Technology Report

DCIG

Microsoft 365's New Best Friend: AI-infused Data Protection Software

By DCIG Principal Data Protection Analyst, Jerome Wendt

DCIG

TECHNOLOGY REPORT

Microsoft 365's New Best Friend: AI-infused Data Protection Software

Contents

The Age of Denial: It's Officially Over

Not so long-ago businesses could try to live in denial about their chances of being affected by ransomware. For better or worse, a recent Verizon report officially brought this age of denial to an end. Among its findings, it found that ransomware does not discriminate and has become ubiquitous affecting all size businesses about equally.

In creating this report, Verizon examined over 16,000 actual, real-world incidents and over 5,000 data breaches. These occurred in 2023 across businesses in all industries. Businesses in every industry—educational, financial, food services, government, healthcare, information, insurance, manufacturing, mining, and technology—experienced these events.

Email remains the most common attack vector by which ransomware enters businesses.

The report further found that both small and medium businesses (SMBs) and large organizations increasingly get attacked in the same way. Due to different size organizations now using similar services and infrastructure, their attack surfaces closely resemble one another. This has led to hackers using the same attack vectors since they work equally well on all businesses.

Across them, email remains the most common attack vector by which ransomware enters businesses. Verizon found that business email compromise doubled across its entire dataset from 2022 to 2023. This increase in the use of email for attacks comes despite the number of ransomware attacks not growing statistically from 2022 to 2023.[1]

This puts services such as Microsoft 365 in the spotlight. Microsoft 365 commands 30 percent of office productivity software worldwide and 44 percent of the US market share.[2]

As a result, ransomware targets data stored in Microsoft 365's OneDrive, Outlook, SharePoint, and Teams in its attacks. Protecting data stored in these applications from ransomware dictates that businesses employ the appropriate solutions now.

Microsoft's Data Protection Offerings

Businesses may logically first look to and expect Microsoft to protect any data they store in Microsoft 365. In response, Microsoft has taken multiple steps to meet this growing business expectation.

To ensure high levels of application and data availability and security, Microsoft hosts Microsoft 365 in Microsoft Azure. Hosted there, businesses gain access to its physically secured data centers that offer high levels of availability and redundancy.

Microsoft also provides multiple cybersecurity tools. These include a cyber secure perimeter with firewalls, antivirus software, and multiple tools for monitoring and detecting cyber threats.

Microsoft 365's available cybersecurity tools now include Microsoft Defender. Defender prevents ransomware by detecting and disrupting attacks within Microsoft 365 itself. It works across multiple Microsoft 365 components to include Exchange and Teams and offers built-in automation to reverse malicious activities.[3]

Finally, Microsoft plans to introduce its own Microsoft 365 Backup solution sometime in 2024. While still in preview, organizations may soon access and use it as part of the Microsoft 365 Admin Center under Settings. Using this option, they can perform backups and restores of Exchange, OneDrive, and SharePoint data.[4]

Defenses and offerings such as these may lead businesses to conclude that Microsoft alone offers sufficient levels of data protection. By taking advantage of and utilizing these tools, they may see little or no need for additional data protection software.

Microsoft's Stated Position on Data Protection

Before any businesses decide they do not need any additional data protection software, Microsoft's published position contradicts that conclusion. Microsoft adheres to a shared responsibility model that encompasses protecting data hosted in any Microsoft service.

Since Microsoft 365 is a software-as-a-service (SaaS) and available from Microsoft, it falls under Microsoft's shared responsibility model. In this model, Microsoft only assumes responsibility for delivering its Microsoft 365 service and maintaining its availability. Further, Microsoft assumes no responsibility for data stored by businesses in Microsoft 365. Rather, it clearly states businesses ***always retain responsibility*** for their data.[5]

> ***Microsoft recommends that businesses regularly back up data that they host with Microsoft using a third-party backup application.***

Microsoft recommends that businesses regularly back up data that they host with Microsoft. The Service Availability section of the Microsoft Server Agreement includes some cautionary notes about Microsoft's cloud services, which include Microsoft 365.

It highlights how no Microsoft cloud services come with guaranteed levels of service and may suffer occasional disruptions and outages. It then recommends businesses use third-party applications and services to back up data stored in its cloud services.[6]

This recommendation from Microsoft should prompt businesses to recognize that Microsoft may not meet all their data protection needs, even with its forthcoming Microsoft 365 Backup offering. If anything, businesses should heed Microsoft's prompting to use a third-party backup application to back up their Microsoft 365 data.

Two Factors that Influence the Buying Decision

The question for many businesses then becomes, *"Which third-party application should they use to back up and protect the data they host in Microsoft 365?"* The answer to this question for each business somewhat hinges on two factors:

- The Microsoft 365 services, or components, that each business uses.
- The level of protection that the third-party application provides for data stored in Microsoft 365.

Backup Factor #1: The Microsoft 365 Services Used by a Business

To select a third-party backup solution, businesses must first quantify the Microsoft 365 services that they use. While the answer to this question may sound simple on the surface, it can possibly become quite complex.

Many businesses may assume they only use and store data in Exchange or Outlook, OneDrive, SharePoint, and Teams. However, businesses may fail to realize these represent only four of the over 50 applications and services available in Microsoft 365.[7]

Since few businesses use all Microsoft 365 services, they focus on backing up data in Microsoft 365's four core services. Unfortunately, businesses still cannot assume every any backup application will fully protect all their data in these four core Microsoft 365 services.

In the case of the forthcoming Microsoft 365 Backup, it has yet to mention any support for Teams. In contrast, most third-party backup applications advertise backing up Microsoft 365 data that resides in all four services. However, many do not back up these four Microsoft services as comprehensively as businesses might need or expect.

For instance, most third-party Microsoft 365 backup applications protect Exchange and OneDrive quite well. However, significant differences emerge when comparing how well they protect data stored in SharePoint and Teams. Only a few provide comprehensive, in-depth backup for these two Microsoft 365 services.

Running afoul of Microsoft 365 service limitations may represent the larger challenge when doing large restores.

Backup Factor #2: Protect and Restore Data Stored in Microsoft 365

Businesses may tend to first evaluate Microsoft 365 backup applications based on how well they back up Microsoft 365 data. That viewpoint certainly has merit. Backup remains a core component of a third-party Microsoft 365 backup application for multiple reasons. Microsoft can and does infrequently go offline. Users may also accidentally delete, overwrite, or change data.

However, solely evaluating third-party Microsoft 365 backup applications on their backup capabilities no longer represents the optimal approach. Backing up or restoring Microsoft 365 data presents a potentially larger challenge than businesses may realize. This issue primarily surfaces when businesses need to back up or restore large amounts of data from or into Microsoft 365.

Consider restores. Restoring hundreds of gigabytes or terabytes of data to Microsoft 365 takes time and can be tedious. However, running afoul of Microsoft 365 service limitations during these times may represent the larger challenge in the restoration process. Microsoft throttles the number of API calls that applications may make to Microsoft 365 services during a specified period.

For instance, a specific application can make no more than 10,000 API requests in a 10-minute period to Outlook. Microsoft also limits an application to uploading no more than 150MB into Outlook during a 5-minute period. Microsoft imposes similar limitations on OneDrive, SharePoint, and Teams when making API or upload requests to them.[8]

Microsoft throttles access by third-party applications to resources within Microsoft 365 for practical reasons. It takes these steps to safeguard Microsoft 365's operations. However, throttling impacts the ability of third-party backup applications to complete their job in a timely manner. If performing large data restores into Microsoft 365, this activity may take hours, days, or even weeks to complete.

These Microsoft 365 service limitations should prompt businesses to re-examine how to best protect their data in Microsoft 365. While restoring small amounts of data into Microsoft 365 rarely represents a challenge, large restores become problematic. This makes it incumbent upon businesses to take steps to avoid data loss in the first place.

To achieve this objective requires using a third-party backup application that protects data while it still resides in Microsoft 365. This requires the backup application to actively monitor Microsoft 365 for activities that contribute to data corruption or loss.

Ransomware and user error represent the two most common reasons for data corruption or loss. To identify and prevent either of these occurrences, the third-party backup application must minimally accomplish the following key objective. It must detect, alert on, and potentially stop suspicious activity and behavior on data residing in Microsoft 365.

The Need for Artificial Intelligence in Third-party Microsoft 365 Backup Applications

Performing these functions requires third-party Microsoft 365 backup applications to include artificial intelligence (AI) as a core capability. The backup application will still perform backups and restores of Microsoft 365 data. However, the backup application's AI feature should constantly monitor the business' data hosted in Microsoft 365.

Third-party Microsoft 365 backup applications should now include AI as a core capability.

In this role, it looks for any suspicious activity with respect to the business' data. For instance, it may monitor large or unexpected amounts of read activity on Microsoft 365 data. Since over 90 percent of ransomware events start with data exfiltration, this may indicate an attack has begun.[9]

It may also monitor for large or unusual data changes or deletions in Microsoft 365. While the activity may be appropriate, it may alternatively indicate the start of a ransomware attack. It may also indicate an intruder has hijacked or obtained user credentials to access Microsoft 365.

A third-party backup application actively monitoring for these activities provides at least two potential benefits for businesses. It can minimally generate alerts and make businesses aware of these activities. However, it can also ideally act and prevent data exfiltration, deletion, or encryption from ever occurring.

This prompt reaction to any suspicious behavior also provides other important benefits in a Microsoft 365 environment. It can mitigate the need for businesses to perform large scale restores of data into Microsoft 365.

Even should ransomware or an intruder delete or encrypt some data, an early warning and taking immediate action can help minimize any data loss. This keeps data restores small and helps ensure non-disruptive use of Microsoft 365 even when an event occurs.

These benefits make AI an almost must-have component for any third-party Microsoft 365 backup application being considered. It both complements current Microsoft data protection features and positions businesses to get in front of any potential ransomware event.

SpinOne's Robust Data Protection for Microsoft 365

SpinOne offers this new generation of robust data protection that businesses need to holistically protect their Microsoft 365 data. SpinOne starts by providing three options for deep, yet flexible, levels of data protection for Microsoft 365 available today. These options include Backup and Archive, Backup with Ransomware Detection and Response, and Backup with Data Loss Prevention (DLP).

Like other third-party Microsoft 365 backup applications, SpinOne, by default, protects all key components of OneDrive, Outlook, SharePoint, and Teams. However, SpinOne sets itself apart by delivering deep, granular levels of protection in both SharePoint and Teams.

In SharePoint, it represents one of the few backup applications that protects SharePoint's Content Database, Settings and Views, and Site Groups. Likewise, in Teams, SpinOne stands apart from competitors by protecting 1:1 User Messages and Group Mailbox Calendars.

Once it protects Microsoft 365 data, SpinOne then gives businesses a choice of cloud storage targets to store backups. They may choose to keep their backups in Microsoft Azure. However, should Microsoft Azure go offline, businesses may lose access to both Microsoft 365 and their backups.

To avoid this scenario, businesses may separately choose to store their backups in Amazon Web Services (AWS), Google Cloud, or their own cloud storage. In this way, SpinOne backups remain accessible even should Microsoft 365 become unavailable.

However, backing up Microsoft 365 represents only one side of the equation. Businesses must consider the time it takes for them to recover and to what point in time they can recover.

SpinOne addresses these concerns by first offering a 2-hour ransomware recovery service level agreement (SLA). SpinOne's 2-hour SLA distinguishes itself in two ways. It represents of the few SLAs available in the market. Then, it delivers recoveries as fast as or faster than almost any of its competitors.

Further, Spin.AI includes technology in SpinOne to help organizations avoid having to grapple with RPOs, RTOs, or SLAs. Instead, SpinOne seeks to detect ransomware attacks, stop them, and recover any compromised data before the business must formally act.

SpinOne's greatest strength lies in how it implements and leverages AI to detect and act on suspicious activities in Microsoft 365.

SpinOne Infuses AI into Microsoft 365 Data Protection

SpinOne's greatest strength lies in how it implements and leverages AI to detect and act on suspicious activities in Microsoft 365. SpinOne infuses AI functionality into its software-as-a-service (SaaS) which always monitors activity in Microsoft 365.

Its AI feature uses a behavioral analysis algorithm that constantly analyzes activity in a business' Microsoft 365 account. SpinOne uses behavioral analysis as opposed to other techniques such as pattern matching or virus signatures.

Ransomware continues to rapidly evolve with hackers now using AI to create new ransomware strains. Using behavioral analysis currently provides the best means available to proactively detect new ransomware strains.

SpinOne's behavior analysis algorithm also provides another distinct benefit. As a SaaS service, SpinOne monitors activity across hundreds of thousands of Microsoft 365 user accounts in thousands of businesses. This provides it with real-time visibility into any new forms of ransomware activity occurring in any of these accounts.

This visibility has contributed to SpinOne becoming more effective at identifying ransomware than other antivirus solutions. By way of example, Spin.AI recently compared how well SpinOne did against Microsoft Defender in identifying common forms of ransomware.

In this internally conducted test, SpinOne simulated eleven (11) different types of ransomware attacks. During the test SpinOne successfully identified each ransomware strain, isolated it, and stopped the in-progress ransomware attack. In contrast, Microsoft Defender could only identify a small number of them.

Now, in full disclosure, Spin.AI did set the conditions for the test and ran the test itself. Further, Spin.AI used Microsoft Defender's administrator dashboard default settings during the test. As such, one might expect Spin.AI to successfully detect all ransomware strains in a test it set up and ran.

However, Microsoft Defender in its default configuration failed to detect many common ransomware strains. This default configuration likely resembles the one that businesses may adopt if using Microsoft Defender in their Microsoft 365 environment.

In contrast, SpinOne's AI-infused data protection does more than detect these and other ransomware strains. It generates an alert. It isolates the attack and stops an in-progress ransomware attack. Finally, it identifies and restores any data changed, deleted, encrypted by the ransomware attack. In this way, SpinOne works with Microsoft to ensure businesses have uninterrupted access to Microsoft 365 and their data.

Microsoft 365's New Best Friend: SpinOne's AI-infused Data Protection

Living in denial about either ransomware's pervasiveness or a business' reliance upon Microsoft 365's continuous availability comes with significant risks. Any downtime of Microsoft 365 for whatever reason minimally impacts business operations and often results in lost productivity and sales.

This makes Microsoft 365 a prime target for many strains of ransomware. This also makes it prudent for businesses to adopt solutions that identify and stop ransomware attacks on Microsoft 365 before they impact production.

Microsoft already offers multiple features and services to ensure Microsoft 365 remains highly available and secure. This is to Microsoft's credit. It remains focused on constantly improving its various offerings, services, and platforms to better meet its customers' needs.

However, Microsoft publicly acknowledges that businesses need to look to third parties to address certain needs. Obtaining a third-party backup application that backs up, restores, and protects Microsoft 365 data represents one of those needs.

SpinOne's AI-infused data protection SaaS represents such a solution that meets these needs. Spin.AI has developed SpinOne to protect data stored in Microsoft 365 in three ways as it:

- Efficiently backs up Microsoft 365 data with some of the highest backup throughput speeds available.
- Effectively restores data into Microsoft 365, often completing restores in under two hours.
- Comprehensively protects data still in Microsoft 365 by detecting ransomware, isolating it, stopping in-progress attacks, and restoring any affected data back into Microsoft 365.

Spin.AI's three-pronged approach to Microsoft 365 data protection does more than protect Microsoft 365 data. SpinOne's AI-infused data protection solution represents the new standard by which all businesses should measure third-party backup applications. In so doing, businesses maximize their investment in Microsoft 365 while having the confidence that any data they store in it remains safe from a ransomware attack. ■

> ***SpinOne's AI-infused data protection solution represents the new standard by which all businesses should measure third-party backup applications.***

Sources

1. https://www.verizon.com/business/resources/T3b9/reports/2023-dbir-executive-summary.pdf. Pg. 6. Referenced 2/13/2024.
2. https://www.statista.com/statistics/983299/worldwide-market-share-of-office-productivity-software/; https://www.statista.com/statistics/983321/worldwide-office-365-user-numbers-by-country/. Referenced 2/27/2024.
3. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-office-365#tabx9b8a3721f0524083a6ae013152d5755c. Referenced 2/14/2024.
4. https://learn.microsoft.com/en-us/microsoft-365/syntex/backup/backup-overview. Referenced 3/26/2024.
5. https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility. Referenced 2/14/2024.
6. https://www.microsoft.com/en-gb/servicesagreement/#6_serviceAvailability. Referenced 2/14/2025.
7. https://www.microsoft.com/en-us/microsoft-365/products-apps-services. Referenced 2/14/2024.
8. https://learn.microsoft.com/en-us/graph/throttling-limits. https://learn.microsoft.com/en-us/sharepoint/dev/general-development/how-to-avoid-getting-throttled-or-blocked-in-sharepoint-online. Referenced 2/28/2024.
9. https://www.blackfog.com/the-state-of-ransomware-in-2023/. Referenced 2/28/2024.

About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of TOP 5 Reports and Solution Profiles. More information is available at **www.dcig.com.**