GIGAOM

Image credit: monsitj

Ned Bellavance
Jul 2, 2021

The Cost of Microsoft 365 Data Protection

Analyzing the Total Cost of Ownership for Microsoft 365 Data Protection Solutions

Data Protection, Data Storage

The Cost of Microsoft 365 Data Protection

Analyzing the Total Cost of Ownership for Microsoft 365 Data Protection Solutions

Table of Contents

1. Summary

Organizations are adopting solutions like Microsoft 365 (formerly Office 365) to reduce administrative burden, simplify management, and gain access to rapidly evolving products and services. Microsoft 365 now has more than 258M monthly active users (MAU), a 4x increase in four years.

While the adoption of software as a service (SaaS) has been a tremendous advantage to the productivity of organizations, it is not a panacea. As with on-premises solutions, Microsoft 365 apps like Exchange Online, SharePoint Online, and Teams (which is a purely cloud app) still require added functionality from third-party vendors to provide features like data protection and robust data loss prevention. Moreover, many applications within Microsoft 365 are designed for general use cases and lack industry-specific features, forcing many organizations to look for third-party solutions to meet their business and technical requirements. For example, limitations in the eDiscovery features offered by Microsoft 365 may mean a customer will need to find a third-party solution that enhances or replaces the native eDiscovery functionality.

In this document, we will analyze Microsoft 365 licensing and features to reveal potential feature or functionality gaps. Then we will look at how Druva, a cloud data protection platform, can enhance Microsoft 365. Finally, we will show how implementing Druva in tandem with Microsoft 365 can deliver maximum value to customers with a better total cost of ownership (TCO).

2. Challenges with Microsoft 365 Data Protection

Microsoft 365 is a suite of products aimed at improving productivity and collaboration within and across organizations. Previously, companies would host and manage applications like Microsoft Exchange and SharePoint in an on-premises data center. Moving to Microsoft 365 lowers administrative overhead, increases the pace of innovation, and introduces features that were not available in on-premises deployments. However, adopting Microsoft 365 does not remove all customer responsibility for properly managing the products and data in the service.

Like all SaaS offerings, Microsoft 365 operates under a shared responsibility model that delineates the service components for which Microsoft and the customer are responsible. For instance, Microsoft is responsible for the physical security of its data centers and the availability of the Microsoft 365 services. The customer is responsible for properly securing data access through controls, meeting compliance requirements, and creating backups of data to an external location if necessary.

Microsoft may offer features that help its customers achieve required data controls, security, and redundancy, but it is up to the customer to properly configure and manage these features—and to understand them. For example, within Exchange Online, SharePoint Online, and OneDrive for Business, deleted data is available for recovery for 14 days by default and for a maximum of 30 days, after which Microsoft will permanently delete it unless there is a retention policy that stipulates otherwise. Microsoft does not offer a traditional backup solution to retain data for longer periods of time, though there are some workarounds and features, such as retention policy and legal hold, that can force a longer retention time for specific items.

To meet compliance and legal requirements, clients may want to take advantage of Microsoft 365 features like Azure Information Protection, eDiscovery, and data loss prevention (DLP). However, this is where the Microsoft 365 licensing policy becomes a challenge.

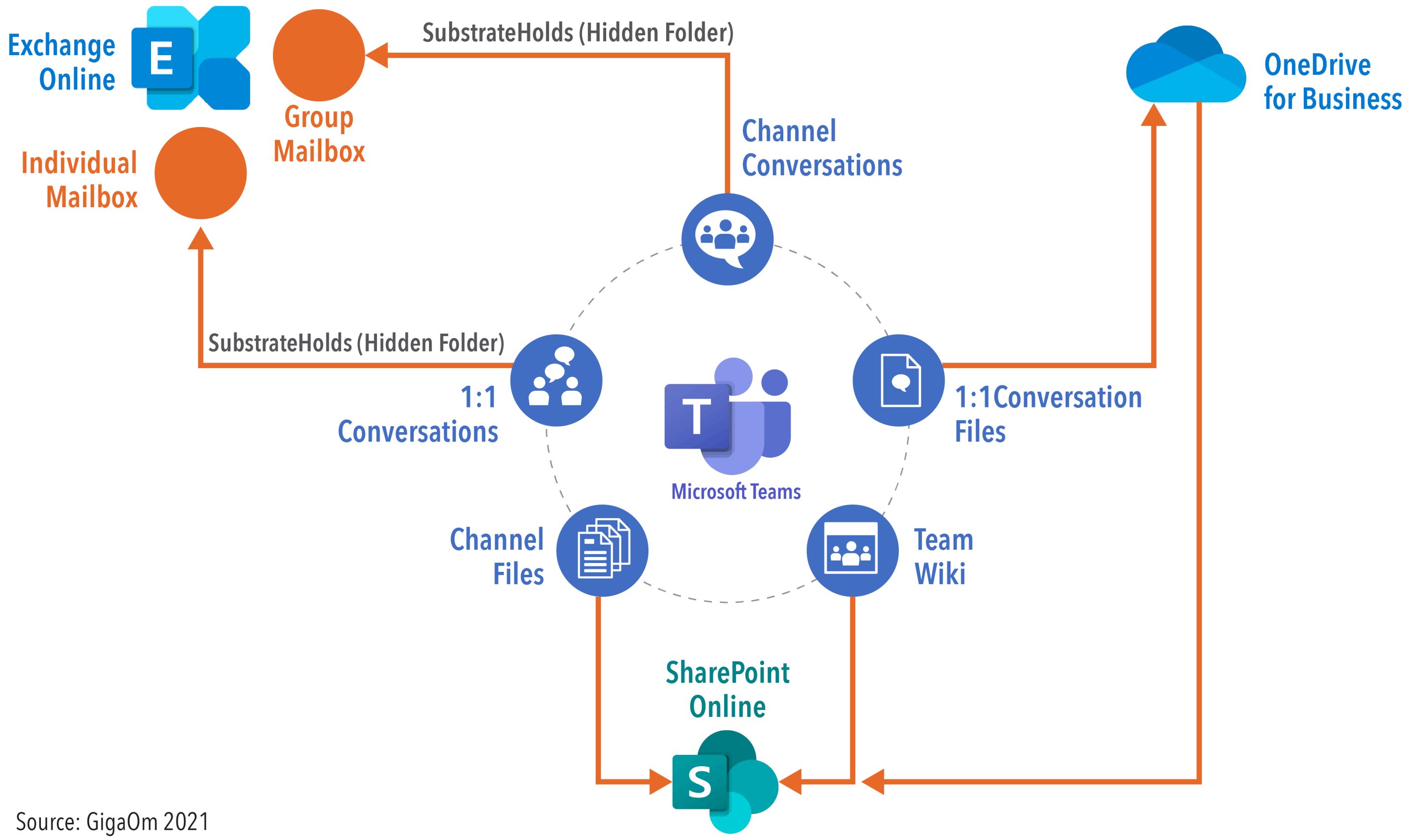
Microsoft 365 is licensed at the individual user level, and the features and functionality available to a user depend on what type of license they have been assigned. Features are bundled by license type, which means that a user may require a more expensive license to gain access to a specific feature. The jump in pricing between license types is significant, for example, E5 ($57) is $25 more than E3 ($32).

Taking advantage of those advanced features requires an enterprise-level license at the E3 or E5 level. Kiosk and frontline workers, who do not need such features and typically have an F3 license, would require licensing beyond their needs to access a single feature, incurring a significant cost increase of up to $47 per user per month.

Depending on the features needed, it can often make financial sense to implement a third-party solution rather than purchase a more expensive license. Druva is one such platform that can enhance Microsoft 365 by providing backup and recovery capabilities, and going even further to include features such as eDiscovery, legal hold, and more—for a lower price. Let’s take a look at two examples of how Druva can address the critical gaps in Microsoft 365.

Backup and Recovery

Microsoft 365 provides ways to retain data and recover a recent deletion, but it does not provide a long-term recovery solution. Moreover, for a product like Microsoft Teams that uses other Microsoft solutions, including SharePoint Online, OneDrive for Business, and Exchange Online, as well as Teams itself for storing data, things become more complicated, as shown in **Figure 1**. Properly backing up Microsoft Teams, and more importantly, recovering Teams data is extremely challenging.



Source: GigaOm 2021

Figure 1: Teams Services

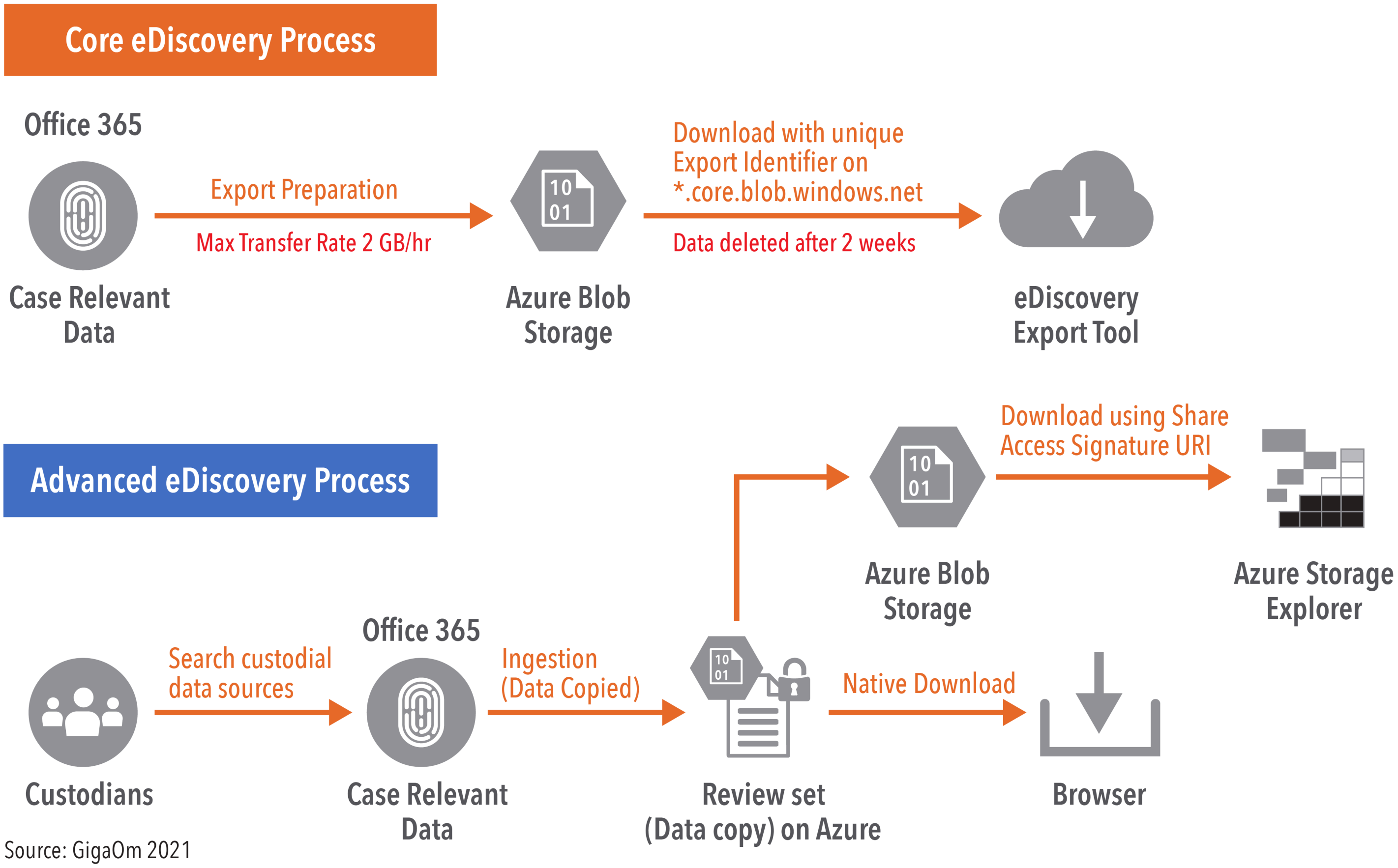
Imagine a Team was created in Teams for a special project we'll call Project Alpha. The project concluded six months ago, and the Project Alpha Team was deleted. Now a user desperately needs to recover project files from the SharePoint site associated with Project Alpha. Unfortunately, deleted Teams are only retained for 30 days and the associated SharePoint Online files for 93 days. After that, the data is permanently deleted.

Without another solution in place, Project Alpha's files are gone and that end user is out of luck. But that would not be the case if the customer had Druva for Microsoft 365. Druva can fully back up and recover Teams data for whatever retention period is deemed necessary. It understands the linkages between the disparate components of Microsoft Teams, and is able to protect each of those components, including the associated SharePoint content.

If Project Alpha had been protected by Druva, not only would you be able to recover the missing files, you would be also able to recover the entire Project Alpha Team and place those files in the proper context. Druva is also able to back up and restore data housed in Exchange Online, Exchange Online Public Folders, SharePoint Online, and OneDrive for Business.

Beyond Backup

A common request from legal and compliance teams is the ability to perform eDiscovery and place user data on legal hold. Microsoft 365 offers eDiscovery capabilities, as shown in **Figure 2**, but these require advanced, expensive licensing. Moreover, there are limits to the features and functionality of the Microsoft 365 eDiscovery solution, in terms of both the speed and amount of data exported as well as timely restore. In addition, users who are not licensed for the eDiscovery features will not be included in the search results. For time-sensitive matters that require immediate investigation, these limitations can seriously hamper the execution of legal discovery.



Source: GigaOm 2021

Figure 2: Microsoft eDiscovery Process

Druva's eDiscovery option removes many of the constraints applied by Microsoft 365, adding simpler workflows to address the needs of legal departments. Legal eDiscovery executed through Druva can include non-Microsoft 365 data sources as well. All eDiscovery data lives on Druva storage outside of Microsoft 365, avoiding a lengthy export process for long-term retention.

3. Druva for Microsoft 365

Druva for Microsoft 365 is a SaaS solution that requires no hardware or software on-premises. The platform is built on top of AWS and managed by Druva, and can also protect and manage data from other SaaS applications, like Google Workspace or Salesforce, and from endpoints such as laptops and desktops.

Data backed up by Druva is stored using multi-region redundancy with a 99.99999% data durability assurance and a 99.95% uptime SLA. The data is deduplicated, secured with a 2-factor encryption scheme, and stored in an immutable format. Data thus protected cannot be altered, protecting it from both accidental and intentional deletions and ransomware. To comply with regional and local data sovereignty laws, customers can choose where their data is stored. Druva has multiple security and compliance certifications and is the first Microsoft 365 data protection vendor certified for FedRAMP.

Druva offers three distinct plans priced per user, per month—Business, Enterprise, and Elite, priced at $2, $4, and $7, respectively, for the SaaS productivity protection plan, which includes Microsoft 365 and Google Workspace. These are the published prices, without any potential discounts applied, and these are the values we will use for our TCO analysis.

Each plan supports data protection for core Microsoft 365 applications. The Enterprise and Elite plans include additional features. The Enterprise plan, for example, supports public folders, PST download, and preserved users (archiving end user data), while the Elite adds more comprehensive features such as federated search, eDiscovery, and defensible deletion. Let’s take a closer look at these features.

Federated Search enables metadata search across all files and emails protected by Druva, including Exchange mailboxes, SharePoint libraries, OneDrive for Business, and Microsoft Teams. Federated Search is similar to Microsoft’s Content Search, but differs in the scope of data included and the search functionality supported. Federated Search can include endpoint devices protected by Druva, expanding the scope of discovery beyond Microsoft 365.

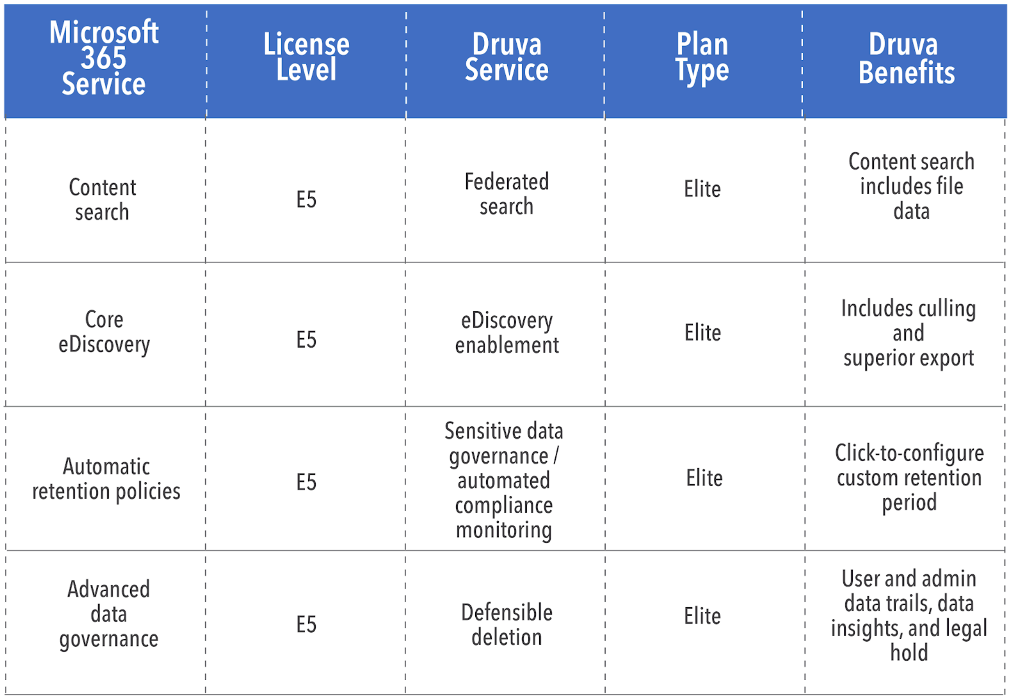
eDiscovery supports multiple operations, including placing items on legal hold to prevent deletion, pre-culling filters to reduce the volume of results, and integration with other eDiscovery platforms for export of data for litigation purposes.

Sensitive Data Governance / Automated Compliance Monitoring helps monitor sensitive data for compliance and detect such data on a proactive basis across multiple sources. This add-on for Enterprise or Elite licenses supports regional compliance templates, reporting, and alerts.

Defensible Deletion is an Elite-only feature that **lets you purge** data stored in Druva when necessary due to compliance, malware infection, or data infractions.

As **Table 1** shows, Druva provides functionality that is comparable to or better than Microsoft 365. And as we will see, this comes at a far better price per user.

Table 1: A Comparison of Microsoft 365 and Druva High-Level Licensing



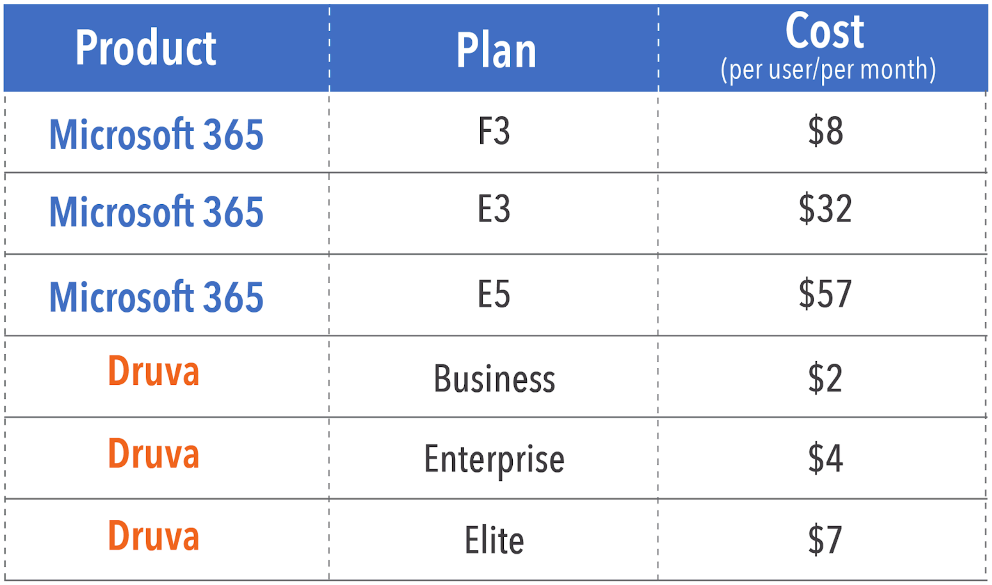
Microsoft 365 Service	License Level	Druva Service	Plan Type	Druva Benefits
Content search	E5	Federated search	Elite	Content search includes file data
Core eDiscovery	E5	eDiscovery enablement	Elite	Includes culling and superior export
Automatic retention policies	E5	Sensitive data governance / automated compliance monitoring	Elite	Click-to-configure custom retention period
Advanced data governance	E5	Defensible deletion	Elite	User and admin data trails, data insights, and legal hold

Source: GigaOm 2021

4. Cost-Benefit Analysis

To truly understand the cost-benefit proposition of using Microsoft 365 and Druva in tandem, let's examine three use cases and the costs associated with them. We'll base the pricing for Microsoft 365 and Druva on current retail prices, as shown in **Table 2**.

Table 2: Microsoft 365 and Druva Licensing Costs



Product	Plan	Cost (per user/per month)
Microsoft 365	F3	$8
Microsoft 365	E3	$32
Microsoft 365	E5	$57
Druva	Business	$2
Druva	Enterprise	$4
Druva	Elite	$7

Source: GigaOm 2021

Use Case 1: eDiscovery at Acme Corporation

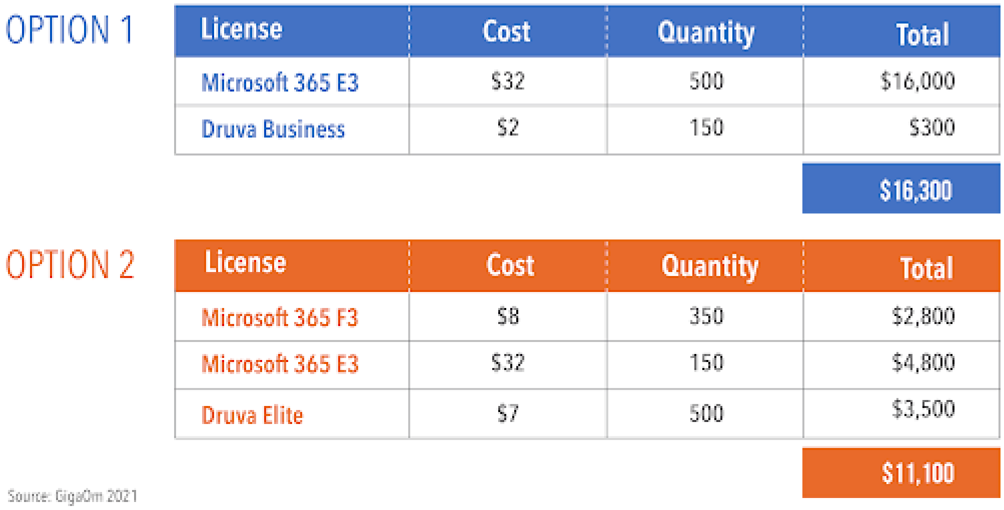
Let's first consider Acme Corporation, which has 500 employees using Microsoft 365. The company is a mix of 150 office workers and 350 field workers who work primarily on mobile devices. Acme needs eDiscovery to be available for all employees and data preservation to last beyond 30 days for the 150 office workers.

There are two potential solutions. Acme could purchase 500 E3 licenses to cover all employees, enabling them to use the Core eDiscovery service from Microsoft 365. For data protection, it could purchase 150 Business plan licenses of Druva for their office employees.

The alternative would be to purchase 350 F3 licenses for the field workers and 150 E3 licenses for the office employees from Microsoft. From Druva, the company could purchase 500 Elite licenses to meet their eDiscovery needs and provide data protection to their office workers. The F3 license from Microsoft 365 limits users to the mobile and web-based versions of Microsoft Office applications, which would be adequate for field workers.

Table 3 shows how the annual costs would work out.

Table 3: Use Case 1 Annual Cost



OPTION 1

License	Cost	Quantity	Total
Microsoft 365 E3	$32	500	$16,000
Druva Business	$2	150	$300
			$16,300

OPTION 2

License	Cost	Quantity	Total
Microsoft 365 F3	$8	350	$2,800
Microsoft 365 E3	$32	150	$4,800
Druva Elite	$7	500	$3,500
			$11,100

Source: GigaOm 2021

Total savings in license costs with Druva: $5,200 a year.

By taking advantage of Druva's eDiscovery feature, Acme Corporation would save $5,200 annually on licensing costs. As a bonus, the company would get data protection for the 350 field workers included in the Druva Elite license.

Use Case 2: Contoso Data Sovereignty

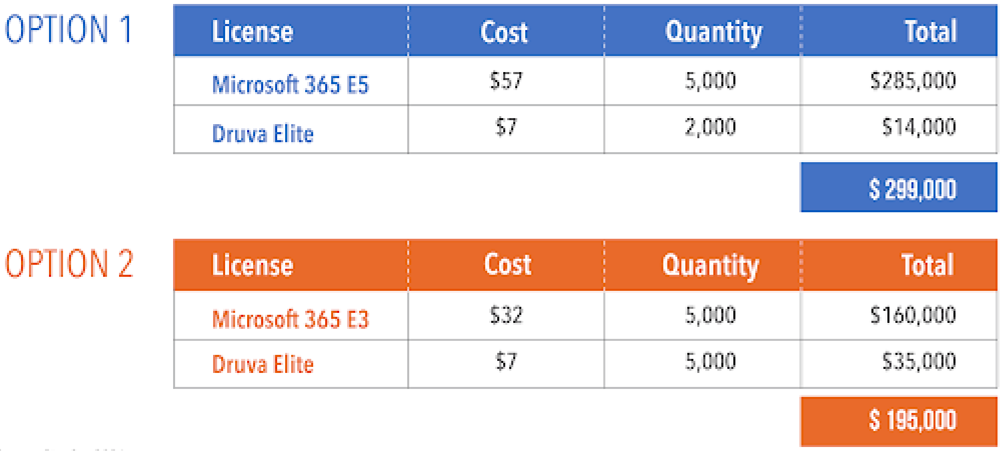
Now let's take a look at Contoso Corporation, a 5,000-seat enterprise with 3,000 employees in North America and 2,000 in the European Union. Employees across the organization need eDiscovery and content search. Data associated with the European employees must reside within the EU, and data must be purged if requested by a former employee or current customer, as directed by General Data Protection Regulation (GDPR). All Exchange mailbox, OneDrive, and Teams data must be backed up and retained for up to two years. Finally, the North American office was recently hit with ransomware, and wants to ensure that it has data protection solution safeguards in place against future attacks.

Once again, there are two ways to enable the necessary services outlined by Contoso Corporation. Under the first option, Contoso could purchase E5 licenses for all company employees to provide content search and eDiscovery. The EU employees will need Druva's Defensible Deletion feature, which is part of the Elite plan.

Under the second option, Contoso can purchase Elite plans from Druva for all employees to leverage the eDiscovery and Federated Search features included in the plan. Instead of purchasing E5 licenses from Microsoft, Contoso can go with the less costly E3 licenses for all its employees.

Table 4 shows the annual costs for the two alternatives.

Table 4: Use Case 2 Annual Cost



OPTION 1

License	Cost	Quantity	Total
Microsoft 365 E5	$57	5,000	$285,000
Druva Elite	$7	2,000	$14,000
			$ 299,000

OPTION 2

License	Cost	Quantity	Total
Microsoft 365 E3	$32	5,000	$160,000
Druva Elite	$7	5,000	$35,000
			$ 195,000

Source: GigaOm 2021

Total savings in license costs with Druva: $104,000 a year.

By leveraging Druva's eDiscovery and content searching functions, Contoso can forgo Microsoft's E5 licenses and save $104,000 annually.

Use Case 3: Legal Hold at Elmwood Trust

For our third use case, let's consider Elmwood Trust, a financial services organization with 10,000 employees and an average turnover rate of 16%. Because it is in the financial services industry, the company is required to retain employee data for individuals in key departments for two years after they leave the organization. On average, of the 1,600 employees that separate from the company each year, 5% of employees (80) must have their data retained for 24 months. Elmwood is using E3 licenses from Microsoft 365 and Elite licenses from Druva for all current employees.

To keep the data on Microsoft 365 intact and legally defensible, the company needs a valid license associated with each account. While it is possible to create inactive mailboxes without a license on Exchange Online and retain OneDrive for Business files for an extended period of time, the loss of user account associations and the potential alterations in chain of custody could cause legal headaches for the compliance department.

An alternative to keeping active licenses for former employees is to use Druva backup to preserve their data externally. Additionally, Druva's Preserved Users feature allows Elmwood Trust to retain former employee data without an assigned license for up to 10% of its current active license count. By offboarding the preservation of users' Exchange and OneDrive content for terminated employees, the company is able to reassign both Druva and Microsoft 365 licenses to new employees instead of increasing its licensing cost.

Maintaining E3 licenses for 80 terminated employees would cost $61,440 annually. By taking advantage of the preserved user licensing with Druva, Elmwood could retain the terminated employee data at no additional cost. With 10,000 active employees assigned Druva Elite licenses, 80 preserved users per year falls well below the 1,000 (10%) preserved user limit. Over the course of two years, Elmwood Trust would save $122,880 in Microsoft licensing costs for the 80 preserved users.

5. Conclusion

Adopting a SaaS solution like Microsoft 365 provides multiple benefits to an organization such as decreasing administrative burden, simplifying management, and enabling new features in a rapid cadence. However, as we have seen, the features in Microsoft 365 may not meet all of an organization's requirements. A key example is the lack of robust, long-term data protection in Microsoft 365. Organizations for which this is a necessity will need a third-party solution that meets their data protection and retention requirements. They will find that solution in Druva.

Microsoft 365 feature sets are bundled together at increasingly expensive licensing tiers, often forcing organizations to spend significantly more to gain access to a single feature at a higher license level. Rather than purchasing the more expensive license, augmenting Microsoft 365 with a third-party solution like Druva provides the same or better features at a lower price point.

Combining Microsoft 365 and Druva empowers organizations to find the right mix of features to meet their business and technical needs while minimizing licensing costs. Companies can take advantage of best-of-breed collaboration and productivity tools from Microsoft 365 while simultaneously ensuring that their data is protected and recoverable through Druva.

More information about how Druva and Microsoft 365 work better together can be found on Druva's Microsoft 365 solution page.

6 About Ned Bellavance

Ned Bellavance is an IT professional with almost 20 years of experience. He has worked with Fortune 500 companies and SMBs across multiple verticals, developing and deploying both on-premises and cloud-based architectures. Ned has authored books on the Azure Kubernetes Service and on HashiCorp Terraform and holds several industry certifications from vendors, including Microsoft, VMware, AWS, and Citrix.

7. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

8. Copyright