ransomware attacks have evolved and become increasingly sophisticated with the integration of artificial intelligence (AI) capabilities. Adversaries are leveraging AI algorithms to enhance their attack techniques, making them more targeted, evasive, and difficult to detect. AI-powered ransomware can adapt and learn from its environment, enabling it to bypass traditional security measures and exploit vulnerabilities more effectively. This growing sophistication of ransomware with AI poses a significant challenge for organizations.

### A new focus

But not only have attack schemas changed, but their targets have as well. As today's businesses continue to pour their dollars and data into newly deployed SaaS applications, cybercriminals focus their efforts on these data-rich cloud platforms. In fact, there has been a 300% increase in SaaS cyber attacks.[4]

And, with such a large customer base to mine, Microsoft 365 continues to be the top target for phishing campaigns and other ransomware attacks.[5]

### Risks are mounting

The impact of ransomware-triggered shutdowns and data loss is profound on the victim organizations. First, there's the payout itself. A successful ransomware event, on average, costs about $1.85 million[6] with no guarantee of getting the data back in working order. Then, there's the impact to your brand and negative market perception. It's led to lost investors, clients, and revenue. Last, there is downtime, which is a critically relevant factor for Microsoft 365. Microsoft 365 downtime and the lack of access to critical business data, the lasting adverse effects can extend far beyond the painful financial losses, becoming a drag on operations—and the bottom line—for months or years to come.

## PLAYING YOUR ROLE IN DATA PROTECTION

Despite Microsoft 365's importance on business operations, there is a growing disconnect in how to protect (and who is responsible for protecting) data living within it. Many organizations hold the misconception that cloud service providers (including Microsoft) are responsible for BOTH administering the SaaS application AND protecting the customer data living within it. That's what the cloud is for, right? Wrong.

**The reality? They're not.**

Microsoft provides a highly resilient platform and goes to great lengths to secure data residing within Microsoft 365. However, like cloud service providers, they follow what is known as the shared responsibility model, where they own the underlying infrastructure—and the customer is responsible for protecting their data. Failure to acknowledge the customer's role in data protection has introduced unmanaged risk to countless businesses as they often assume that the native tooling and default configurations are good enough. Sadly, this misstep leaves many companies ill-equipped to properly combat and deal with ransomware attacks—many realizing this gap only after irreversible data loss or a destructive breach has occurred.[7]

**Fulfilling your business' role in the shared responsibility model:**

**The cloud service provider's (CSP's) role:**

The cloud service provider is responsible for the infrastructure and underlying services.

**Your (the customer's) role:**

Data protection is the customers' responsibility. This includes data entering, stored within, and leaving the system.

## DEDICATED SOLUTION REQUIRED

Protection measures don't stop with simply understanding the shared responsibility model; they require purpose-built tools to properly safeguard and recover data from today's threats. We find three key components where dedicated solutions extend beyond native capabilities—to offer cyber resilient data protection from ransomware, internal bad actors, and accidental deletion events.

### Data Isolation

While malicious attacks can encrypt business data in Microsoft 365 production environments, separate and immutable backups maintain a protected data copy that cannot be tampered with, altered, or deleted in the event of a breach. By storing data copies outside of Microsoft 365 in a separate security domain, third- party solutions can ensure that ransomware attacks which successfully penetrate Microsoft environments, cannot also infect backup copies.

### Extended Retention

While Microsoft offers short-term retention via its recycling bins, it's critical to employ a long-term data retention policy and solution that removes any limitations you might otherwise encounter with your SaaS-native backup options. This means all active and deleted data can be recovered in the event of a breach, regardless of how old the data is.

### Rapid Recovery

Backing up data means nothing without recovery. When it comes time to restore business-critical data within Microsoft 365, it's imperative that you have fast, flexible, and full-fidelity recovery options. Purpose-built solutions offer the performance and precision needed to quickly restore invaluable data, limit downtime, and deliver higher levels of business continuity.

## YOUR GUIDE TO MICROSOFT 365 PROTECTION

Microsoft 365 encompasses an abundance of critical emails, files, communications, sites, and more. Your data backup should tap into as much of this data as possible. Leading solutions like Commvault® Cloud, powered by Metallic® AI, give you in-depth coverage of data living across Microsoft 365, including Exchange Online, SharePoint Online, OneDrive for Business, and Teams. This ensures no application is left behind and that your invaluable productivity data is comprehensively protected from data loss and attack.

**Here are 5 key must-haves when selecting a data protection solution.**

### Built in Storage and Retention

The right cloud backup solution doesn't have limitations. With Commvault, you get air-gapped storage and extended retention included for all-inclusive TCO. Not only are backup copies isolated and separate from Microsoft 365 source data, but customers get better peace of mind—knowing that your data is always recoverable.

### Employ Rapid Recovery Controls

Not all solutions are created the same. Commvault gives users unrivaled control to quickly restore data with full fidelity back to a specific location or points-in-time. Users can immediately search to locate relevant data sets, and roll specific items or entire applications back to previous versions, helping recover data rapidly in the event of a breach or attack.

### Don't Skimp on Security

Effective data protection starts with a strong foundation. Commvault Cloud is built on hardened security and a multi-layered approach to security. All backup copies are isolated from source environments, data is encrypted at-flight and at-rest, and zero-trust user access controls prevent unwarranted access to systems and data.

### Look Beyond Microsoft 365

Commvault Cloud delivers the coverage, security, and scale to empower businesses of all sizes to tackle their biggest data protection challenges. With comprehensive coverage across SaaS applications like Microsoft 365 and Dynamics 365, and hybrid cloud workloads running in Azure like SAP HANA, Oracle, Kubernetes, and more—Commvault delivers comprehensive coverage of Microsoft 365, the Microsoft Cloud, and beyond.

## Next steps

Simplify and save with Commvault's Cloud-Delivered SaaS cyber protection. Experience cost and complexity reduction with our hassle-free deployment, hands-off maintenance, and no big upfront investments required. Cyber resilience for wherever your data lives.

Get more value from your data and gain true cyber resilience without compromising your business. Visit https://www.commvault.com and **contact us** for more information.

[1] SighHouse, CH Daniel, Microsoft 365 Suite Revenue and Growth Statistics (2023), January 2023.

[2] Macrotrends, Microsoft Revenue 2010-2023

[3] AAG, The Latest 2023 Ransomware Statistics

[4] Jai Vijayan, Dark reading, Researchers Report First Instance of Automated SaaS Ransomware Extortion, June 2023.

[5] Microsoft Office 365 still the top target among phishing attacks: https://www.techrepublic.com/article/microsoft-office-365-still-the-top-target-among-phishing-attacks/

[6] Astra, Nivedita James Palatty, 100+ Ransomware Attack Statistics 2023: Trends & Cost, October 2023.

[7] The SaaS App Scaries: Staying Ahead of Ransomware Missteps: https://metallic.ioblog/saas-app-scaries-ransomware

To learn more, visit **commvault.com**