Osterman Research

# WHITE PAPER

**White Paper** by Osterman Research
Published **July 2020**
Sponsored by **Yubico**

# Improving Performance and Security While Driving Down the Cost of Microsoft 365

# Executive Summary

Microsoft 365 (the new package of offerings formerly known as Office 365) is Microsoft's cloud service offering for individual productivity, team collaboration, and enterprise communication, complemented by a set of security and compliance capabilities. Microsoft offers several services bundles for Microsoft 365, and it recently rebranded the personal and business market focused versions of Microsoft 365 under its wider Microsoft 365 nomenclature. For the time being, the Microsoft 365 plans focused on the enterprise market are still available with Microsoft 365 branding. It is unclear how long Microsoft will retain the Microsoft 365 E3 and E5 service names, but its challenge will be differentiating these from the duplicated stream names in the current Microsoft 365 plan family (which could be as simple as jumping to E3, E5, E7 and E9, but conjecture on branding directions for Microsoft is not our intent). This white paper focuses on the Microsoft 365 plans targeted at the Enterprise market – E3 and E5.

## KEY TAKEAWAYS

Microsoft 365 delivers a range of long-offered and new style productivity and collaboration tools, ranging from cloud-enhanced versions of the original Word, PowerPoint and Excel suite, along with cloud-delivered editions of Exchange and SharePoint that negate the need for on-premises servers, the new Microsoft Teams application, and a plethora of less adopted services such as Microsoft Planner and Yammer. It's a capable offering that's been widely embraced by organizations across the world.

Equally, however, is the reality that Microsoft 365 comes with some shortcomings in the areas of security, archiving, backup, data protection, eDiscovery, and other key aspects of the offering. Relying solely on the native capabilities in Microsoft 365 can lead to challenges, such as missed security threats, duplicate efforts to perform eDiscovery across an organization's data landscape, and the inability to recover accidently deleted data. The use of third-party solutions in parallel with Microsoft 365 can address many of the platform's shortcomings. Many third-party vendors build best-of-breed offerings rather than taking a broad-stroke approach to features.

***Microsoft 365 comes with some shortcomings in the areas of security, archiving, backup, data protection, eDiscovery, and other key aspects of the offering.***

Evaluating the initial adoption or ongoing use of Microsoft 365 requires a due diligence process. Our suggestions include:

- Do a deep dive on the security, archiving, data backup, and eDiscovery features available in Microsoft 365, paying attention to the engineering reality of what is available today. Marketing promises and assertions offer some insight (and will usually run ahead of the engineering directions), but the code is the reality.

- Develop a clear understanding of your organization's requirements, processes, legal situation, and regulatory compliance mandates as these intersect with the capabilities offered in Microsoft 365. Build this understanding through engagement with the various teams responsible for these issues within your organization. Your analysis will highlight where the features available in Microsoft 365 come up short against your organization's requirements.

- Shortlist and prioritize the buying criteria for your organization. Buying decisions look different when the criteria changes – for example, lowest initial cost versus total cost of ownership versus having access to the right functionality.

- Prepare a plan for how the shortcomings in Microsoft 365, as highlighted for your organization in Step 2 above, will be addressed before rolling out Microsoft 365. This includes considering how third-party solutions fit as part of addressing these shortcomings. It's unlikely that reduced security capabilities, less responsive eDiscovery tools, or insufficient data protection capabilities will benefit your organization.

- Understand how third-party vendor solutions can supplement the native capabilities in Microsoft 365 to improve performance, reduce risk, reduce administrative effort, drive down costs, and offer a better fit between requirements and capabilities.

### ABOUT THIS WHITE PAPER

This white paper is sponsored by Yubico; information about the company is provided at the end of this paper.

# Improving Security in Microsoft 365

Microsoft offers a set of default security capabilities in Microsoft 365, as well as making available more advanced protections in its higher priced Microsoft 365 licensing packages. These security capabilities provide a baseline of protection for Microsoft 365-centric apps and content, but threats continue to evade Microsoft's protections and many organizations also have apps and systems that are not provided as part of Microsoft's offering. Third-party security solutions can deliver higher catch rates for spam, phishing, and malware, and can also strengthen defenses against more sophisticated threats, including business email compromise (BEC) and account takeover attempts. Afterall, using Microsoft exclusively to protect Microsoft has historically not been a winning strategy.

### CATCH RATES FOR MALICIOUS CONTENT

Catch rates for all malicious content must be high, including ransomware, fileless malware, spam, phishing, and other advanced threats (such as timed threats in documents and URLs that turn malicious only after initial scanning has completed) must be very high. It only takes one phishing email that evades detection and gets acted on to result in a compromised account, and if the compromise is not identified immediately, the successful attacker can move laterally to compromise additional internal accounts, seed ransomware across the data estate, or create fraudulent invoicing trails. Likewise with broad-based phishing attacks, which have increasingly been used for distributing ransomware.

***Catch rates for all malicious content must be high.***

### CO-EXISTENCE WITH THIRD-PARTY SOLUTIONS

Security solutions from third-party vendors must be able to co-exist with Exchange Online Protection (EOP) and Advanced Threat Protection (ATP) in Microsoft 365. Co-existence is necessary because few organizations are all-in exclusively with Microsoft 365, and thus need to build comprehensive protections that deliver coordinated security across the entire landscape of people, data and systems. Co-existence is also necessary because no single vendor will ever catch and prevent all inbound and outbound threats, and thus strong multi-vendor solutions enable organizations to build stronger defenses in light of an enterprise security and risk analysis. While EOP and ATP are helpful offerings, threat-ladened emails are still regularly getting delivered to inboxes, such as fake Microsoft 365 billing demands and phishing emails from previously compromised accounts. Independent email security vendors often include leading-edge innovations that detect threats not caught by Microsoft's tools.

### MALWARE

The infiltration of malware can be the result of payloads in an email; a malicious link in an email, a social media post or a poisoned search engine result; or via a drive-by attack while web surfing. While many bad actors have moved onto other attack vectors, more traditional malware remains a common one. It's also important to note that new forms of malware are sometimes fileless: to avoid detection by anti-virus tools, malicious sites will insert HTML and JavaScript into browser memory that function as spyware to steal credentials. Without any kind of executable file to examine, these threats can avoid malware detection systems.

## TARGETED ATTACKS

Threat actors are continually devising new attack methods to outrun advancements in security defenses. Targeted attacks and other advanced threats are becoming increasingly difficult to identify without causing large numbers of false positives, and thus strong protections are essential. Microsoft 365 offers a set of capabilities to protect against targeted and advanced threats, but complementary offerings from some third-party vendors can deliver stronger protections in a number of areas.

- Microsoft 365 Advanced Threat Protection (ATP) offers enhanced document and URL checking safeguards for Microsoft file types and email messages routed through Exchange Online in Microsoft 365. Organizations with non-Microsoft 365 versions of Microsoft Office (e.g., Office 2019 and earlier), file types beyond the apps in Microsoft 365, and on-premises email systems that don't route email through Microsoft 365, will not be protected by Safe Links and Safe Attachments. Third-party solutions often provide link verification and attachment analysis for a broader set of file types and applications.

- Email is the common denominator between organizations for communication, sharing documents and requesting help, and while newer style tools – such as Slack and Microsoft Teams are becoming more widely adopted – email remains the predominant channel within organizations too. With so much interaction and business happening through email messages, the ability to assure the trustworthiness of every email message is essential. Broad-based phishing and targeted spear-phishing emails are a frequent vector for seeking to compromise account credentials, and there's a general sense across the industry that phishing emails are getting more deceptive and thus harder to catch by employees. At some point, it will become impossible for all but the most highly trained security professionals to tell the difference between a valid email message and an impersonation or threat-bearing one. It is essential, therefore, that the identification of credential phishing messages is highly effective – for email messages from external parties, compromised internal accounts, and compromised accounts at firms in the supply chain.

- Time-of-click URL checking, as offered by Microsoft 365 ATP Safe Links, supports dynamic scanning of URLs in Office documents and URLs in Outlook email messages. By design, Safe Links does not support URL scanning for other productivity and collaboration apps used by employees within an organization.

- Once a malicious email message reaches a user's inbox, the likelihood of the user being compromised increases greatly. As soon as an active threat in the email message is detected, that intelligence should be shared across all inboxes to eradicate other copies or derivates of the message in real-time – or close to it. Zero-Hour Auto Purge (ZAP) in Microsoft 365 offers some capabilities for sharing intelligence and taking policy-defined actions on email messages in Exchange Online only. It is unclear how close to real-time signal sharing happens for newly identified malicious emails.

- Microsoft 365 offers several protections against CEO Fraud and BEC attacks, such as policies for anti-phishing, anti-spoofing and anti-impersonation. Anti-impersonation settings are only available with the Microsoft 365 E5 plan and require an explicit declaration of domains to watch out for. Third-party vendors add advanced protections not available in Microsoft 365, such as protections against homograph domain attacks (from look-alike and sound-alike domain names), deep checking on domain similarities (including across international character sets), and email writing style analysis, among others. Email style analysis, for example, triggers warning alerts when the writing style of an email appears unusual or abnormal in comparison to a previously developed model of the writing style of the supposed sender. Advanced capabilities to protect against CEO Fraud and BEC attacks reduce the likelihood that a threat actor will succeed, because early warning signs in the message and its characteristics are used to stop the attack before it reaches the targeted users.

***Threat actors are continually devising new attack methods to outrun advancements in security defenses.***

## AN INTEGRATED VIEW

Despite a proliferation of security capabilities in Microsoft 365, security staff still struggle to maintain a big picture view of current and evolving threats. The point offerings in Microsoft 365 provide product or type specific threat analysis within Microsoft 365, but a single, integrated interface for monitoring all security solutions in Microsoft 365 is not available, nor is one available that combines security threat signals across Microsoft 365, other cloud services, and on-premises software. Some third-party security solutions excel in providing integration across multiple solutions.

In our ongoing 2019 analysis of Microsoft 365, we have noted that a single, consolidated list of all threat types should be offered to improve a security analysts' overall understanding of the changing threat landscape. Threat Explorer in Microsoft 365 offers only filtered slices of threat data – for example, malware, phishing, and user-reported threats – but not a consolidated list. However, as of May 2020 Threat Explorer has been updated to include a new "All Email" view, something that was not there previously.

## DATA LOSS PREVENTION AND SECURE MESSAGING

DLP solutions protect against accidental and malicious leakage of sensitive information by employees; it's a security solution to minimize the quantity and severity of insider threats. General purpose DLP solutions use brute force approaches to stop-and-block messages and documents that violate policy. More specialized DLP solutions, on the other hand, offer an array of nuanced capabilities to keep communication flowing, for example by sanitizing a message by redacting sensitive information or encrypting it, in situations of accidental sharing rather than blocking the message entirely (and requiring manual intervention to release). Many organizations benefit from the availability of nuanced policy configuration and enforcement options.

- Data loss can happen through any file type, and a DLP solution should work across all of the file types and applications used by people within an organization. The DLP offering in Microsoft 365 protects Microsoft Office file types and common web formats, but not much beyond. Organizations with widespread usage of file types not covered by Microsoft 365 should look at third-party DLP solutions which provide much broader coverage of file types used across organizations.

- An extensive set of standard, DLP policies enables organizations to rapidly achieve protection against data loss. Even if these are only enabled in monitoring mode, policy matches quickly highlight areas of risk and concern. Microsoft offers only a single out-of-the-box DLP policy in Microsoft 365 that identifies credit card numbers in email messages. No other policies are available out-of-the-box and new policies must be curated by each organization instead (although Microsoft does offer a set of templates for creating new DLP policies). Some third-party solutions include a more extensive set of DLP policies that are enabled by default, providing immediate protection for customers.

- DLP policies should be configurable to work only in specific jurisdictions or regions, rather than unilaterally across the entire organization. Microsoft 365 includes some abilities to limit the applicability of DLP policies by jurisdiction, but these focus on explicit inclusions or exclusions using Exchange distribution groups, SharePoint sites, OneDrive accounts, and Teams chat and channel messages; there is no option for jurisdictional configuration. Only organizations subscribing to the Multi-Geo service in Microsoft 365 can limit DLP policy execution by jurisdiction.

- Messages and content that violate a DLP policy should be able to be directed to a role – such as the sender's manager or a document author's departmental compliance manager – rather than to a specific individual (e.g., a security administrator). Role-based routing and notification ensures proper review of

***DLP policies should be configurable to work only in specific jurisdictions or regions, rather than unilaterally across the entire organization.***

content for breaches of sensitive information rules, the details of which are more likely to be hidden from security administrators. DLP policies in Microsoft 365 can only route violations to a specific individual.

## IDENTITY ACCESS MANAGEMENT

Identity access management offers nuanced security methods for reducing risk, limiting exposure, and enforcing higher protections when needed. Attributes about the user, their login location, their current device, and the type of action they are requesting – among others – can be evaluated in combination to determine risk levels applicable to a given login attempt, access request or attempted action. If risk is low – for example an employee in the office on their corporate device is requesting a document in SharePoint – access can be granted immediately. Alternatively, a login attempt from a senior finance executive from an overseas location on an Internet terminal to access the payroll spreadsheet should trigger many more security signals, and in response, for example, an additional multi-factor authentication prompt could be required, or only read access to the spreadsheet given. In the current context of many employees newly working from home, nuanced security is essential. Microsoft 365 E3 does not offer identity access management for Office apps; a subscription to the highest priced Microsoft 365 offering is required (Microsoft 365 E5), or instead a license Azure AD Premium. Third-party vendors also offer identity access management tools to support Microsoft 365 customers, and all can be secured through multi-factor authentication methods.

Fundamentally, conditional access and rights management policy is part of the identity administrative options that are used to set different levels of access based for users. Setting parameters on who can access what data is one way to "monitor" who and how data might pass from one place to another is a best practice. The whole notion of "risk mapping" is focused on who has access to which type of company data. The more sensitive the information, the higher the need to put in place additional layers of security. As one example, a security key for privileged accounts can be used to confirm a user's credentials so that impersonations cannot occur.

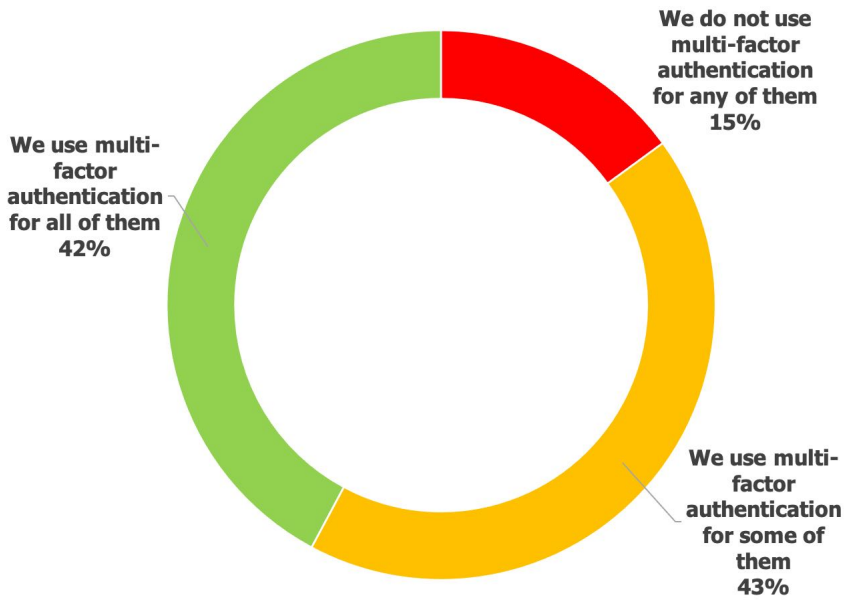
## STRENGTHENING AUTHENTICATION

Relying on a username and password as the credentials for gaining access to a system or data has proven highly insecure and costly. People forget their password and call their internal help desk for a reset (costing IT staff time on password resets). People give their password away to a threat actor – unintentionally usually – through a successful phishing attack (which leads to a data breach with all the associated financial consequences). Or people use a short list of common or easy to break passwords through brute force attacks (which also leads to a costly data breach or ransomware attack). Too many Microsoft 365 accounts are insecure due to the reliance on passwords. Removing passwords as the credential of choice is a strong step in the right direction of enhancing security and decreasing the likelihood of account compromise and data breaches. Similarly, organizations reduce risk by requiring that their third-party vendors take an equally cautious approach to how their systems integrate with Microsoft 365. Third party vendors that rely on the storage and use of admin credentials to connect systems are cautioned against.

***Relying on a username and password as the credentials for gaining access to a system or data has proven highly insecure and costly.***

Our research found that only 42 percent of organizations employ multi-factor authentication for all of their non-admin users in Microsoft 365, while slightly more use multi-factor authentication for only some users. However, for more than one in seven users, multi-factor authentication is not employed, as shown in Figure 1.

Figure 1
Use of Authentication in Microsoft 365 Environments




*Source: Osterman Research, Inc.*

***Too many Microsoft 365 accounts are insecure due to the reliance on passwords.***

The problem is that too many Microsoft 365 accounts are insecure due to the reliance on passwords. Removing passwords as the credential of choice is a strong step in the right direction of enhancing security and decreasing the likelihood of account compromise and data breaches. Newer authentication approaches for Microsoft 365 based on public key cryptography enabled by a hardware token or security key represent the current best-in-class security on offer for Microsoft 365, reducing the likelihood of successful attacks by orders of magnitude. If going passwordless is too far a step to take, at minimum enable a strong form of multi-factor authentication, eschewing reliance on SMS codes and email messages for either an Authenticator app (a secure option) or a hardware security key (the most secure option). The use of Azure MFA or smart card infrastructure to secure login to Active Directory accounts used to access Microsoft 365 provides a robust defense to account takeovers and other threats. Moreover, accessing Microsoft cloud-based apps can be accomplished from both on-premises and hybrid methods, and so it is essential to secure the infrastructure using a more secure method as discussed above.

## EMAIL RETRACTION

When a user sends a message in error, Microsoft's approach for retracting the email in Microsoft 365 only serves to highlight its content to the recipients, since the retraction message requests recipients to delete the message but takes no automated action to do so. If sensitive data has been inadvertently sent to unauthorized recipients, it is entirely up to their judgment to comply with the retraction request. For administrators, there are several options available for automatically removing unread messages from mailboxes within the originating Microsoft 365 tenant, but if an automated deletion request is scoped wrongly many other messages will be deleted as well, and these capabilities do not work for messages sent beyond the tenant.

## REMOVING MALICIOUS CONTENT

In our 2019 analysis of Microsoft 365, we wrote that once malicious content is identified in a mailbox, it should be possible to remove all instances of it from all mailboxes in one step. At the time, Microsoft 365 offered Zero-Hour Auto Purge

(ZAP), which only partly addressed this requirement. ZAP would automatically move a newly classified malicious message from a user's inbox to their Junk folder but could not delete it permanently or move the offending message to the quarantine, meaning the user still retained access through their Junk folder. Microsoft 365 also offered PowerShell options for hard deleting malicious content, but if scoped incorrectly, it would also hard-delete valid content from users' mailboxes.

Now, however, messages classified as spam or phish can now be moved to Quarantine, rather than to the user's Junk Folder. For phish messages, the movement applies for both read and unread messages. For spam messages, the processing only applies to unread messages in a user's inbox. Even so, this does not work for Exchange on-premises mailboxes, even if they are supported by Exchange Online Protection (EOP).

Moreover, Microsoft is in the process of deprecating the earlier Search Mailbox PowerShell command that hard-deleted messages. It is being replaced with New-ComplianceSearchAction which offers a purge action for removing malicious content from all mailboxes and shared mailboxes, but unlike the earlier cmdlet, only soft deletes messages. On balance, Microsoft now meets the requirement we suggested in 2019.

## Improving Management of Microsoft 365

While Microsoft 365 offers a number of administrative capabilities, there are some challenges involved with managing the platform using native tools when conducting things like forensic analysis. For example:

- There are multiple screens and consoles for admins to access, all with different views and no consolidated view of on-premises and cloud activity. For example, the Microsoft 365 Audit Log service does not capture events from on-premises Microsoft servers for organizations with a hybrid setup, such as Active Directory domain controllers, Exchange Server and SharePoint Server, in addition to Microsoft 365.

- Auditing can be difficult to configure. Admins must configure audit policies separately for on-premises and cloud workloads. There is no way to monitor audit policies in the event they change or are disabled by other administrators.

- There is limited alerting, searching and reporting functionality. Alerting is inconsistent across on-premises and cloud workloads and it is not possible to search audit activity across on-premises and cloud. Admins cannot search based on actor (i.e., who initiated the activity) or many other important fields.

- It can be difficult to interpret events. Audit data is raw (contains SIDs, GUIDs and other IDs), lacks friendly display names and the format changes. Moreover, there is no normalized format of what fields are displayed, so event formats will vary depending on the event or cloud workload an admin is reviewing.

- There is a limited history of audit data. Audit data is retained only for a limited time before it is permanently lost. For cloud workloads, the retention period varies based on workload and subscription type. Retention but can be as short as seven days, but Microsoft can change retention periods at any time. For on-premises workloads, the retention period varies based on the volume of activity. Plus, the limited data retention has significant implications for organizations that must comply with legal or regulatory retention requirements that dictate retention of this data for much longer periods. This can hinder an organization's ability to investigate security incidents because they lack sufficient historical evidence to search.

***While Microsoft 365 offers a number of administrative capabilities, there are some challenges involved with managing the platform using native tools.***

# Improving Archiving in Microsoft 365

Decisions on meeting compliance requirements and mitigating business risk shape an organization's preferred strategic approach to archiving, backup and eDiscovery. With Microsoft 365, Microsoft delivers its own particular flavor of archiving, backup and eDiscovery. Particularly for organizations with data outside of Microsoft 365, but even with those heavily Microsoft 365 centric, the use of third-party solutions can offer better alignment with how an organization wants to deal with these issues than blindly adopting Microsoft's model.

Archiving ensures that relevant content is kept for compliance, record keeping, employee searching, and historical analysis. Archived content should be kept for as long as required, stored securely to prevent content alteration (e.g., tampering), stored securely to prevent unauthorized access (e.g., data breach), and deleted when retention timeframes have lapsed. For the few organizations that solely use the major workloads in Microsoft 365 and operate under only light compliance mandates, Microsoft's approach to archiving may meet current requirements. For the majority, however, where multiple data producing systems are used, compliance mandates are becoming more strident, and third-party content is proliferating, using a third-party archiving solution is likely to provide better native support for disparate content types and repositories.

- Preserving the content and metadata of messages, posts, documents and other content items in as native a format as possible ensures the original context and metadata are captured. This is essential for subsequent data restoration, if required, or for early case assessment in response to an eDiscovery request. Microsoft ignores the native format principle in Microsoft 365, converting third-party data into an Exchange email format on ingestion – for diverse content types such as documents, Facebook posts, and Twitter messages. Check whether the modern data formats in use by your organization are better supported in third-party tools, as opposed to relying on Microsoft's one-size-fits-all legacy approach.

- Compliance teams, legal departments and senior management benefit from having an integrated, centralized view of all archived data, that can be both browsed and searched. With Microsoft 365, data that has been created in an appropriate Microsoft 365 workload can be searched (but not browsed), along with data ingested from third-party systems. For organizations with data stored outside of Microsoft 365, a multi-repository, centralized view is not possible without using third-party tools.

- Creating a separate, independent location for archived data is required by some organizations, rather than relying on an in-place archival approach. Microsoft only supports in-place archiving of Microsoft 365 data, along with using Microsoft 365 as a separate archival storage location for third-party data (after ingestion and conversion to an Exchange email message format). For Microsoft 365 data, archiving to a separate location is not supported by Microsoft, but is on offer from third-party vendors.

- Retention, preservation and disposition policies apply uniformly and without variation across a user's mailbox and their archives in Microsoft 365. There is no option for granular targeting of policies to support differential requirements, such as disposition policies that apply differently to a user's archive than their primary mailbox. More granular options with support for targeted requirements are offered by some third-party vendors.

***A third-party archiving solution is likely to provide better native support for disparate content types and repositories.***

# Improving Data Backup and Recovery

Archiving is often confused for backup and vice versa, and while these are both best practices offering strategic value, they differ substantially:

- Archiving is intended for continuous and long-term (sometimes indefinite) retention of all relevant business content that might be needed for regulatory, legal, knowledge management or analytics purposes. The goal with archiving is to retain business records for long periods to protect loss of critical business data.

- Backup is focused on capturing periodic snapshots all of the content on an endpoint, server or other device for purposes of quickly recovering from a hardware failure, a ransomware attack, a rogue employee's or administrator's deletion of data, or some other problem that results in data loss. For organizations that value quick response and easy recovery of critical data in Microsoft 365, backups are an essential component of any data protection infrastructure.

Third party backup is necessary for the protection of data and serves a variety of useful functions, supporting an IT team's need for agility in restoring lost data in current use. This functionality becomes even more critical given Microsoft's handling of data in Microsoft 365.

***Microsoft offers only 1-1-0 backup, due to no additional copies beyond the original data, stored only in Microsoft 365, and with no data stored offsite beyond Microsoft 365.***

## WAYS THAT NATIVE RECOVERY FALLS SHORT

Microsoft does not offer a "yes, absolutely" statement for the ability to recover data that has been accidentally or maliciously deleted or corrupted from the various workloads within Microsoft 365. Rather, customers are confronted with a long list of "it depends" statements, which vary by workload and even by features within a given workload. For organizations that need certainty for data protection and recovery – rather than exceptions with lots of wriggle room for Microsoft to effectively say "it's your own fault" – a third-party backup solution should be considered.

Most organizations need certainty for data protection and recovery – rather than exceptions with lots of wriggle room for Microsoft to effectively say "it's your own fault" – and opt for a third-party backup solution.

- Microsoft's paradigm for data backup in Microsoft 365 is different to how third-party data backup solutions work. Microsoft 365 embraces a data backup "in-place" approach, with data restoration enabled through a complex of trash bins from which users can recover their own deleted items, special trash bins with extended actual deletion timeframes from which administrators can recover deleted items, and exemptions on data deletion in legal hold situations. Third-party solutions, on the other hand, avoid the in-place paradigm in preference for an actual backup of data outside of the native and original data system.

- Microsoft's approach for protecting data stored in Microsoft 365 relies on Microsoft 365 protecting itself, which violates the fundamental 3-2-1 principle of data protection. The principle states that three copies of data should be made, on two different forms of storage media, and with one of the three copies stored away from the original system. Microsoft, by contrast, offers only 1-1-0 backup, due to no additional copies beyond the original data, stored only in Microsoft 365, and with no data stored offsite beyond Microsoft 365.

- Data protection is not uniform across the various Microsoft 365 workloads, with retention timeframes and recovery approaches variable across Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams. Further reducing assurance of recovery integrity is the variation within workloads by content types – such as channels, files and conversations within Microsoft Teams.

- Recovering corrupted data from an Exchange mailbox, OneDrive account or SharePoint site is not well supported in Microsoft 365. Point-in-time recovery is not available for Exchange mailboxes- an essential feature should an inbox be infected with ransomware. A third-party backup vendor allows you to restore an individual user's inbox to a state in time before the attack occurred.

- Granular recovery is not supported in OneDrive accounts (restoration is only to a point in time in the past 30 days, subject to the recycle bin not being emptied), and all content restored for a SharePoint site or subsite is "all or nothing" (granular recovery is not supported, as with OneDrive). Third-party solutions offer granular and flexible recovery options, down to the individual email or file folder level and without data overwrites.

- Recovery and management of departed user data in Microsoft 365 follows time-based retention policies and can be cumbersome to access and control. Third party backup supports moving documents between OneDrive accounts without having to restore the entire account, and more seamless off-boarding of users while retaining access to key company documents stored in their OneDrive account.

## OTHER ISSUES TO CONSIDER

Microsoft offers several strategies for backing up and recovering data in Microsoft 365 that might be changed or lost, but there are more serious issues for Azure Active Directory (AD) recovery. Just as on-premises AD recovery is important to prevent outages in the event of a human configuration error or (worse yet) a cyber-attack, the same goes for Azure AD given an organizations' increasing reliance on Azure AD for authentication to various non-Microsoft cloud apps (in addition, of course, to Microsoft 365).

Many customers make the mistake of assuming they are covered in Azure AD since they are hybrid, meaning they sync on-premises AD to Azure AD. If they have on-premises AD recovery, it will be recovered and then re-sync to the cloud.

But that's not the case, since Azure AD has objects and properties that do not exist in on-premises AD, including, Roles, Licenses, Multi-Factor Authentication (MFA) settings, Conditional Access policies, Dynamic group definitions and Applications and service principals. In short, recovering data in Azure AD using native tools works well if the scenario fits two fairly rigid guidelines:

- Admins want to recover an Azure AD user, Microsoft 365 group or Azure AD application that was deleted (not modified).

- No more than 30 days have passed since the object was deleted.

For other scenarios, such as those below, admins will need a backup and recovery solution:

- Azure AD objects that are soft deleted including user and guest accounts, Microsoft 365 groups (including associated data such as properties, members, e-mail addresses, Exchange Online shared inbox and calendar, SharePoint Online team site and files, OneNote notebook, Planner, Teams, and Yammer group and group content), and Azure AD applications.

- Azure AD objects that are immediately hard deleted include security groups, distribution groups, service principals, conditional access policies and devices.

- Soft-deleted objects remain in the Recycle Bin for only 30 days. After that, they are permanently deleted.

***Recovery and management of departed user data in Microsoft 365 follows time-based retention policies and can be cumbersome to access and control.***

- Many Azure AD objects have complex configurations or specific interactions with other systems. Those details are not captured by the Recycle Bin and cannot be restored from it.

- Finally, the Recycle Bin is for deleted objects only. If an object has been changed rather than deleted, the Recycle Bin cannot help an admin restore the object to its previous state.

## eDISCOVERY

Both threatened and actual legal action requires tools to expedite discovery of responsive content across an organization's data landscape, enabling the legal team to quickly assess the extent of the organization's legal exposure, or to decide that the action is without merit. If content must be preserved for a pending legal action, the ability to seamlessly place legal holds across content systems ensures compliance with procedural rules and avoids further charges of spoliation.

Reliance on Microsoft 365's tools for eDiscovery comes with some shortcomings:

- Microsoft repeatedly says that its search timeframes for content and eDiscovery searches are reducing, but no SLA is offered to put weight behind the promise. Search timeframes are thus only best-effort and organizations can never be sure how Microsoft 365 will respond on a given day, a situation that some third-party eDiscovery vendors refuse to embrace in preference for an actual SLA.

- Organizations with multiple corporate data repositories require the ability to use a cohesive eDiscovery tool to search all repositories, both in the cloud and on-premises. Data should be queried in whatever original content systems have been embraced by the organization, without first requiring ingestion into Microsoft 365. Microsoft's eDiscovery tools in Microsoft 365 support content search for native content in most Microsoft 365 workloads, and also for whatever other data has been imported into Azure (for analysis with Advanced eDiscovery in Microsoft 365) but is unable to search Exchange and SharePoint servers on-premises, nor any other corporate data repositories in use by the organization. Some third-party vendors offer eDiscovery tools that search across all corporate data repositories, eliminating the need for using multiple, disparate eDiscovery systems.

- Project and task tracking capabilities for case management enable clear communication and task allocation between multiple people working on an eDiscovery case. Microsoft's eDiscovery tools in Microsoft 365 do not offer project and task tracking capabilities. Organizations should look to third-party tools for better support of eDiscovery workflow.

- Litigation holds should be enforceable across all relevant corporate data repositories used by the organization, both in the cloud and on-premises. The tools in Microsoft 365 enable litigation holds to be placed on most of the content types in Microsoft 365 (most, but not all), and content in on-premises repositories is both invisible to an eDiscovery search and non-addressable by litigation hold. This is true irrespective of whether the repositories are based on Microsoft's server tools or those of any other vendor. Organizations with multiple data repositories that require unified litigation hold capabilities should explore what third-party vendors have to offer.

- Organizations with people in multiple legal and compliance jurisdictions often require the ability to restrict eDiscovery searches by jurisdiction or region, so that compliance professionals in a given region are not able to include people outside their region in a search scope. Microsoft offers some capabilities to enable search restrictions in its Compliance Boundaries offering. This involves selecting a directory attribute that will segregate people into different compliance groupings, and this is enforced through search permission filters across a Microsoft 365 tenant. However, Microsoft's approach with Compliance Boundaries is

***Litigation holds should be enforceable across all relevant corporate data repositories used by the organization, both in the cloud and on-premises.***

fundamentally flawed, because while the specified attribute ensures identification of users within the boundary, there is no historical tracking of users by boundary attribute; it offers real-time identification only not historical alignment. A scoped search will therefore, by design, be unable to find any content for users who were previously in a different boundary for a historical search but have subsequently moved into a new boundary.

- eDiscovery cases created in the original version of Advanced eDiscovery in Microsoft 365 cannot be transitioned to the new version. Historical cases will be orphaned in the original version, and Microsoft announced that it will not be providing support to organizations for eDiscovery cases in the original version from October 2020. Even within Microsoft 365, therefore, organizations reliant on eDiscovery capabilities will have multiple eDiscovery dashboards to check depending on the version offered by Microsoft. This is not the first time Microsoft has deprecated eDiscovery capabilities in Microsoft 365 without a migration path for existing eDiscovery cases.

# Cost of Ownership Issues to Consider

There are a significant number of SKUs for Microsoft 365 covering a wide range of price points, some of which are industry-specific. However, the two plans we will consider in this analysis are Microsoft's two most popular business/enterprise plans, E5 and E3, which retail for $57.00 and $32.00 per user per month, respectively.

***There are a significant number of SKUs for Microsoft 365 covering a wide range of price points, some of which are industry-specific.***

Plan E5 provides the full array of security, archiving and other capabilities available in Microsoft 365, but it is possible to employ Plan E3 in combination with third-party solutions that will either supplement or replace some of the native capabilities in Microsoft 365. In the opinion of Osterman Research, there are three primary reasons for doing so:

1. Improve the performance of Microsoft 365 in key areas like security, archiving, backup, etc.

2. Provide for a more efficient and effective set of capabilities for organizations that employ non-Microsoft solutions.

3. Drive down the overall cost of Microsoft 365.

## COMPARING THE PLANS

As shown in Figure 2 below, here are two basic options for deploying Microsoft 365 and what is included in each.

**Figure 2**
**Capabilities in Microsoft 365 Plans E5 and E3**

| Capability | Plan E5 | Plan E3 |
|---|---|---|
| Microsoft 365 applications (Word, Excel, PowerPoint, OneNote and Access) | Included | Included |
| Office mobile apps and Office for the web | Included | Included |
| Outlook | Included | Included |
| Exchange | Included | Included |
| Bookings | Included | Included |
| Microsoft Teams | Included | Included |
| SharePoint | Included | Included |
| Yammer | Included | Included |

**Figure 2 (cont'd.)**
**Capabilities in Microsoft 365 Plans E5 and E3**

| Capability | Plan E5 | Plan E3 |
|---|---|---|
| OneDrive for Business | Included | Included |
| Microsoft Stream | Included | Included |
| Sway for Microsoft 365 | Included | Included |
| Power Apps | Included | Included |
| Power Automate | Included | Included |
| Planner | Included | Included |
| To Do | Included | Included |
| MyAnalytics | Included | Included |
| Windows Enterprise | Included | Included |
| Microsoft 365 Admin Center | Included | Included |
| Microsoft Intune | Included | Included |
| Windows Autopilot, fine-tuned user experience, and Windows Analytics Device Health | Included | Included |
| Microsoft Endpoint Configuration Manager | Included | Included |
| Windows Hello, Credential Guard, and Direct Access | Included | Included |
| Azure Active Directory Premium Plan 1 | Included | Included |
| Microsoft Advanced Threat Analytics | Included | Included |
| Windows Defender Antivirus and Device Guard | Included | Included |
| Microsoft 365 data loss prevention | Included | Included |
| Windows Information Protection and BitLocker | Included | Included |
| Azure Information Protection 1 | Included | Included |
| Microsoft Secure Score | Included | Included |
| Microsoft Security and Compliance Center | Included | Included |
| Audio calls | Included | Not Included |
| Phone system | Included | Not Included |
| Power BI Pro | Included | Not Included |
| Azure Active Directory Premium Plan 2 | Included | Not Included |
| Microsoft Defender Advanced Threat Protection | Included | Not Included |
| Microsoft 365 Advanced Threat Protection | Included | Not Included |
| Azure Advanced Threat Protection | Included | Not Included |
| Azure Information Protection 2 | Included | Not Included |
| Cloud App Security | Included | Not Included |
| Advanced eDiscovery, Customer Lockbox, Advanced Data Governance, Service Encryption with Customer Key, Privileged Access Management | Included | Not Included |

*Source: Osterman Research, Inc.*

***For many years, Osterman Research has been tracking organizations' philosophies with regard to how they would like to deploy Microsoft 365.***

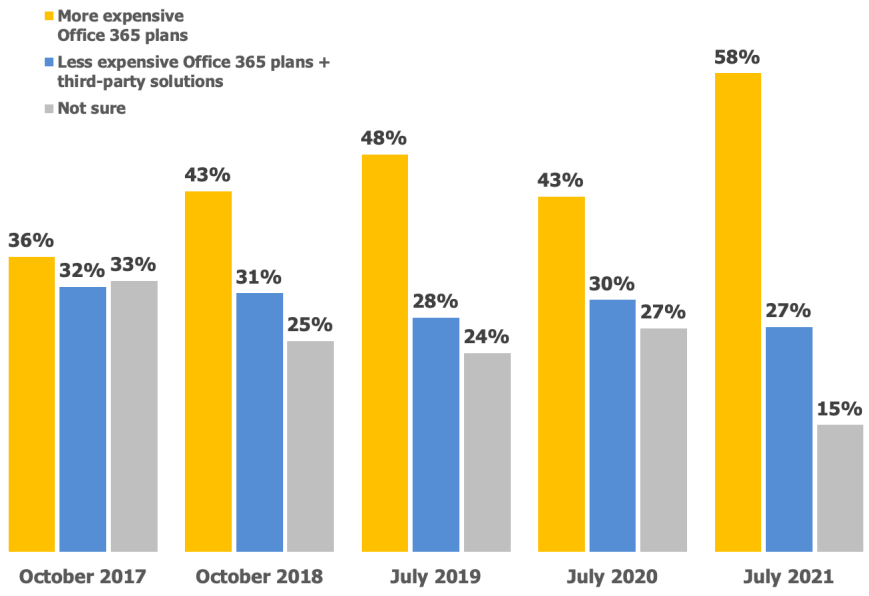
So, what decision makers need to determine in their evaluation of Microsoft 365 is whether they should implement the "full meal deal" – Plan E5 – at $57.00 per user per month, or implement a more limited set of Microsoft-provided capabilities – Plan E3 – at $32.00 per user per month (along with whatever discounts can be obtained from Microsoft).

## USING THIRD-PARTY SOLUTIONS

For many years, Osterman Research has been tracking organizations' philosophies with regard to how they would like to deploy Microsoft 365 – namely, go with the top plan from Microsoft (Plan E5 or its equivalent); or use a less expensive, less capable plan in combination with third-party solutions that supplement Microsoft's native capabilities. As shown in Figure 3 from various Osterman Research survey exploring

this issue, a plurality of organizations want to deploy more expensive plans, but many are simply not sure how they ultimately would like to proceed.

**Figure 3**
**Past and Projected Preferences for Deploying Office/Microsoft 365**




*Source: Osterman Research, Inc.*

If decision makers opt to consider Plan E3, they need to determine which of the features not available in Plan E3, but available in E5, they would like to replicate (or improve) with third-party solutions. Assuming list prices for both Microsoft 365 plans, that would give decision makers a budget of up to $25.00 per user per month for these third-party solutions. Our analysis of pricing from a variety of vendors found the following prices for various third-party solutions that can be used in conjunction with Microsoft 365 for low-volume purchases:

- **Security**
  Cloud solutions that will provide a robust set of security capabilities on par or somewhat more capable than Microsoft 365 Advanced Threat Protection average approximately $5.25 per user per month. Adding in the cost of a security key or hardware token will add only minimally to the cost on a per-user basis – assuming a three-year lifetime for a security, the cost would equal only about $1.20 per user per month.

- **Archiving**
  Cloud-based archiving solutions that will archive email and files from Microsoft 365 accounts, as well as from other cloud-based solutions, average approximately $5.60 per user per month.

- **Backup and recovery**
  Solutions that will provide true backup and recovery capabilities that are superior those available in Microsoft 365 average approximately $5.00 per user per month (but some solutions cost less).

- **Integrated solutions**
  An integrated solution that includes email security, archiving, eDiscovery and compliance capabilities – often suitable primarily for smaller organizations – average about $5.60 per user per month.

***If decision makers opt to consider Plan E3, they need to determine which of the features not available in Plan E3, but available in E5, they would like to replicate (or improve) with third-party solutions.***

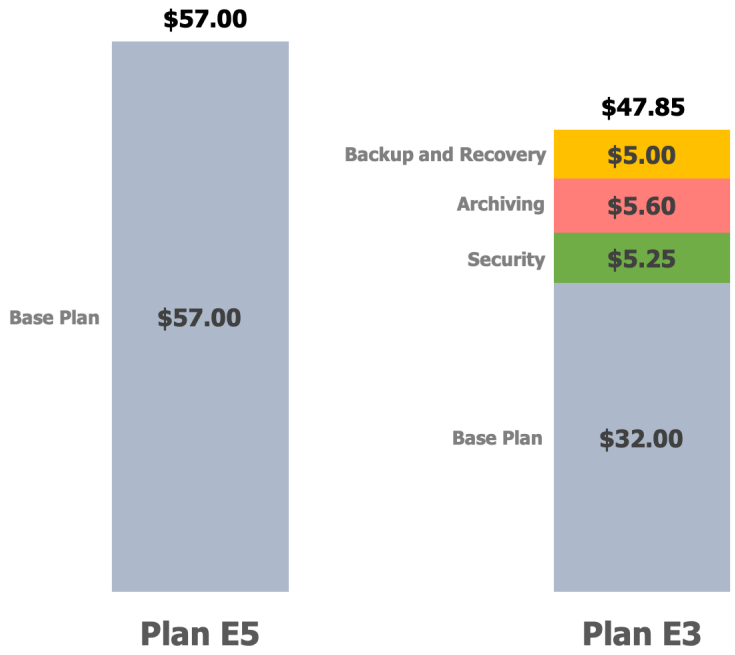
- **CASB solutions**
  A CASB solution, similar to the Cloud App Security offering in Microsoft 365 Plan E5, averages about $9.65 per user per month.

It's important to note that prices vary widely across different vendors' solutions, but these averages are a good representation of pricing for current solutions. Moreover, for the sake of comparing "apples-to-apples", we have not included third-party capabilities like email uptime/continuity that will increase the reliability of Microsoft 365 deployments.

## COMPARING THE COSTS

As shown in Figure 4, a combination of Plan E3 with three third-party solutions – to provide security, archiving and backup and recovery capabilities – will total $47.85 per user per month compared to $57.00 per user per month for Plan E5. This represents a savings of 16 percent. For an organization of 1,000 users, that represents a savings of $329,400 over a three-year period.

**Figure 4**
**Costs of Plan E5 vs. Plan E3 With Third-Party Solutions**




*Source: Osterman Research, Inc.*

***A combination of a lower level Microsoft 365 plan, like E3, in combination with third-party solutions will offer three important advantages compared to using Plan E5.***

Of course, there can be significant variability in terms of discounts that might be obtained by Microsoft plan or third-party vendors, different SKUs that are used for different users across the organization, the evaluation process in the selection of third-party solutions, and so forth. In response to this variability, however, it's our contention that a combination of a lower level Microsoft 365 plan, like E3, in combination with third-party solutions will offer three important advantages compared to using Plan E5:

- A lower overall total cost of ownership.
- Better performance than the capabilities provided natively within Microsoft 365. By no means are we implying that the native Microsoft capabilities aren't useful

and provide good functionality, but our review points to more robust performance with various third-party solutions.

- The ability to better support non-Microsoft data sources and applications.

What we have not compared here are the less quantifiable costs, such as native security in Microsoft 365 that could miss a security threat that a third-party solution would not have allowed.

# Next Steps

When managing or considering the move to Microsoft 365, ensure the decision includes input from IT architects, security professionals, and those responsible for the organization's legal, risk and compliance practices. Avoid unilateral decision making, since its impacts are multi-lateral and multi-faceted, and affects the organization for years to come. Having a clear understanding of the features and functions in Microsoft 365 – including Microsoft's near-term roadmap – is a necessary part of this due diligence process.

Decision makers should understand the limitations in Microsoft 365 before deployment, rather than being surprised after the fact that what they assumed to be true was baseless hearsay or wrongly asserted by Microsoft's marketing machinery. Unfortunately, this is not always the case and decision makers are faced with underserved constituents and missing capabilities that compromise the organization in the areas of security, archiving, data protection and eDiscovery.

Part of understanding the limitations in Microsoft 365 is undertaking a comparative cost analysis to ascertain the licensing cost savings available by using third-party solutions in combination with the lower priced Microsoft 365 plans. For example, organizations with multiple data repositories subject to eDiscovery and litigation hold should check if the higher priced Microsoft 365 plans are as cost effective as a lower priced plan with a best-of-breed third-party solution instead. The same is true in the other areas covered in this white paper.

For a more comprehensive cost analysis beyond licensing only, factor in the differential labor costs incurred to accomplish similar tasks using Microsoft 365 only and Microsoft 365 with third-party tools.

***Decision makers should understand the limitations in Microsoft 365 before deployment, rather than being surprised after the fact.***

# Summary and Conclusions

Microsoft 365 offers a comprehensive set of tools for productivity and collaboration, is widely used by organizations across the world, is growing very quickly, and has a strong business partner network available to support organizations taking the plunge into cloud services. In other words, the risk to an organization of non-performance by Microsoft with Microsoft 365 for productivity and collaboration is low. Most organizations will benefit from using Microsoft 365 in comparison to deploying on-premises solutions, such as Exchange. If it aligns with your business needs and IT strategy, we encourage you to consider embracing Microsoft 365.

In the areas of security, archiving, data protection, eDiscovery, and other key aspects of the platform, be aware that Microsoft 365 has some shortcomings. While its feature sets are improving, there are fundamental architectural decisions in Microsoft 365 in the above areas that Microsoft has so far been unwilling to revisit, such as native support for non-Microsoft 365 data repositories, and an alternative to in-place archiving. Using third-party solutions offers a strategic route for organizations where the one-size-fits-all approach of Microsoft 365 actually doesn't fit. In fact, many cybercriminals use an instance of Microsoft 365 to test their attacks before they are executed, and thus greater heterogeneity has even further benefits.

This white paper has covered a broad range of topics, highlighting areas of shortcoming in each. Your internal due diligence process, by comparison, needs to focus on the specific business, security and compliance requirements for your organization, and should lead to a prioritized list of essential capabilities and an honest evaluation of your organization's risk tolerance. Microsoft 365 may or may not meet these essential requirements, and even if Microsoft does offer some capabilities of relevance, a third-party solution may provide even better fit-to-purpose.

## Sponsor of This White Paper

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts.

The company's core invention, the YubiKey, delivers strong hardware protection, with a simple touch, across any number of IT systems and online services. The YubiHSM, Yubico's ultra-portable hardware security module, protects sensitive data stored in servers.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed and loved by 9 of the top 10 internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.

yubico

www.yubico.com

@Yubico

+1 844 205 6787

sales@yubico.com