6 Questions To Ask Vendors Before Choosing Their Archive Migration Or Email Archiving Solution

OVERVIEW

Today, legacy email archiving software, such as Veritas Enterprise Vault, Dell EMC SourceOne, Mimecast, OpenText AXS-One Archive, and GWAVA Retain, haven't kept pace with the times, exposing their customers to data breach and ransomware risks, and forcing them to create risky workarounds to search and access the data. In the case of SourceOne, support is being dropped altogether. Additionally, isolating data from other data subject to retention requirements hinders data insights and creates obstacles to effectively managing legal holds and eDiscovery or leveraging the data for AI applications. As a result, organizations like yours are increasingly looking for more modern alternatives. Your corporate digital transformation initiatives, the adoption of cloud-based technologies, retirement of technical debt and AI-driven initiatives make cloud-based email and digital communications archiving a much more attractive prospect.

Migrating from an on-premises email archive to the cloud (or from a legacy archiving application in the cloud) should provide a way to not only securely manage your inactive and sensitive data but also support your digital communications governance needs going forward.

This guide outlines key questions you should ask any archive migration or email archiving vendor before you select a solution.

Question 1

Have you migrated data from our type of email archive before?

What assurances can you give me that everything is migrated successfully? Will the migration be seamless to end users?

Whether you're migrating data from an on-premises archive like Enterprise Vault or SourceOne, a SaaS solution like Mimecast, Smarsh, ZL, or Global Relay, you should mitigate migration risks by ensuring the vendor has extensive experience successfully migrating data from your type of email archive. When planning an email archive migration, keep in mind the importance of preserving data authenticity should the data ever be subject to an investigation and the migration's impact on end users. It's crucial to verify that the migration of your current archived data can be completed without damaging the chain of custody or impacting your day-to-day operations.

Question 2

Can you archive other types of data besides email at a scale that meets our needs?

In addition to email, will your organization need to archive data from other applications? For instance, collaboration data from applications such as Microsoft Teams or Splunk? Or SMS data, audio and video? What about structured data from legacy applications?

As you think about data archiving going forward, you should plan for the different data types your organization will need to retain as well as how you'll need to access them. In the future, email may only account for a small percentage of the data that your team will need to archive, manage and make available for search or business intelligence. Ensure the vendor can demonstrate how they will be able to cost-effectively scale, in terms of data types *and* data volume, to support your ongoing and future workloads.

ARCHIVE360

Question 3

Can you migrate our journal data?

Are your currently archiving journal data for regulatory compliance? Will you need to journal data in the future?

Depending on why you're looking to migrate your email archive and your archiving needs in the future, you will need to plan for what to do with your legacy journal, as well as where and how you will compliantly archive journal data in the future.

Do you know how much archived data you have? Does that include data for inactive and departed users?

Prior to implementing a new email archiving policy (including archiving directly within Microsoft 365), organizations should review what data they have and decide where and how they want to manage it going forward. If there is a need to archive journal data, you will need to be sure the 3rd party vendor can do so compliantly, cost-effectively, and in a manner where you retain control of your data (e.g. - meet data sovereignty requirements, ensure data authenticity, charge excessive fees to migrate data away from their platform, etc.).

ARCHIVE360

Question 4

How will my data be stored and processed?

In the future, do you want your archive hosted on-premises, online through a traditional SaaS solution, or in your own cloud tenant?

How you answer these questions can impact the level of control your organization has over its data. Not all cloud-based archives offer the same level of control. Traditional and multi-tenant SaaS solutions often come with restrictions - such as data portability, storage and data processing limits, and infrastructure and application security protocol ownership.

With Archive360's single-tenant, dedicated SaaS solution you have complete control over your data – where it is stored, how it is processed, and who can access it.

ARCHIVE360

Question 5

How much control will we have over data security and data sovereignty?

Thinking about your new email archiving solution, will your security policies and processes be set by your security teams or by the archive vendor you choose? And who has the rights to create, store, and access your data's encryption keys? Will you be able to dictate where data is stored, processed and managed to support your data sovereignty obligations?

The best email archiving software integrates with your existing security infrastructure and posture, in keeping with your existing policies and protocols allowing you to manage your own encryption keys. And allows you to control where (in which country) and how (immutability) data is stored and processed and who has access to it.

ARCHIVE360

Question 6

What can I do with the archived data?

Will your legal and eDiscovery teams be able to review the archived data in full context (including GIFs, emojis, etc)? Will your analytics team be able to mine the data for insights? Or can your compliance team uniformly and consistently govern data across enterprise systems? Will the data be secured and ready for AI modeling?

The ability to access your emails and files in their original format with comprehensive metadata is crucial if you want to carry out analysis and use the latest cloud-based tools to harness AI (Artificial Intelligence) and ML (Machine Learning). This is also critical for your in-house or external counsel or Records Management teams, depending on what industry you're in and how often historical records need to be accessed.

Why Leading Organizations Choose Archive360 for Email and Digital Communications Archiving

- Eliminate legacy email archive costs
- Account for all data with a complete chain of custody
- Mitigate data security & privacy risks
- Classification and policy-based data retention, legal hold, and entitlements
- Seamlessly accelerate data migration
- Facilitate data discovery (one search across data from multiple systems)
- Centralize communications and data governance
- Unmatched options for protecting your data
- Manage all types of data at scale across organization system
- Seasoned data migration and archiving expertise

ARCHIVE360

Archive360 is the unified data governance company transforming how organizations identify, collect, manage, and act on their data. Businesses and government agencies worldwide rely on the security, scalability, and scope of our cloud-native platform to address their increasing data governance obligations across growing volumes of disparate data. With Archive360, our customers are eliminating data silos, securing data access, increasing data insights, while reducing cost and risk. Archive360 is a global organization that delivers its solutions both directly and through a worldwide network of partners.

Archive360 is a Microsoft Cloud Solution Provider, and the Archive2Azure™ solution is Microsoft Azure Certified.

To learn more, please visit **www.archive360.com**