Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **April 2023**
Commissioned by **OpenText Cybersecurity**

Comparing OpenText Enterprise Messaging, Microsoft Exchange Server, Microsoft 365, and Google Workspace

Executive Summary

This white paper compares four messaging systems designed for enterprise organizations:

- OpenText Enterprise Messaging
- Microsoft Exchange 2019 (on-premises)
- Exchange Online in Microsoft 365
- Google Workspace

KEY TAKEAWAYS

The key takeaways from this research are:

- **Migration of messaging systems is costly and disruptive**
  Migrating from one messaging system to another is a costly and disruptive process, regardless of the products involved. There are some valid reasons for migrating—such as poor technical performance by a vendor or lack of a future product roadmap—but irrespective of the logic and rationale, the costs are unavoidable.
- **Similar history and background, with Google Workspace the newest offering**
  OpenText Enterprise Messaging (including GroupWise) and Microsoft Exchange (on-premises and in Microsoft 365) share a similar legacy to the mid-1990s. Gmail in Google Workspace is the newest offering to market (mid-2000s).
- **Many similarities and several significant differences**
  The four messaging systems share similarities in approach to client and device support, delivery mechanism (although Google Workspace is exclusively a cloud-only service), secure messaging, and future product roadmap announcements. There are significant differences in the upgrade process (and associated costs), archiving and e-discovery, and data loss prevention.
- **Investment continuity for customers with GroupWise**
  With the reinvigorated and extended offering by OpenText of Enterprise Messaging, along with a future product roadmap, customers using GroupWise should evaluate the costs and benefits of continuing to invest in what they have.
- **OpenText's solution is less expensive to license than the other platforms**
  We calculated the three-year cost of licensing for an organization with 500 employees for each messaging platform discussed in this white paper. Based on publicly available information, the three-year cost for OpenText is less than for the other three platforms.

Migrating from one messaging system to another is a costly and disruptive process, regardless of the products involved.

ABOUT THIS WHITE PAPER

OpenText Cybersecurity commissioned this white paper. Information about the company and its relevant solutions is provided at the end of this paper.

To Migrate or Not

Migrating from one messaging system to another—irrespective of the two systems—is a process laden with significant costs, technical disruption, and potential productivity blunders. We can make several general comments that apply to virtually any messaging migration:

- **Messaging is more than just email**
  Email is a foundational communications service for organizations and extends its tentacles into many non-email aspects of an employee's workday, such as scheduling meetings and resources, tracking tasks, and forming a personal repository of conversations. Changing any messaging system can be very disruptive, no matter the benefits that a new system might offer.
- **There are good reasons for migrating to another messaging system**
  There are valid reasons for migrating away from a current messaging system. These include poor technical performance by a vendor (including multi-hour outages of cloud services), failure to deliver promised enhancements, key product capabilities no longer covered by support agreements, the formal cancellation of the product, the vendor going out of business, the vendor changing its investment priorities (and de-emphasizing its messaging offering), lack of a future product roadmap, and insufficient wider ecosystem support for your messaging platform of choice. Any of these reasons can form a valid case for migration (and the more reasons, the stronger the business case), but the customer organization still must go through the costly and disruptive process of undertaking the migration.
- **There are good reasons to avoid migrating to another messaging system**
  There are key reasons to avoid migrating to another vendor for messaging, including high-profile outages of their cloud offerings, the expectation of high future costs to stay up to date, and uncertainty around their product or service roadmap. When another vendor's messaging system is a primary target for cybersecurity threats, it is best to avoid it if possible. Regulatory restrictions due to data privacy concerns, among others, also signal the need for great caution when advocating a migration to another messaging system.
- **Lost productivity and downtime during migration is much higher than any potential licensing cost savings**
  Any migration is normally disruptive to employees who must learn a new email system and integrate it into their way of working. The cost of downtime and lost productivity often outweighs any licensing cost savings.

The cost of downtime and lost productivity often outweighs any licensing cost savings.

History and Background of Each Platform

OpenText Enterprise Messaging	Microsoft Exchange Server 2019	Exchange Online in Microsoft 365	Google Workspace
The evolution of Novell GroupWise, introduced in the mid-1990s based on technology that Novell acquired from WordPerfect.	Introduced in the mid-1990s. Latest version is Exchange 2019. Mature offering and Microsoft would prefer customers to move to the cloud.	Introduced in mid-2011 based on Exchange Server 2010. Now outstrips Exchange Server in capability. Microsoft 365 offers additional services.	Cloud-only collaboration platform with a range of capabilities. Introduced mid-2000s.

- **OpenText Enterprise Messaging**
  The overarching idea of Novell GroupWise was to deliver an integrated messaging and collaboration platform that offered customers choices in platform support and a wider technical ecosystem. Micro Focus built on this history with the introduction of Enterprise Messaging, demonstrating continuity of investment and support, and extending the value proposition of GroupWise with an integrated suite of compliance, management, chat-based workspace, and administration capabilities. A new standalone version of GroupWise outside of Enterprise Messaging is also available, which includes instant messaging and mobility capabilities. With Micro Focus now part of OpenText, OpenText is continuing the investment in Enterprise Messaging.
- **Microsoft Exchange 2019 (on-premises)**
  The big idea of Exchange Server was reliable enterprise-class email, and as Microsoft has rolled out new on-premises versions every few years since its introduction, this value proposition has been refined. Early forays into extending Exchange into new areas have spawned separate servers, such as Skype for Business Server (previously Lync Communications Server and Office Communications Server). Over the past decade, Microsoft has increasingly put its engineering effort into Microsoft 365, and while an on-premises deployment model is still supported, Microsoft would prefer its customers to migrate to Microsoft 365 (which includes Microsoft Teams, which is not available for on-premises deployment). Moving from one version of Exchange to the next has always been a complex and time-consuming undertaking. Many customers skipped on-premises versions of Exchange to avoid this cost and complexity. Microsoft has pushed hard on Microsoft 365 to prevent this version skipping.
- **Microsoft Exchange Online in Microsoft 365**
  Exchange Online was Microsoft's second attempt to counter the burgeoning success of Google's Gmail and other cloud-based services from the mid-2000s; it was originally a cloud-delivered version of Exchange Server 2010. From the early days of Microsoft 365, Microsoft has prioritized its engineering investments in Exchange Online, so that Exchange Online receives new capabilities in advance of Exchange Server. The wider Microsoft 365 offering delivers an all-encompassing set of productivity and collaboration cloud services.
- **Google Workspace**
  Google Workspace is the latest iteration of Google's email and collaboration service targeted at business and enterprise customers. The roots of Workspace date to 2004, when Google introduced a consumer email service called Gmail. Google subsequently introduced the Google Apps for Your Domain service, given the interest from the education and business markets in Gmail. Google runs the entire Workspace service using only a web browser, thereby doing away with the need for client software. Google Docs introduced the world to real-time browser-based multi-person collaboration.

From the early days of Microsoft 365, Microsoft has prioritized its engineering investments in Exchange Online, so that Exchange Online receives new capabilities in advance of Exchange Server.

What Each Platform Offers

OpenText Enterprise Messaging	Microsoft Exchange Server 2019	Exchange Online in Microsoft 365	Google Workspace
Offers email, instant messaging, file sharing, and mobility along with archiving, eDiscovery, litigation hold, backup and failover, and other capabilities.	Email server only, including archiving, litigation hold, eDiscovery, and data loss prevention. Integrates with other Microsoft servers and services for other capabilities.	Web-based email and archiving service, unless part of a wider Microsoft 365 plan that gives rights to the Outlook client (and other Microsoft 365 services such as SharePoint and Teams).	Offers Gmail, Calendar, office productivity tools, and meeting capabilities. The Enterprise plan includes archiving, unified search, and security and business controls.

- **OpenText Enterprise Messaging**
  Enterprise Messaging offers email, instant messaging, and mobility (GroupWise), file sharing, and a chat-based workspace (TeamWorks) for enterprise customers. It includes unified archiving and eDiscovery with litigation hold; anti-virus and anti-spam protection; backup and failover capabilities; and mailbox management, forensics, reporting and monitoring. Customers have choices in operating system, directory service, and email clients (while there is a native email client for Windows, a native Mac or Linux client is not available).
- **Microsoft Exchange 2019 (on-premises)**
  Email-only server. Customers must run Exchange on Windows Server, use Active Directory, and for full end-user capabilities the latest version of the Outlook client. The architecture for how email data is stored means that Exchange uses a lot more storage resources than other offerings on the market. This is expensive to manage, challenging to back up, and complicated to restore from. Customers often architect storage for Exchange based on how long it takes to back up an Exchange database.
- **Microsoft Exchange Online in Microsoft 365**
  Exchange Online Plan 1 offers web-based email services with a 50 GB mailbox including anti-malware, anti-spam, and basic archiving. Plan 2 offers a larger mailbox of 100 GB and adds litigation hold, hosted voicemail, a larger archive mailbox, and data loss prevention. Other capabilities are added as part of an Enterprise plan (or equivalent Government or Education plan), including desktop Office applications, document collaboration, and a chat-based workspace. Customers can mix and match plans for specific groups of workers in their organization. While Microsoft 365 offers a value-priced bundle of capabilities if the multitudinous products are used in a coherent way, many organizations use Microsoft 365 only for Exchange Online and the Office applications.
- **Google Workspace**
  Google Workspace offers cloud-based email, calendar, meeting, and office productivity services. The enterprise plans include data loss prevention, integration with third-party archiving tools, and email encryption. Google Workspace has no advertising, unlike Google's offerings for consumers.

In summary, there is a generally consistent approach across the four messaging systems, with the more expensive service offerings required to meet enterprise mandates.

Enterprise Messaging offers email, instant messaging, and mobility (GroupWise), file sharing, and a chat-based workspace (TeamWorks) for enterprise customers.

©2023 Osterman Research

Support for Clients and Devices

OpenText Enterprise Messaging	Microsoft Exchange Server 2019	Exchange Online in Microsoft 365	Google Workspace
Native Windows client and web-based client with responsive design to optimize user experience on all desktop and mobile device platforms. Support for native applications on Mac and Linux.	Native Windows and Mac clients, browser-based access on multiple platforms, and official mobile clients.	Native Windows and Mac clients, browser-based access on multiple platforms, and official mobile clients.	Browser-based and app-based access on multiple platforms to the various services in Workspace. Integration with native applications on Windows, Mac, and Linux.

The four products feature cross-platform support via web browser access, and directly provide native apps for selected platforms and devices:

- **OpenText Enterprise Messaging**
  Enterprise Messaging offers a native client for Windows and a web-based responsive design approach for desktop and mobile device platforms. Enterprise Messaging also supports native mail, calendaring, and contact applications on Mac, Linux, iOS, Android, and Windows Phone devices. OpenText does not offer its own native apps for Mac and Linux.
- **Microsoft Exchange 2019 (on-premises)**
  Microsoft offers the Outlook client on the Windows and Mac platforms, as well as mobile apps for iOS and Android tablets and smartphones. Mobile apps for Windows Mobile and Windows Phone are still available, although Microsoft no longer supports either of these mobile operating systems. Browser access to Exchange Server is available on multiple platforms.
- **Microsoft Exchange Online in Microsoft 365**
  Microsoft offers the Outlook client on the Windows and Mac platforms, as well as mobile apps for iOS and Android tablets and smartphones. Mobile apps for Windows Mobile and Windows Phone are still available, although Microsoft no longer supports either of these mobile operating systems. Browser access to Exchange Online is available on multiple platforms.
- **Google Workspace**
  Google's original design philosophy was to enable customers to avoid using installed applications on computers and devices, thereby simplifying initial deployment and ongoing administration. With the rise of tablets and smartphones, however, Google now offers and maintains apps for the various Workspace services across Android and iOS devices. All Google services can also be accessed using a modern browser, and Google provides details on how customers can connect Gmail to email clients such as Outlook. Finally, Google Chromebooks running ChromeOS can connect to Workspace, offering a lightweight device that gives full access to Workspace and other Google services without requiring any data to be stored locally.

The four products feature cross-platform support via web browser access, and directly provide native apps for selected platforms and devices.

Delivery Mechanisms

OpenText Enterprise Messaging	Microsoft Exchange Server 2019	Exchange Online in Microsoft 365	Google Workspace
On-premises server, private cloud service, or partner hosted service including hybrid.	On-premises server, with hybrid option with Exchange Online.	Cloud service, with hybrid option with Exchange 2019 on-premises.	Cloud service only; no on-premises or hybrid option.

- **OpenText Enterprise Messaging**
  Enterprise Messaging can be deployed as an on-premises server, in a private cloud, or as a hosted service via partners with hybrid options. Enterprise Messaging supports a range of operating systems and directory services.
- **Microsoft Exchange 2019 (on-premises)**
  Exchange 2019 is an on-premises email server that requires many other Microsoft components to work, including Windows Server, Active Directory, the .NET Framework, and 64-bit server-class hardware. Deploying Exchange requires a deep embrace of the Microsoft stack, which means organizations have to rip and replace functioning but non-supported IT elements to get Exchange working, e.g., Linux servers. Customers running Exchange 2019 have the option of linking with Exchange Online for complementary services, as there are no plans for on-premises equivalents of many of the newer capabilities in Exchange Online; customers are therefore largely forced to have a hybrid setup, adding cost and complexity. Exchange comes with significant ongoing maintenance and administration requirements, which requires retaining Exchange professionals with specialist knowledge or outsourcing Exchange management to a third party. Keeping Exchange working is beyond the skill level of general-purpose IT professionals.
- **Microsoft Exchange Online in Microsoft 365**
  Exchange Online is available exclusively as a cloud service, either as a component of a larger Microsoft 365 plan (e.g., Enterprise E3 or E5) or specifically through an Exchange Online plan. Under the shared responsibility model of cloud services, Microsoft takes on many management and administration tasks that were previously the responsibility of the customer, including a continual stream of upgrades. Embracing Exchange Online requires rethinking network topology, bandwidth, and network optimization due to email traffic flowing to the cloud and back, rather than within the enterprise network. Exchange Online has experienced multiple high-profile outages in recent months and years, due to problems with the service and Azure Active Directory; Microsoft historically has not been great at communicating during the outages. For customers with sensitive data that they don't want to put into the cloud, a hybrid environment with Exchange on-premises will be required, which duplicates costs. Exchange Online requires constant licensing to retain access—the pay-as-you-go model means that your organization owns nothing.
- **Google Workspace**
  Gmail in Workspace is a cloud-only email service that is generally adopted as part of a wider shift to Google's online office productivity capabilities instead of using Microsoft Office. While generally reliable, there have been some notable outages in the Google ecosystem. As with Exchange Online, the pay-as-you-go model requires constant licensing (with monthly and annual plans available) to avoid losing access to all emails, documents, files, and archived data.

Cloud services require constant licensing to retain access. The pay-as-you-go model means that your organization owns nothing.

Upgrading to New Versions

OpenText Enterprise Messaging	Microsoft Exchange Server 2019	Exchange Online in Microsoft 365	Google Workspace
In-place upgrades. Offers an easy way of installing the latest version at any time.	Complex, complicated, and expensive upgrade process. More "migration" than "upgrade".	Microsoft continually refines and upgrades Exchange Online and the wider Microsoft 365 experience.	Google continually refines and upgrades Google Workspace, including the Gmail service.

- **OpenText Enterprise Messaging**
  Enterprise Messaging can be upgraded in-place, and upgrades have generally been error-free. Service packs can be used to install the entire system, and customers can skip versions without problems. Customers are responsible for deploying upgrades or can engage business partners to assist.
- **Microsoft Exchange 2019 (on-premises)**
  Upgrading from one version of Exchange to the next has always been a complex, complicated, and expensive process for customers, one on which business partners have built significant IT services organizations. Microsoft only supports the current and second-to-latest versions of Exchange, with Cumulative Updates being released every three months. Cumulative Updates have been known to cause problems and instability.
- **Microsoft Exchange Online in Microsoft 365**
  Microsoft introduces changes to Exchange Online and Microsoft 365 on a continual basis—with more than 500 updates in progress across Microsoft 365 in March 2023. While administrators can decide whether to upgrade quickly or wait for the general release, they are eventually forced to comply with Microsoft's changed service definitions and revamp internally developed training and adoption resources. Microsoft treats Microsoft 365 as a learning sandbox and has changed direction mid-course on new features and administrative requirements. For example, when Office 365 Groups was introduced, it was initially positioned as a new user-focused service for team collaboration but morphed over time into a unified back-end plumbing service for group management. In addition, Microsoft has made several attempts to provide a unified and coherent compliance center with legal hold and eDiscovery capabilities, with new versions often incompatible with earlier approaches. Such changes of direction have frequently caused confusion, angst, and additional work for Microsoft 365 customers.
- **Google Workspace**
  Google is responsible for upgrading and refining its offerings, and has added new capabilities over time, including data loss protection (DLP), integration with third-party archiving products, and a hosted email encryption service. Google updates the look and feel of its services depending on which version of its design language is currently in vogue. In 2022, Google released more than 300 new features across all Google Workspace services, including more advanced appointment scheduling, email marketing, and new AI capabilities.

In 2022, Google released more than 300 new features across all Google Workspace services, including more advanced appointment scheduling, email marketing, and new AI capabilities.

Archiving and eDiscovery Capabilities

OpenText Enterprise Messaging	Microsoft Exchange Server 2019	Exchange Online in Microsoft 365	Google Workspace
Unified archiving solution for email, social media, instant messaging, and mobile communications. Includes eDiscovery tools and support for litigation hold.	In-Place Archiving for Exchange offers archiving only for Exchange content; requires a premium license for each user. In-Place eDiscovery available for Exchange Server and Exchange Online mailboxes.	Exchange Online Archiving is a premium service. Offers in-place archiving for Exchange Online and Exchange Server. Archiving and eDiscovery intended for Exchange and Microsoft 365 items only.	Google Vault offers archiving and eDiscovery for Google content only. Enterprise customers also have the option of using a third-party archiving solution.

- **OpenText Enterprise Messaging**
  Enterprise Messaging includes archiving for email. Retain Unified Archiving is a premium archiving solution which supports multiple email systems (e.g., Microsoft 365, Exchange, Gmail, GroupWise, Bloomberg, and IBM Notes), instant messaging apps (e.g., WhatsApp, WeChat, Telegram, Signal), and mobile communications (e.g., SMS/text messages, MMS, BlackBerry Messenger, and phone call logs). The unified archive is accessible by administrators and end users. Authorized individuals can undertake eDiscovery searches and place legal holds. Retain Unified Archiving can be deployed on-premises or as a cloud service from OpenText.
- **Microsoft Exchange 2019 (on-premises)**
  Microsoft offers in-place archiving where Exchange emails and other items can be archived to an additional mailbox that's associated with the user's primary Exchange mailbox. This is a premium offering and each user requires an Enterprise client access license. In-Place Archiving only supports Exchange Server and Skype for Business Server; it cannot be used to archive content from other messaging systems. In-Place eDiscovery can search a user's primary and archive mailboxes in Exchange Server and Exchange Online and put items on legal hold. Search results are not automatically kept up to date and additional steps may be required to locate messages protected by Information Rights Management. When a user account is deleted from Active Directory, Exchange will mark the user's Exchange mailbox for deletion, even if it is on legal hold. User accounts must instead be disabled and the mailbox specially protected.
- **Microsoft Exchange Online in Microsoft 365**
  Exchange Online Archiving, a premium service available separately or integrated into higher-priced Microsoft 365 plans, offers in-place archiving for Exchange Online and an alternative for Exchange Server (in a hybrid setup). This is only intended for Exchange items, not third-party content. eDiscovery is offered for Exchange only or for wider Microsoft 365 content. Auto-expanding archives in Exchange Online Archiving cannot be moved to Exchange Server on-premises.
- **Google Workspace**
  The Business Plus and Enterprise editions of Workspace include Google Vault, a cloud-only service providing domain-wide search for email and documents in Workspace, along with e-Discovery and legal hold capabilities. Customers wanting a unified archive that includes non-Workspace content must subscribe to the Enterprise plan, which integrates Workspace content with a third-party archiving service. Customers needing more than basic eDiscovery capabilities will need to use a third-party tool. Dynamic email, a capability turned on by default in Google Workspace, undermines the very definition of an email message and thus raises critical archiving and eDiscovery concerns since dynamic content can change each time a message is opened. Such changes are not subject to content compliance rules.

Retain Unified Archiving is a premium archiving solution for OpenText Enterprise Messaging which supports multiple email systems, social media services, and mobile communications.

Email Security and Encrypted Messaging

OpenText Enterprise Messaging	Microsoft Exchange Server 2019	Exchange Online in Microsoft 365	Google Workspace
Comprehensive messaging protection. Encrypted email available through Voltage SecureMail.	Exchange Server offers basic anti-malware capabilities. Customers can integrate Exchange with various Microsoft 365 services for protection against advanced threats at additional cost.	Exchange Online Protection for anti-spam, anti-virus, and anti-malware. Protection against advanced threats is via Defender for Office 365, which is included in some plans and available at extra cost for others.	All customers get basic email security controls. Enterprise plans unlock advanced controls and encrypted messaging options.

- **OpenText Enterprise Messaging**
  Enterprise Messaging offers anti-virus and anti-spam capabilities, email content filtering, and blocking of inappropriate images (e.g., pornography). It protects against denial-of-service and distributed denial-of-service attacks and blocks access to malicious websites and content. These capabilities are available to secure GroupWise, Exchange, Microsoft 365, Gmail, and other messaging systems. This solution is available for on-premises deployment and as a cloud service. For end-to-end email encryption, customers can subscribe to Voltage SecureMail by OpenText, a premium email encryption offering for on-premises, cloud, and hybrid deployments.

- **Microsoft Exchange 2019 (on-premises)**
  Various Transport Rules in Exchange Server offer protection against spam, viruses, and spyware, although these haven't changed much over the past decade. Microsoft says that its Exchange Online Protection (EOP) service in Microsoft 365 offers more features and easier management; EOP is available on subscription for organizations using Exchange Server. Defender for Office 365, previously Advanced Threat Protection, can protect Exchange Server against phishing, business email compromise, and advanced malware. Third-party security solutions are available too. Exchange Server uses various types of encryption to protect sensitive information. Information Rights Management (IRM) is the preferred approach for encrypting and protecting messages.

- **Microsoft Exchange Online in Microsoft 365**
  EOP, a component of Exchange Online, provides protection against spam, viruses and malware. For additional cost, Defender for Office 365 (previously Advanced Threat Protection) adds capabilities for click-time protections against malicious web links, safer attachment handling (including sandboxing unsafe attachments), and enhanced tracking and reporting. Both services are available only as a cloud service. EOP is also available to license separately for organizations using other email servers, including those using Exchange Server (as discussed above). Microsoft 365 Message Encryption provides automatic policy-based encryption of messages that meet pre-defined rules.

- **Google Workspace**
  All Workspace customers are protected from viruses, spam, malware, phishing, and other types of malicious attacks, and machine learning is being increasingly used to identify previously unseen message-borne threats. Google blocks file types that are often used for carrying security exploits, e.g., executable files. Customers on Enterprise plans gain access to advanced security controls, such as pre-delivery detonation of attachments to check for embedded malicious threats in a protected sandbox. Enterprise-plan subscribers also have the option of using S/MIME for encrypting outbound messages.

Exchange Online Protection, a component of Exchange Online, provides protection against spam, viruses, and malware.

Preventing Data Loss

OpenText Enterprise Messaging	Microsoft Exchange Server 2019	Exchange Online in Microsoft 365	Google Workspace
No native capabilities for DLP.	DLP capabilities using Exchange Transport Rules, defined in the Exchange Admin Center.	Microsoft 365 DLP policies support Exchange Online and other workloads. Exchange Online–specific DLP capabilities deprecated.	Content compliance available in Workspace Enterprise plans for Drive, Gmail, and Chat. Uses OCR for DLP scanning of images.

- **OpenText Enterprise Messaging**
  Enterprise Messaging does not offer DLP (data loss prevention or data leak prevention) for pre-delivery identification of messages that contravene policies. Enterprise Messaging offers post-delivery auditing and oversight for messages through OpenText GroupWise Forensics for after-the-fact identification of messages in violation of policies. DLP capabilities are available if customers subscribe to Voltage SecureMail by OpenText, a premium offering.

- **Microsoft Exchange 2019 (on-premises)**
  Exchange identifies sensitive information in messages and attachments using DLP policies that are enacted using Transport Rules. DLP policies use multiple content examination techniques to identify sensitive data in messages and attachments, e.g., keyword and text pattern matches, document fingerprinting (where Exchange creates a sensitive information type based on a standard company form that usually contains sensitive information), and dictionary matches. Each organization must create their own set of relevant DLP policies based on templates supplied by Microsoft, acquired from third parties, or created inhouse. Policy Tips warn users that the message they are writing may contain data that contravenes a DLP policy; these are displayed on supported email clients only. DLP is a premium offering and requires users to be licensed for the Enterprise CAL.

- **Microsoft Exchange Online in Microsoft 365**
  The Exchange Server heritage for DLP is used in Exchange Online—including transport rules, sensitive information types, and more. DLP for Exchange Online has until recently been managed via the Exchange Admin Center (EAC), but Microsoft is strongly pushing customers to use its new unified DLP policies in Microsoft Purview (previously the Security & Compliance Center) by deprecating DLP capabilities for Exchange Online in the EAC. New unified DLP policies in Microsoft 365 can be applied to Exchange Online only, or to multiple workloads including Teams, SharePoint, and OneDrive. DLP for Exchange Online is available in Exchange Online Plan 2 and the higher-priced Enterprise plans add DLP for other workloads.

- **Google Workspace**
  DLP for Gmail was added to the Business and Enterprise plans in 2015. It was subsequently limited to Enterprise accounts only from 2017. In Google Workspace Enterprise, DLP is available for Drive, Gmail, and Chat. Google's DLP service uses a library of general-purpose pre-defined content detectors and offers the option to use specific content detectors for various countries and vertical markets. OCR (optical character recognition) is used to identify sensitive data contained in images. The DLP service can quarantine inappropriate messages and documents, inform senders of the need to change the information, or block the message and notify the sender. Google uses intelligent approaches to identify offending content and documents that go beyond merely reading the file type. DLP rules can be established for individuals and teams. Google offers recommendations on DLP rules that are customized based on a data protection insight report created for each organization.

Enterprise Messaging offers post-delivery auditing and oversight for messages through OpenText GroupWise Forensics for after-the-fact identification of messages in violation of policies.

Regulatory Reaction and Concerns

OpenText Enterprise Messaging	Microsoft Exchange Server 2019	Exchange Online in Microsoft 365	Google Workspace
No issues when installed on-premises with all components under the control of the deploying organization.	No issues when installed on-premises with all components under the control of the deploying organization.	Banned in schools and some government agencies in Germany and France over data privacy concerns.	Banned in educational institutions in Denmark and France over data privacy concerns.

- **OpenText Enterprise Messaging**
  The regulatory concerns raised by European regulators for cloud services owned by American corporations with opaque data handling practices do not apply to OpenText Enterprise Messaging when installed on-premises with all components under the control of the deploying organization.
- **Microsoft Exchange 2019 (on-premises)**
  The regulatory concerns raised by European regulators for cloud services owned by American corporations with opaque data handling practices do not apply to Microsoft Exchange Server when installed on-premises with all components under the control of the deploying organization. On the other hand, due to the spate of vulnerabilities in Exchange Server being abused by nation-state and state-sponsored actors, it remains to be seen if Exchange Server is restricted for use by government agencies.
- **Microsoft Exchange Online in Microsoft 365**
  Data protection authorities in several European countries have banned the use of Microsoft 365 due to significant data privacy concerns. In Germany, Microsoft 365 is already banned in educational institutions, and other public sector organizations have been warned about its data privacy shortcomings. Based on a two-year investigation, German data protection authorities ruled that the lack of transparency from Microsoft regarding the processing of personal data for its own purposes puts Microsoft 365 out of compliance with the GDPR. In France, its Cloud at the Center initiative requires the use of secure, abuse-protected cloud solutions, a summary judgment that excludes Microsoft 365. Consequently, public officials in France are prohibited from using Microsoft 365 and educational institutions are banned from using the free or paid versions of Microsoft 365 and Google Workspace.
- **Google Workspace**
  The Danish data protection authority ruled that schools in the Helsingør municipality cannot use Google Workspace due to lack of compliance with the GDPR. The ruling applies in principle to other municipalities as well. Academics in France have been advised by the Ministry of Education to avoid Microsoft 365 and Google Workspace due to conflict with France's Cloud at the Center initiative. The ban includes both free and paid versions. How far the ban of Google Workspace spreads across the European Union remains to be seen. Aside from Google Workspace, several countries have also raised concerns about how Google handles data in other offerings, such as Google Analytics.

German data protection authorities ruled that Microsoft's lack of transparency regarding the processing of personal data for its own purposes puts Microsoft 365 out of compliance with the GDPR.

©2023 Osterman Research

Roadmap for the Future

OpenText Enterprise Messaging	Microsoft Exchange Server 2019	Exchange Online in Microsoft 365	Google Workspace
OpenText is working toward a well-integrated suite of offerings.	Unclear future for Exchange Server, as Microsoft would prefer customers to migrate to Exchange Online. Support will continue for the foreseeable future.	Exchange Online is strategic to Microsoft's future in the cloud, and it maintains a public list of current and near-term improvements.	Better integration across the various apps in Workspace. Google maintains a public list of current and near-term improvements.

The four vendors take a similar approach to roadmap announcements: near-term updates are publicly disclosed but longer-term directions are less clear:

- **OpenText Enterprise Messaging**
  OpenText continues to invest in the individual products in the Enterprise Messaging suite with a quarterly release cadence. For GroupWise, integration with Zoom for online meetings is due in Q2 2023 and with Microsoft Teams in Q4. The web interface is being updated continually, with functionality investments across the address book, calendar, overall usability, and scheduling. TLS 1.3 support is coming in the next release of the Secure Messaging Gateway, along with various SMTP command and authentication updates. Improving security is a major focus in Retain, as well as user interface updates and more integration points with Microsoft 365 workloads. Data sovereignty and security continue to be core design points across all products.
- **Microsoft Exchange 2019 (on-premises)**
  Microsoft and its partners have made a massive push to get organizations off Exchange Server. Microsoft prefers organizations to use Microsoft 365, where it is easier for Microsoft to maintain technical control, mitigate vulnerabilities, and earn more through subscription revenues. The widespread use of Exchange Server has made it highly attractive to cybercriminals and tens of thousands of organizations worldwide have been compromised in recent years. Microsoft had to divert engineering resources away from the promised Exchange Server 2021 to address vulnerabilities in earlier versions, ultimately condemning the version to never ship. The next version of Exchange is now promised for 2025, although full details will not be released until 2024. Microsoft will continue to prioritize features in Exchange Online and offer various ways for Exchange Server and Exchange Online to work together in a hybrid mode.
- **Microsoft Exchange Online in Microsoft 365**
  Microsoft 365 is a top strategic priority for Microsoft. Microsoft continues to improve, enhance, refine, and complement the experiences in Exchange Online and Microsoft 365. Microsoft maintains an extensive public roadmap for the overall service, with almost 600 updates in development or rolling out (as at March 2023). For Exchange Online specifically, updates under development cover email security, information barriers, and multi-geo administration. Earning more revenue from each customer is an important priority for Microsoft, which it achieves by adding new desirable features to higher-priced plans only, as well as by increasing the base price of current plans after adding new features.

Microsoft prefers organizations to use Microsoft 365, where it is easier for Microsoft to maintain technical control, mitigate vulnerabilities, and earn more through subscription revenues.

- **Google Workspace**
  Google is focused on delivering a more coherent and consistent experience across the various apps in Workspace, leveraging the best capabilities of each within the other apps. The interface of the key apps in Workspace has recently been updated. Google aims to provide core apps that align with the new realities of a hybrid workforce, and to add new apps that offer more intelligent ways of working. Google maintains a public roadmap of upcoming changes. Security is positioned as a big focus for Google Workspace.

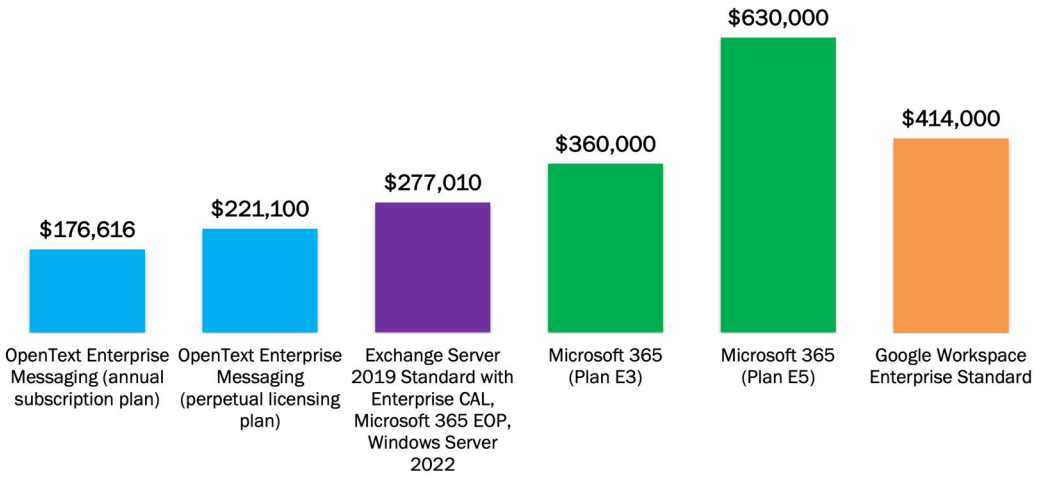
Cost Model

We calculated the three-year cost of licensing for an organization with 500 employees for each messaging platform discussed in this white paper. Pricing is based on publicly available information:

- **OpenText Enterprise Messaging**
  Priced in two different configurations: firstly, pricing per mailbox using the annual subscription plan, and secondly, pricing per mailbox with the perpetual licensing and annual maintenance plan. Includes allowance for an additional 10% of mailboxes for shared mailboxes.
- **Microsoft Exchange Server**
  Microsoft Exchange Server 2019 Standard, with the Enterprise CAL. Requires licensing for Windows Server, too. EOP in Microsoft 365 is employed as a supplemental security solution.
- **Exchange Online in Microsoft 365**
  Microsoft 365, showing pricing for the Enterprise E3 and E5 plans. Exchange Online is one component of E3 and E5.
- **Google Workspace**
  Google Workspace Enterprise Standard (300 is the maximum number of subscribers in an organization with the Google Workspace Business plans).

The three-year cost for the OpenText platform under both pricing configurations is less expensive than the other three platforms profiled in this paper. See Figure 1.

Figure 1
Three-Year Cost of Ownership in a 500-Seat Environment



Source: Osterman Research (2023)

About OpenText Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention to detection and response, to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber-resilience via a holistic security portfolio. Powered by actionable insights from our real-time contextual threat intelligence, OpenText Cybersecurity customers benefit from high-efficacy products, a compliant experience, and simplified security to help manage business risk.

Visit opentext.com.

opentext™ | Cybersecurity

www.opentext.com

@OpenText

+1 800 499 6544

© 2023 Osterman Research. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, nor may it be resold or distributed by any entity other than Osterman Research, without prior written authorization of Osterman Research.

Osterman Research does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

248-000079-001