Legacy Archive Migration Best Practices for a Smooth Transition

For decades, organizations have been archiving emails to meet regulatory and business requirements. In many cases, this means that companies have millions of emails stored in outdated systems. Updating archives to take advantage of the benefits of a modern environment can prove complicated. But following legacy archive migration best practices help.

Email archiving provides a way for companies to preserve emails indefinitely. Archiving often proves necessary to achieve regulatory compliance. It also provides for business continuity and plays a key role in eDiscovery and internal audits.

Several scenarios may necessitate the need to migrate email archives. For example, as more workloads move to the cloud, vendors begin to sunset legacy systems. Also, modern archive solutions offer a host of features that many legacy systems cannot provide.

Understanding the Legacy Archive Migration Process

The migration process involves extracting archived emails from legacy archives and ingesting them into the new system. While the process sounds straightforward, it can prove quite complicated. A thorough system review will help the archiving team determine the best plan of attack.

Stakeholders with an understanding of the business and regulatory requirements at play should examine the data stored to assess the amount, types, and age of the archived data. Factors such as the number of emails, the type and size of attachments and the amount of duplicate emails will determine the time and cost involved.

With an understanding of the data, the team then chooses the best migration option and outlines a strategy. A clear picture of the goals for the migration will inform the choice of a migration option.

For instance, lifting and shifting the entire archive from a legacy archive system to a cloud archive will ensure compliance. But it may not prove practical. Alternatively, the team could consolidate data from the legacy archive into an XML repository. This also ensures compliance and supports eDiscovery, but it makes accessing archived data from active mailboxes difficult.

Most likely, the optimal solution will combine a partial XML repository with a cloud archive. This provides regulatory compliance while keeping archived emails accessible from regular email.

Getting Locked into a Proprietary Solution

Many of the existing on-premise archive solutions have engineered options for storing data in the cloud. They can assist you in moving your on-premise data to their cloud solution. Fortunately, the majority of local on-premise solutions from the major vendors have published API's. These programs allow third party vendors to interface with the data and to extract and move that data to other locations.

However, the same platforms that were relatively OPEN while in your datacenter can prove to be difficult if not impossible to access from the cloud with third party tools. That means moving away from these vendors may require the expense of having the vendor you are leaving provide those services. Even worse, they may require the process of painstakingly exporting data from their cloud solution in restricted small increments.

Thus, before deciding where to place your archive data, you should understand the risks and potential costs associated with data storage and management. You don't want to get locked into a proprietary cloud solution.

Migration Obstacles to Overcome

Like any data migration, a legacy email archive migration brings challenges, including some hurdles unique to email archives. First, an archive that has been in use for years, even decades, contains massive amounts of data. Moving millions of emails without incurring any data loss can prove time consuming and feel daunting. But preventing data loss is critical for compliance.

Second, to achieve compliance and provide legally defensible data for eDiscovery, organizations need to demonstrate a clear chain of custody. This involves providing irrefutable evidence that the archived data has not been altered.

Finally, the migration process must take stubbing into account. When an email is archived, it can leave behind a pointer, or "stub," in the live email system. While stubs save space and allow for quick retrieval of archived data, they can complicate migrations. Without the right tools, the migration process will break the link between the archive and live mail.

Legacy Archive Migration Best Practices

By following best practices, organizations can overcome migration hurdles and achieve a successful, even painless, migration. Start by gathering stakeholders to identify potential pain points and carefully outline a migration strategy. Also review and update (or create) email retention policies.

Additionally, take time to review any applicable industry or legal requirements. The regulatory environment has evolved rapidly in recent years, and each year brings a host of new requirements. This may affect your archiving strategy and decisions about what to move.

Finally, choose your new email archive solution carefully. For instance, look for the following:

- Tamper-proof archives with a defensible chain of custody – To demonstrate compliance, the archiving system must provide a clear, unalterable chain of custody. Many regulations stipulate that the archiving system must also prevent anyone from editing archived data.
- Tight security controls – Cyber security plays a big role in compliance. This includes ensuring encryption of all data in transit and at rest. It also includes strong access management with multi-factor authentication and comprehensive auditing.
- Efficient search and retrieval – Users and legal teams must be able to easily search the entire archive, even at scale. This means obtaining search results in seconds rather than minutes or hours. The system should provide comprehensive eDiscovery features, allowing for granular searches.

The migration experts at Messaging Architects bring the tools and expertise to seamlessly migrate your legacy email archives. Whether you use MXLogic, GWAVA Retain, HP Autonomy or another legacy system, we will help you extract a complete, defensible data set. This includes reconciling stubs and maintaining the chain of custody.