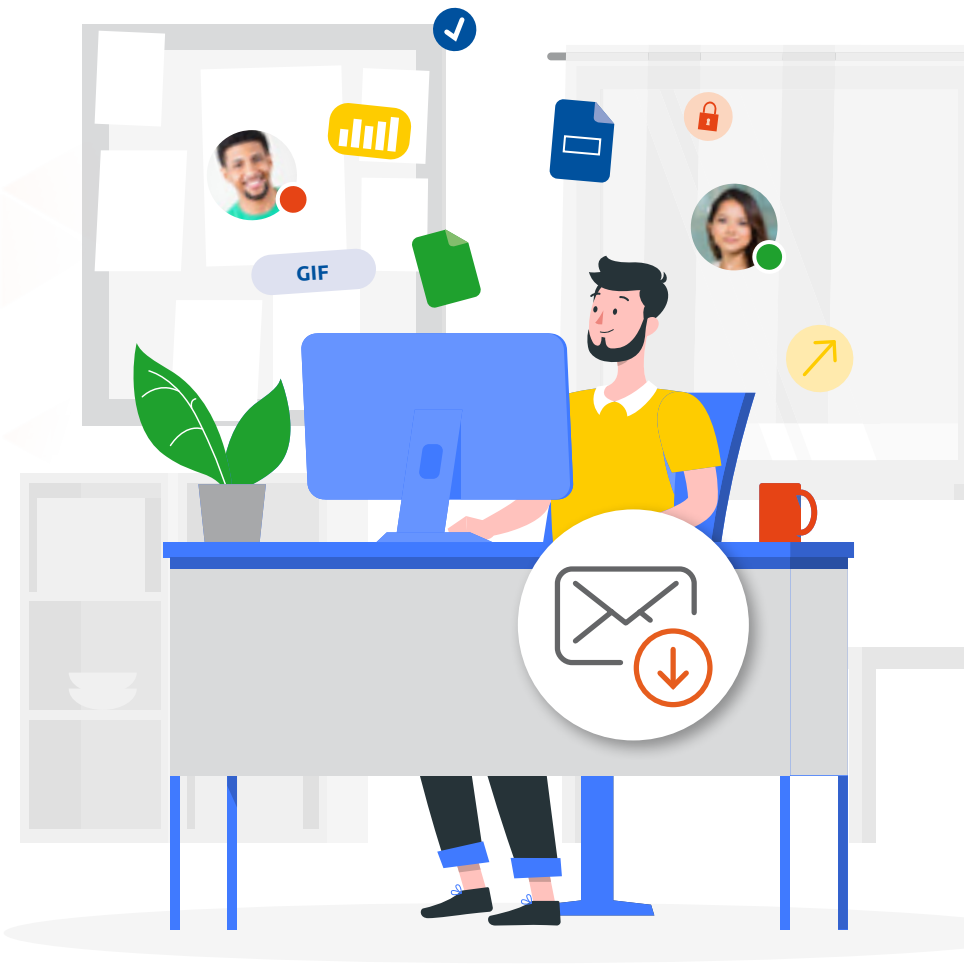


The Benefits of an Independent Email Archiving Solution for Users of Google Workspace

The Experts in Email Archiving
www.mailstore.com

Introduction

Professional information management that satisfies all legal and regulatory requirements is a key corporate task in the digital age, and this holds especially true for email management. Emails can contain a huge amount of business-critical information, all of which needs to be backed up with the aid of reliable archiving and backup solutions that allow companies to meet the legal requirements and have round-the-clock access to relevant business data, while enjoying effective protection against data loss.

Cloud-based, integrated communication environments are becoming increasingly popular in terms of digital collaboration. Alongside Microsoft 365, one of the best-known products is Google Workspace, which was previously known as G-Suite and has been available to Google customers since October 2020. The software suite comprises a variety of Google programs (such as Gmail, Google Drive and Hangouts) and with Google Vault an information management tool that allows emails to be archived. Companies using Google Workspace should, therefore, take a close look at Google Vault to understand the features and benefits of the archiving function, as well as its limitations and vulnerabilities.

This white paper provides detailed information on the subject of email archiving and examines

- why email archiving should be an important element in your IT strategy,
- the strengths and weaknesses of Google Vault,
- why a third-party solution can be the best fit when it comes to archiving emails, and
- the requirements an archiving solution has to meet.

Contents

Key Findings

- Particularly in the USA, Google Workspace is the preferred solution for an increasing number of small and medium-sized businesses (SMBs), and organizations from the education sector. Reasons include the large number of digital communication and collaboration functions, together with Google's reputation as a reliable provider.
- The all-inclusive solutions offered by major cloud providers can simplify the work carried out in IT departments and are a particularly attractive option for anyone wishing to work from home. IT decision-makers are nonetheless duty bound to handle critical business data with due sensitivity and diligence.
- Organizations depend on reliable backup and archiving capabilities as the safest way to protect, preserve and keep critical data (much of which is stored in email systems) constantly available. Failure to adequately protect data can have serious consequences, including legal issues in the form of penalties for non-compliance with current rules and regulations, not to mention the risk of data loss and a fall in productivity.
- Every business needs a reliable email archiving solution in order to preserve business records stored within emails and, depending on the solution, to allow an employee to retrieve information from the email archive quickly and efficiently with the help of appropriate search functions.
- Platform-integrated archiving solutions such as Google Vault as part of the Google Workspace communications environment have vulnerabilities in terms of certain email archiving requirements. These issues can be avoided by using an independent solution.

Why Archive Emails at All?

Although professional communication based on tools like Slack and Google Hangouts has increased significantly, email remains the preferred medium for transferring business data and information. A company's email stock will therefore contain a large number of critical documents, for example:

- Contracts
- Personnel data
- Orders
- Shipping records
- Customer agreements
- Replies to technical support queries

Failure to store emails and their file attachments properly can have undesirable consequences for a company. For example, depending on country and sector, processing emails and storing this data over time so that it remains permanently available can be subject to different legal and regulatory requirements. This applies particularly to heavily regulated sectors of industry, such as healthcare, the financial industry, governmental and educational industries in which sensitive personal data is frequently sent and received by email.

Email archiving can be a great help when it comes to observing requirements like these, which are usually laid down by a company's management and then implemented by the local IT team. A breach of archiving duties can result in fines and other sanctions and, in certain circumstances, even litigation under civil law.

At the same time, email archiving can make it easier to deploy emails as evidence in legal proceedings. In the event of litigation where emails are being used as evidence or where data subjects are asserting their rights under the EU's General Data Protection Regulation (GDPR), a company employee or external auditor must be in a position to search for and retrieve data from all its email volumes efficiently at all times.

In the USA, emails have long been used as evidence in court, often giving rise to complex eDiscovery processes in which an organization's entire email stock is trawled for specific information. And in European jurisdiction too, the EU eIDAS regulation has now reinforced the probative value of electronic documents. Therefore, a company should be capable of executing a search through its entire email stock in the case of an eDiscovery scenario and have the data exported in standard format, where necessary.

In light of increasingly severe privacy legislation (e.g. the EU's GDPR, CCPA in California, HIPAA, and FERPA in the USA) and compliance regulations, together with the enduring popularity of electronic correspondence, every company has a responsibility to address the subject of email archiving proactively. The option of archiving relevant emails professionally as the cornerstone of a comprehensive email management concept should be a part of every IT strategy. In this way, it can be ensured that all emails, including their file attachments, are preserved in a complete and tamper-proof manner while providing long-term availability.

Email Governance and Archiving

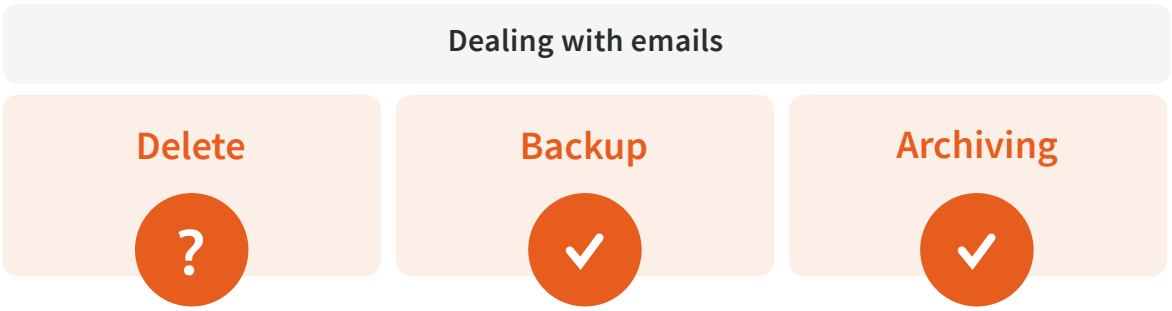
In certain circumstances, an IT department may be unable to implement directives issued by management as part of a corporate email governance strategy without an archiving solution. Such directives could include retention policies for specific emails, centralized backing up of emails stored on local systems (e.g. local PST files, emails that exist solely on email clients), and the ability to restore historic emails.

How Does Email Archiving Work?

The primary objective of any email archiving solution is to make sure that email data remains available and retrievable over a long period of time. To do this, the archiving solution stores copies of all emails in a central archive, thus ensuring the availability and security of data over many years.

The email archive supplements an existing email system (which can, of course, continue to be used as before). The administrator configures which emails are to be transferred to the archive and when, and whether the emails, once archived, should be deleted from the mailboxes on the email server. Ideally, the archive will be able to manage very large volumes of data efficiently.

Email Archiving vs. Backups



Email archiving and email backups are by no means one and the same thing. In the context of business continuity (BC), these are both valuable tools that complement rather than replace one another.

Email backups protect data (ideally, the email archive itself) mainly in the short to medium term (usually 30-90 days), so that the data can be restored when needed. Backups mean that business-critical systems and data can be accessed even in an emergency (e.g., in the event of system failure or a ransomware attack). Backups consist of non-indexed data captured at a specific point in time (snapshot).

Email archives enable emails to be stored for years in a form that is faithful to the original, easy to find, and permanently available. They are the basis of a professional information management strategy that takes all relevant legal and regulatory requirements into account.

Objectives	Email backups	Email archiving
Eliminate mailbox quotas	○	●
Eliminate PST files	◑	●
Reduce storage requirements through de-duplication and compression	◕	●
Reduce the workload of email servers and simplify backup and restore processes	○	●
Provide complete, tamper-proof and long-term email retention	◑	●
Helps to meet compliance requirements	◑	●
Assistance with eDiscovery scenarios	◕	●
Full-text indexing of emails for fast searches	◑	●
End users: restore lost emails quickly and easily	◑	●

● Fully applies ◕ Applies ◑ Partially applies
◔ Applies to a lesser extent ○ Doesn't apply

The ratings in this table are based on the fundamental concepts of backups and email archiving. The functions of an email archiving solution discussed here are based on the range of functions provided by MailStore Server. The functions of backup and email archiving solutions may vary, depending on the provider.

Email Archiving With Google Vault

Google Vault is a Google Workspace tool used for information management and eDiscovery purposes.[1] Companies can use Google Vault to store large amounts of data for any length of time, including not only emails, but also files from other Workspace services such as:

- Google Drive
- Google Chat
- Google Groups
- Google Voice
- Google Meet
- Google Hangouts

With Google Vault, data generated within a Workspace can be clustered by subject, arranged into hierarchies, visualized, and exported. Authorized administrators can search the stored data by user account, organizational unit, date, or according to certain keywords. Also, authorized users can use the tool to view history logs, create access rights and manage user accounts. This can be helpful in the event of investigations, audits, and litigation. It is also possible to assign what are known as “holds” to individual matters. In this case, the data in question are retained until the company removes the hold. A hold always takes precedence over any retention rules, which only apply once the hold has been deleted.[2]

As regards the archiving of emails, Google Vault’s great strength is its full integration in Gmail. That being said, the solution can archive data only once retention rules have been set up.[3] Google Vault users with the authority to create retention rules must state proactively:

- who is allowed to access Vault and perform what kind of actions,
- how long data should be stored,
- which users/groups are affected by which rule, and
- at what time data that is no longer needed should be deleted from user accounts and Google systems.

Google accepts no responsibility for either protecting or retaining customer data. Unless and until an organization has defined retention rules in Google Vault, it is possible for files to be deleted irrevocably by users (or according to the protocol of the relevant Workspace service). After the retention rules defined by the administrator expire, the data is subject to the standard procedure Google uses to delete customer data.[4]

Who Can Use Google Vault?

Google Vault can only manage the data of users with a valid Vault license. This is included in the "Business Plus" and "Essentials" Workspace packages, as well as in the various "Enterprise" and "Education" versions for every employee in the company. Organizations running the more affordable "Frontline", "Business Starter", and "Business Standard" versions, on the other hand, will need to buy extra monthly Vault licenses for every employee whose emails are to be archived.[5] Alternatively, email archiving can be performed using an external third-party solution.

Google Vault licenses included

- Business Plus
- Enterprise Editions
- Education Editions
- Essentials

Google Vault licenses not included

- Frontline
- Business Starter
- Business Standard

[1] What is Google Vault? - Google Vault Help
[2] Get started with holds in Google Vault – Google Vault Help
[3] Set up Vault for your organization – Google Vault Help
[4] How retention works – Google Vault Help
[5] Google Workspace editions – Google Workspace Admin Help

What Are the Limitations of Google Vault?

Google Vault can store emails and file attachments in a tamper-proof manner over long periods of time. According to Google, once you consent to Google's addendum on data processing and to the standard contractual clauses for Google Workspace and Cloud Identity, you will meet the adequacy and security requirements defined under the EU's GDPR. Likewise, by accepting Google's amendment agreement for business partners, you will be compliant with the HIPAA in US geographic locations.[6]

However, to assess the degree to which Google Vault satisfies specific demands in terms of retention and usability, it is important to be mindful of the weaknesses and vulnerabilities of the solution.

Lack of flexibility: Google Vault can archive emails from Google Workspace only. If your emails are located in other cloud services, on-premise email servers, or on local PCs, Vault will only be able to archive the data once they have been migrated to Workspace.[7]

Data residency: Only users of the "Enterprise" or "Education" Workspace packages can define a geographic storage location for their data. Here, users can choose between the USA or Europe, but administrators cannot select a specific country within Europe. It is also not clear who actually has access to the data.[8]

Only one email address per user: Google Vault does not support archiving of multiple mailboxes of a single user, i.e., different email addresses belonging to an individual. The Google Vault license always covers just a single user mailbox.

Limited export formats: Exported emails are saved in either the MBOX or the PST format only. In the event of audits or litigation, the exported files may well need to be converted to different file formats, and an appropriate tool would be required for this purpose.[9]

[6] Compliance amendments for Google Workspace and Cloud Identity – Google Workspace Admin Help
[7] Migrating emails using SMTP resets timestamps – Google Vault Help
[8] Choose a geographic location for your data – Google Workspace Admin Help
[9] Review Vault export files – Google Vault Help

Impractical restore process: Since Google Vault does not allow exported files to be imported directly, an external solution is required to restore exported emails to Google Vault.[10]

Loss of data if users or licenses are deleted: If an employee's account or Vault license is deleted, their data will be irrevocably removed from the archive after 20 days, at the latest.[11] This applies even to data set to "Hold", i.e., data stored "permanently" by Vault. To prevent this from happening, an Archived User (AU) license has to be purchased as an add-on for every employee whose account or Vault license is to be deleted (when they leave the company, for example).[12]

Platform-dependency: The email client and the archive created by Vault use the same platform. If the platform is unavailable for technical reasons, not only will the email client be unusable, but access to the archive will no longer be possible either. In the worst case, data could even be irretrievably lost if emails are deleted due to a technical glitch or because Google Workspace is unavailable.

Cloud only: Google Vault stores archived data in a cloud environment. An on-premise solution is not available.

No self-service for users: Google Vault is a tool intended for administrators and auditors; as such, end users cannot access the stored data. This means that instead of accessing archived emails by themselves, most employees will need to contact their IT department or a competent administrator each time they need to run a search query.

Non-compliance: Due to the limited functionality of Google Vault, companies run the risk of not being able to comply sufficiently with current rules and regulations.[13] Especially in sectors such as finance, healthcare, law, or education, the regulations can be strict, and this merely augments the risk of fines or other sanctions. Indeed, Rule 34 of the Federal Rules of Civil Procedure (FRCP) of the United States of America on their own require companies to retain all information stored in electronic form (ESI), and this includes any information and files contained in emails. In the event of litigation, potential evidence must be accessible quickly and simply.

[10] Google Vault FAQ – Google Vault Help (Restore)
[11] Google Vault FAQ – Google Vault Help (Delete User)
[12] Preserve data for users who leave your organization – Google Vault Help
[13] Google Vault FAQ – Google Vault Help (Backup & Archiving)

Special page: GDPR and Privacy Shield

The EU's Data Protection Regulation (GDPR) governs the processing and storage of personal data. However, as the name suggests, this regulation is applicable not only within the European Union: companies based outside the EU that need to store and process the personal data of EU citizens are also subject to the GDPR's provisions.

In the past, data transfer from the EU to the USA was regulated by a privacy agreement known as the EU-US Privacy Shield. However, following enduring criticism of the Privacy Shield by data privacy activists concerned that U.S. privacy laws failed to match the high level of protection available in the European Union and did not comply with the EU GDPR, a paradigm shift occurred in July 2020.

The European Court of Justice (ECJ) declared the Privacy Shield invalid – as indeed it had the prior Safe Harbor Privacy Principles in October 2015. As a result, companies wishing to store and process the data of EU citizens in the U.S. can no longer rely on Privacy Shield but must find other legally compliant ways. As things currently stand, companies are predominantly using standard contractual clauses, but this is not a permanent solution as the ECJ is obliging EU data protection authorities to check the relevant data transfers and block them, if necessary. Google repeatedly emphasizes that Workspace is GDPR-compliant. However, compliance cannot be guaranteed for data transfers to the USA based on standard contractual clauses, if only because of the Foreign Intelligence Surveillance Act, which permits public authorities to access personal data.

A similar degree of uncertainty vis-à-vis the GDPR is engendered by the Cloud Act (Clarifying Lawful Overseas Use of Data Act). Since March 2018, this US law has required US cloud providers to grant US authorities access to stored data. This also applies if the data are stored outside the USA, for example if a US company is operating a server on European territory.

Binding Corporate Rules (BCRs) can be adopted as an alternative to standard contractual clauses. As these can be quite a problem to implement, however, they are not generally considered viable for small companies.

Since a revision of the Privacy Shield or creation of a completely new legal basis is unlikely in the near future, companies that transfer data from the EU to the USA are currently exposed to a not inconsiderable risk, therefore.

The Benefits of an Independent Archiving Solution

As explained in the previous chapter, Google Vault's inherent weaknesses mean that it is unable to fully satisfy the fundamental requirements of a professional information and email management system. Users of Google Workspace should, therefore, consider procuring an independent archiving solution to avoid problems and reap the potential benefits, which are outlined in the following.

Protection against data loss: Whether by accident, ignorance, or malicious intent: when employees delete emails, a multitude of problems can arise. Scenarios in which a user deletes the entire contents of a mailbox on leaving the company are particularly serious. Around the globe, critical data is lost in this way every day. With the aid of an email archiving solution, all existing and future inbound and outbound email traffic can be fully archived and protected against manipulation, with data loss effectively ruled out.

Reduction in IT cost and effort: Email archiving can help cut the cost of managing emails including the associated IT effort involved (e.g. users submitting specific requests to have emails restored from backups or email servers). Storage requirements and thus mailbox sizes can often be reduced significantly by swapping out content from the mail servers.

Increase in productivity in everyday business: If your company can access its entire email stocks quickly and comprehensively, this can often help to augment staff productivity. It also makes sense to have self-service functionality built into the archiving solution so that users can access the archive, locate emails via full-text search, and restore messages by themselves.

Fast ROI: Using an archiving solution for your emails cuts the workload on your IT department and can help reduce the cost of storage. As a rule, the initial cost of an email archiving solution pays for itself relatively quickly. And a pleasant side-effect is that companies can protect themselves against the financial risk of data loss or legal breaches. Especially for users of the more affordable Google Workspace packages that do not come with Google Vault, an external solution can work out cheaper than buying Vault licenses and additional Archived User Licenses.

Increased autonomy: Rather than storing emails on-premises (i.e., under the direct control of the corporate IT department), many companies opt to use the external servers of a public cloud provider. This requires a degree of confidence in the availability of these services. Archiving your data within a third party email archiving solution is an effective additional safeguard.

Check List: How to Choose the Right Email Archiving Solution

When choosing email archiving software, all legal, economic, and technical requirements should be taken into account in addition to corporate interests. Preparing a list of requirements can make it easier to find an appropriate solution:

- [ ] **Flexible storage management:** Choosing archiving software that uses methods such as de-duplication and compression can help reduce storage requirements. Flexible storage management also means that fast, expensive storage can be reserved for current emails, while older, less frequently accessed emails are stored on cheaper storage.
- [ ] **Easy to install and run:** Simple installation makes it easier to get the software up and running, while intuitive handling facilitates rapid implementation of the archiving system. Having all the necessary components, e.g. database systems, integrated during setup helps save time, while reducing costs and administrative effort.
- [ ] **Archive all existing emails:** The new software should enable existing emails stored in individual mailboxes, public folders, shared mailboxes, and files to be archived simply and efficiently. What is more, a journaling feature must allow all emails to be archived the moment they are sent or received so that they are protected from manipulation.
- [ ] **User-friendly:** Users must be able to access archived emails as usual via Microsoft Outlook, browser, or while on the road with a tablet or smartphone.
- [ ] **Self-service for the user:** Not all archiving solutions allow staff to access email volumes by themselves. But the workload on an IT department can be reduced significantly if the new solution allows users to work productively within their own archive.
- [ ] **Certification:** The archiving solution should support compliance with all the legal requirements. It can be important, for example, that the software permits GDPR-compliant working standards with the corresponding certification, where required.
- [ ] **Flexibility:** The archiving software should support all conventional email systems and archiving methods. Ideally, it should also be possible to realize customized application scenarios via an integrated API.
- [ ] **Fit for purpose:** Your archiving tool must be a good fit for the size and requirements of the business. For example, it is rarely the case that an SMB will need a large enterprise solution, rather software that is tailored to the small or mid-sized company in terms of functional scope and total cost of ownership (TCO).

Run a Detailed Cost Analysis!

Google Vault is available to Workspace users only as part of the more expensive "Business Plus" and "Essentials" packages and in the various "Enterprise" and "Education" versions. Small and mid-sized businesses for whom the less expensive "Frontline", "Business Starter", and "Business Standard" versions are adequate in terms of scale and features would be well-advised to check whether an independent archiving solution might be a more sensible and viable archiving option than buying extra Google Vault licenses and Archived User Licenses (AU).

Summary

Email archiving is one of the most important elements of a professional information management system and should be an integral part of your IT strategy. When selecting a solution to assist with this important task, always consider the individual strengths and weaknesses. Your data should be stored securely and be available for you to retrieve over a long period of time.

Google Vault provides Google Workspace users with a data management tool that, in many scenarios, fails to satisfy all the requirements for professional email archiving that helps to fulfil regulatory compliance.

About MailStore

MailStore specializes in the development of innovative email archiving solutions for small and mid-sized businesses. With tens of thousands of corporate customers in more than 100 countries, MailStore is a global leader in its field. MailStore products and solutions are used by small and medium-sized businesses from all sectors, as well as by public and educational institutions.

MailStore's ambition is to apply the best available technologies to support their customers in making efficient and sustainable use of email as one of the most valuable and comprehensive information resources of our time and to help them to meet a growing number of compliance requirements.

MailStore Software GmbH
Cloerather Str. 1-3
41748 Viersen, Germany
www.mailstore.com

Graphic title page: Designed by slidesgo / Freepik, https://www.pexels.com