



The Business Benefits of Archiving

White Paper

Summary

Email archiving solutions have been available for many years, since they first emerged as a simple way for the IT Department to manage the capacity and improve the performance of their email servers. They have now evolved into complex compliance and discovery solutions, and are central to the successful operation of organizations both large and small.

In this White Paper we identify the four key business drivers for email archiving. We then describe how the latest archiving solutions address these requirements, and highlight the benefits organizations can realize in each of these four areas by implementing an archiving solution.

The Evolution of Archiving

One of the original drivers for archiving was capacity management. Email servers used to be more limited, both in terms of the amount of data they could store and the efficiency with which they could process that data. Archiving addressed these limitations by offloading some of the data to a second tier of storage; as well as storing this data more efficiently, it reduced the load on the email server and improved overall performance for both IT administrators and end users.

Current email servers are now capable of storing almost unlimited volumes of data. Whilst this appears to address the issue of capacity, the cost can be significant and it increases complexity. It brings a new set of problems such as preservation, deletion, compliance and discovery, managing and using that volume of data effectively. These problems apply equally whether the data is stored locally or in the cloud.

All of this is within the context of a continual and unrelenting growth in the volume of email flowing through organizations. Both the number of emails and the size of those emails (including attachments) continues to increase, meaning that email storage requirements for a typical organization can grow by up to 30% per year. It is clear that a 'keep everything' strategy for email is not a workable long-term solution, so organizations need to decide what their approach for managing email is going to be, and to put in place solutions that can meet these needs effectively and efficiently.

Email storage requirements for a typical organization can grow by up to 30% every year.

Business Drivers for Archiving

Capacity management is still a key driver for email archiving, just as it was when the first applications became available back in 2003. Archiving applications have evolved and expanded continuously since then, and now provide comprehensive solutions that address a wide range of business needs, including:



Capacity Management

The volume of email flowing through organizations is typically growing at up to 50% a year, with the number of messages and the average size of each message and attachment both increasing. Organizations that retain all this data within their email server can quickly run out of capacity, as well as experiencing problems with managing and accessing this wealth of information.



Compliance

The business value of email continues to grow, and governments and other regulatory bodies are responding to this by putting in place compliance standards and regulations to ensure email is managed appropriately. The penalties for non-compliance with these can be severe.



Discovery

An increasing number of organizations are having to perform discovery and document review exercises on a regular basis. This may be in response to external litigation, a freedom of information request, or an internal workplace dispute.



PST Management

PST files cause ongoing problems for many organizations today. Often used by end users as personal archives for email and containing valuable business data, these files can be scattered widely across end user devices and network storage.

Capacity Management

The original reason to archive, capacity management is still valid today for organizations that continue to manage their own email server. It's not realistic to retain every email within the live email environment forever. As volume of data increases, simple operations such as retrieval, searching, indexing and backup take longer, use more system resources and become more expensive.

Archiving addresses these issues by moving less frequently accessed information from the live email environment into a secondary location, from where it can be recalled on demand when needed. Users retain access to their email and attachments via their existing email client applications.

Archiving for capacity management can enable organizations to achieve a lower overall cost of ownership whilst providing an improved service to end users. The benefits include:

REDUCED STORAGE REQUIREMENTS	<p>Archiving solutions use two different techniques to reduce the amount of disk space required when they store email data, compared to keeping it within the production email environment. Neither of which have any discernable impact on end users, and they can both deliver significant cost savings:</p> <p>Advanced compression technologies can save 50% or more in overall storage requirements by compressing each email and its attachments before they are archived.</p> <p>Deduplication (or 'single-instance storage') ensures that only one copy of each message or attachment is actually stored within the archive.</p>
INCREASED SERVER PERFORMANCE	<p>Moving older data out of the live email environment and thereby reducing the total volume of data stored will increase the overall performance of the email server, simply because it has less information to process. IT Administrators will also find it easier to manage because there is less data involved.</p>
QUICKER BACKUP AND RESTORE	<p>The amount of data stored within the email server is much smaller, therefore the time it takes to backup this data will be reduced. System recovery operations will also of course be quicker and easier.</p>
CIRCUMVENT MAILBOX QUOTAS	<p>Most organizations enforce a mailbox quota for each user in order to manage the overall amount of data stored with the email server and ensure this does not exceed the limits of currently available storage. These quotas are not popular with end users as they reduce their productivity, and managing them is also often a significant overhead for administrators.</p> <p>By moving less frequently accessed email out of the primary mailbox on an ongoing basis, archiving will allow users to keep as much email as they need without exceeding their quota.</p>
ELIMINATE PST FILES	<p>In earlier versions of Outlook, users were encouraged to move older email from their live mailbox out into 'personal folders' (otherwise known as PST files) using the 'Auto Archive' feature. These files are stored locally, and as data in them does not count against the size of the user's mailbox, they are often used as a means of keeping the mailbox under quota.</p> <p>PST files are not a good long-term solution for secondary storage of email as they are unreliable and easily corrupted or lost, they are often not backed up, and a lot of time can be taken up resolving the problems they can cause. Archiving provides a reliable and robust alternative approach to long-term email storage, and will allow organizations to eliminate the use of PST files completely.</p>

Compliance

Compliance is rapidly becoming a must-have requirement for many companies. The US and Europe are leading this trend, but the rest of the world is following and it will eventually become the norm.

As enterprises of all sizes grow more reliant on email, the business value of that content also grows. Governments and other regulatory bodies are recognizing this by putting in place a growing number of compliance standards and regulations to ensure it is managed appropriately, and the penalties for non-compliance with these can be severe.

Organizations are typically responding by formalizing high level corporate governance guidelines. These must then be implemented in all areas across the organization in order to demonstrate that the business is operating in a compliant manner and to minimize their ongoing legal risk.

The challenge with managing compliance for email is to enforce both the retention and the deletion of email as required, and achieve a balance of saving only what is needed, and only for the time that it needs to be saved. It is not feasible or even acceptable to simply keep everything forever 'just in case'.

Archiving solutions meet this challenge by putting in place a comprehensive set of email management policies which drive ongoing preservation and deletion activities.

PRESERVATION

The first half of the task is to secure and preserve email in accordance with email management policies. The requirement may cover all company communications, but it is more likely that retention policies may target specific key users, or departments that are dealing with particular business functions.

Journal Archiving: Allows email communications to be captured before they can be modified or deleted by users, and ensures an accurate record is secured. It will archive this data in a secure, tamper-proof repository where it can be indexed and made available for subsequent search and retrieval, and to meet requests for eDiscovery.

DELETION

The second half of the task is to ensure that email is deleted in accordance with email management policies. The scope of this activity is wider than for preservation, and usually covers all email within an organization. Therefore, it will include email in user mailboxes as well as in archives and PST files.

Retaining large amounts of email once it is no longer relevant or useful brings significant risks for an organization. Information with no business value increases the cost of eDiscovery, hinders retrieval, and hampers business intelligence efforts through the sheer noise of irrelevant data.

Alongside this, organizations must be able to defend their deletion programs if challenged in courts, otherwise they risk being guilty of spoliation. They should be able to present an audit trail of actions taken, as well as demonstrating an evenly-applied set of policies which are responsible for deleting information.

Certain key users or departments may have specific retention criteria because of the nature of their work. For instance, it may be necessary to keep all email for one particular team for seven years, or to delete all email for another team after ninety days. Outside of those specific cases, it is now becoming common to set a default enterprise-wide deletion policy for all other users (such as deleting all email over two years old).

Discovery

Having recognized the business value of email, and implemented policies to retain and archive it as required, organizations will need to search this email for a number of different business purposes such as internal audits, HR requests and compliance supervision. Most archiving solutions provide a search and retrieval capability for data that has been captured and retained within their archive.

Preparing for Litigation

When faced with a formal need to provide information, such as for a legal case or a Freedom of Information (FOIA) request, it is necessary to undertake a rigorous eDiscovery process for searching and collecting data. Each year an ever increasing number of companies are now facing discovery challenges, and 90% of eDiscovery entails email so this certainly something that should be planned for.

A formal eDiscovery process can be very time-consuming for IT Administrators. If they have already implemented archiving for Capacity Management or for Compliance, and are actively enforcing email retention and deletion policies, then subsequent discovery processes will be more efficient, but they are still a distraction from their day to day job.

Many archiving solutions are now providing the ability for expert end users such as Litigation Managers, Legal Reviewers and Human Resources to undertake the formal Discovery process themselves. As well as taking the burden of discovery away from IT, these role-based solutions are tailored to meet the individual needs of each particular user group, which streamlines the overall process and makes it more efficient.

The end user or reviewer is typically provided with a four stage Discovery process, supporting the early stages of the industry standard EDRM model:

IDENTIFY	SECURE	CULL	EXPORT
<p>The process starts by locating all sources of email that need to be searched. This data could be in an archive, but it could also be in an email server, or even in PST files on end user desktops.</p> <p>The reviewer will search through it to define the initial set of data that needs to be collected, using broad search terms such as custodian (mailbox), date or keyword.</p>	<p>This initial set of data is then stored or tagged in a secure location or archive so it cannot be amended or deleted.</p> <p>At this point the data is effectively on 'legal hold' and the reviewer will notify end users if needed.</p>	<p>Data previously gathered and secured is refined iteratively using more granular search terms, and the reviewer will focus in on exactly what is needed in this particular case, resulting in a smaller and more closely targeted data set.</p>	<p>The final targeted set of data that has been identified is exported out for subsequent detailed analysis or other use.</p>

PST Management

Users may have moved email from their live mailbox out into 'personal folders' (otherwise known as PST files) stored locally. They might have used the 'Auto Archive' feature in Outlook to reduce the size of their mailbox, or they could be using local folders as a convenient way to store and organize their older email.

Although they are in wide use across many organizations, PST files create a number of problems for IT administrators. From a technical perspective they are not a good way to store valuable data for the longer term as the PST is not a robust file format and is easily corrupted.

These files can be stored almost anywhere – typically on end user devices or network. Although IT administrators know these files exist, they are unlikely to know exactly how many they have within their organization or where they are. As a result they will be taking up a considerable amount of storage and incurring costs, but are probably not being backed up on a managed basis and therefore are liable to be lost or misplaced.

From a compliance perspective they are effectively unmanaged and therefore constitute an ongoing risk to the organization. Even if they're within central control, they could very well fall outside corporate governance and retention supervision. They may contain millions of email messages which must be searched and produced in response to eDiscovery and information requests.

PST management solutions are available that provide the ability to regain control over these PST files and the data within them. The starting point is to identify the files, usually by scanning end user machines and network drives. This can be a significant exercise, and the latest highly automated software is designed to enable IT administrators to complete this efficiently with minimum disruption to their users or their operational environment.

Once IT knows where all these files are located, it is possible to ensure that they are backed up on a regular basis and include them in discovery activities, thus ensuring that the data within them is being managed correctly.

Although this will address the immediate issues, it is not a robust approach and therefore does not provide an ideal long-term resolution. Organizations should look to eliminate the use of PST files altogether by using an automated PST management solution such as Barracuda PST Enterprise to delete obsolete data and then migrate the rest of the data from these files back into their email archive.

We have seen that archiving provides a reliable and robust alternative approach to long-term email storage, and PST management solutions are available to discover and archive existing data from PST files. This will allow organizations to eliminate the use of PST files completely.

The average size of a PST file is 1.3 GB - equivalent to more than 100,000 emails.

Many organizations average 3-4 PST files per user.

A View to the Future

Email, and the information within it, has become a valuable asset that is key to the operation of most businesses. It is now the main means of communication both internally and externally, and therefore it is essential to manage this data effectively across the entire organization.

We have seen how email archiving solutions have evolved from their initial role to provide Capacity Management, and how they now deliver a broad set of capabilities for email that include Compliance, Discovery and PST Management.

We are seeing the use of other forms of electronic communication – such as instant messaging and social media – continue to increase in importance. These need to be managed in a similar way to email, and therefore archiving solutions are now evolving to include these other formats.

There will be an increasing desire to search the wealth of information contained within stored email, and to use this to benefit the business. This has proved difficult until recently as email probably represents one of the largest unstructured data sources within most organizations. Highly sophisticated search and analysis techniques are now becoming more readily available, and we can expect to see these included as standard in archiving solutions.

The pressure on IT departments to keep costs under control and to maximize efficiencies will no doubt continue. One effect of this will be a trend of enabling end users and other business stakeholders such as HR and Legal teams to take on tasks that up to now have traditionally been the responsibility of IT.

This is driving the development of new role-based functionality targeted specifically at end users. We already starting to see business users being able to work directly with archiving systems to determine and implement data retention policies, or to search and retrieve the information they need for legal cases.

Conclusion

The simple email archiving applications first seen many years ago have now evolved into highly complex archiving and PST management solutions such as Barracuda Message Archiver and Cloud Archiving Service, and are key to the successful operation of organizations both large and small. They continue to develop in response to ever changing business and technical environments,

About Barracuda Networks, Inc.

Barracuda (NYSE: CUDA) simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications, and data regardless of where they reside. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide, and are delivered in appliance, virtual appliance, cloud, and hybrid configurations. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network security and data protection. For additional information, please visit barracuda.com.

US 2.0 • Copyright 2017 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008
408-342-5400/888-268-4772 (US & Canada) • barracuda.com

Barracuda Networks and the Barracuda Networks logo are registered trademarks of Barracuda Networks, Inc. in the United States.
All other names are the property of their respective owners.

Email archiving solutions are able to manage the complete end to end lifecycle for email.

Finding & securing email data, regardless of its location

Implementing policies to retain & archive only the data that is needed

Retaining this data for as long as it is needed

Making this data available for search & discovery

Deleting this data when it is no longer needed



Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com