WHITE PAPER:
THE INEVITABLE EXTINCTION OF PSTS

Symantec Enterprise Vault.cloud™

The Inevitable Extinction of PSTs

Who should read this paper

Microsoft® Exchange administrators are responsible for the integrity, security, and availability of an organization's email platform. Some of the most common threats to mailboxes are viruses, spam, and hardware failures, but there is another, often overlooked culprit—PST files.

This white paper discusses the problems that PSTs cause as well as a systematic approach for eliminating them.

Content

Executive summary

Microsoft® Exchange administrators are responsible for the integrity, security, and availability of their company's email platform. Some of the most common threats to their organizations' mailboxes are viruses, spam, and hardware failures, but there is another, often overlooked culprit—PST files. Allowing users to retain email messages in PST files may be the most harmful threat to Microsoft® Exchange Server mailbox data.

PSTs, also known as Personal Storage Tables, are file formats that Microsoft Outlook® users can leverage to store calendar items, email messages, and other data outside of their mailboxes to circumvent quotas and free up storage space on mail servers. PSTs are usually distributed throughout an organization on local desktop computers, laptops, file servers, and thumb drives. They often contain a significant amount of valuable company information that may not reside anywhere else.

Since PSTs are not always saved on your corporate network, they pose significant risk and legal exposure. Companies must be able to quickly and easily access this information for legal discovery, regulatory compliance, and knowledge management purposes, but they can't when the files reside in various locations. In addition to being spread across the enterprise, the files may or may not be accessible.

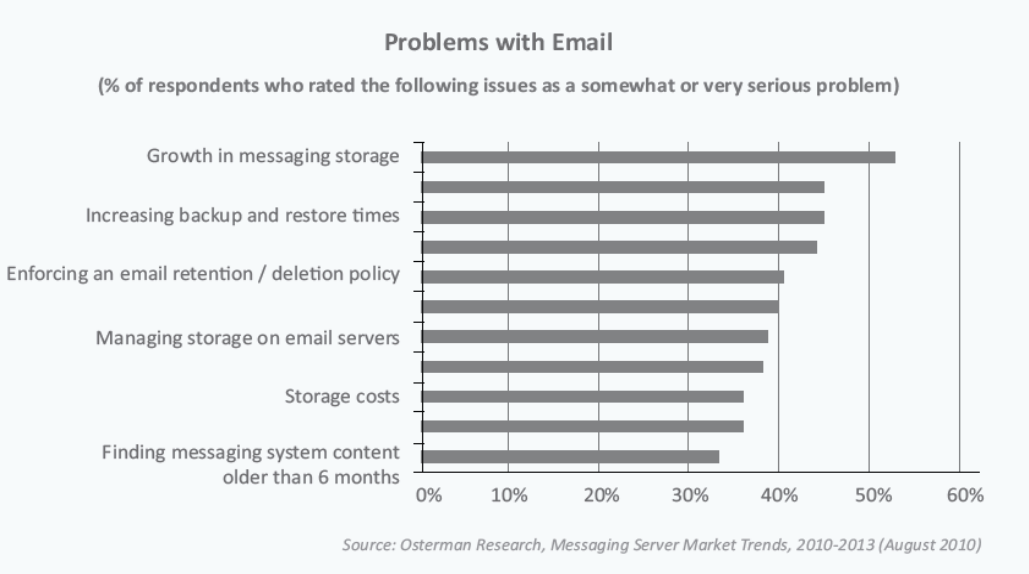
This white paper discusses the problems that PSTs cause as well as a systematic approach for eliminating them. It also offers solutions for centralizing email data, securing intellectual property, mitigating legal exposure, and making IT departments and end users more productive.

The rise of PSTs

In an effort to improve email server performance (slowed down by the continually growing volume of email and attachment sizes) and shrink backup windows, many Microsoft Exchange administrators started imposing mailbox quotas to save money on constantly adding more server storage.

When end users max out quotas, they frequently start searching for alternative ways to retain their important emails and attachments. This is generally where PSTs come into play.

Many of the biggest headaches related to email management stem from PST files, including growth in messaging storage, increasing backup and restore times, excessively large mail stores on the server, enforcing email retention/deletion policies, and storage costs.



Not only do PST files allow end users to get around company mailbox limits, they are also accessible even when users aren't connected to Microsoft Exchange. Anyone who has Outlook at home and employs POP3 to download their email via the Internet probably uses a PST file. This ease of use has contributed to the widespread adoption of PSTs.

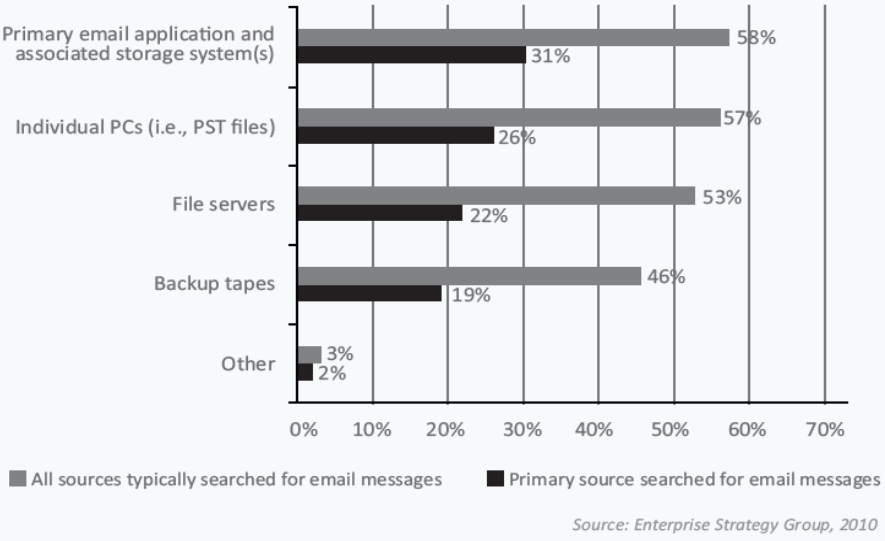
Email = Potential evidence

Electronic discovery (eDiscovery) is becoming significantly more important.

In addition, court decisions over the past few years have also made email content more important for discovery purposes. Judges have held the possessors of electronic content liable for most or all of the costs of legal discovery if the opposing party demonstrated that the discoverable information was of value in a case. Recovery costs are estimated at $500 to $1,000 per backup tape, which can add up very quickly.

Unfortunately, PST files significantly hinder the discoverability of ESI, since they are spread out in so many different locations.

Figure 1



Since these personal archives could be anywhere inside or outside the organization, IT has to search for messages in several repositories when they get an eDiscovery request. Further, having to go through the arduous process of collecting data from local PST files presents three additional problems:

1. The entire process is very disruptive to IT staff, who must stop work on other tasks in order to search through all of the locations where local PST files might reside.
2. The entire process can take a long time to accomplish—weeks in some cases.
3. There is no way of knowing if all of the local PST files have been found, such as those that might be located on local drives or laptops.

PST files contain corporate memory

Approximately three-quarters of information users need to do their jobs is tied to email. As a result, local PST files and other message stores are a critical source of information and contain most of the corporate memory organizations possess.

This information is important for organizations to access, since it not only helps users do their work, but it also contains records of corporate communications with key clients and business partners as well as other intellectual property. An inability to access these records quickly and easily means that corporate knowledge—the most important single asset that nearly all organizations possess—is simply lost.

Problems posed by PSTs

PST files create major problems for companies, including the following:

Control—Microsoft Exchange Server and Outlook don't have built-in tools to centrally manage or monitor how PST files are being used. This isn't an inherent security threat, but administrators do not want data residing somewhere they cannot manage or monitor it. In some cases, end users create "underground archives" to elude mailbox quotas. Once they get close to their mailbox limits, they simply forward email to their Gmail® or Hotmail accounts (where they can get 5 GB mailboxes for free), and then delete the emails from their company mailboxes. This is exceedingly problematic and risky, as your corporate data is out of your IT and legal control.

Compliance—Regulatory requirements are also placing increasing emphasis on the role of email and other electronic content as a source of corporate records. There are a number of regulations, including the Sarbanes-Oxley Act, HIPAA, and the Americans with Disabilities Act, that require organizations of all sizes to retain electronic content for long periods of time. If your organization has retention/disposition policies in place, PST files let users get around those polices. When electronic data is not stored in one place, centrally managed or otherwise accessible to IT staff, retention and deletion policies are much more difficult to enforce.

Data accessibility—Most of the content contained in PST files is not easily accessible to organizations at large, nor is it easily accessible through conventional data recovery tools. Although local PST files are technically accessible to IT staff, finding and collecting all of them in a central repository is difficult, time-consuming, and very expensive.

eDiscovery challenges—PST files complicate eDiscovery efforts and can lead to serious legal or regulatory problems if you cannot find relevant emails when you need them. When IT is asked to search email repositories, they may potentially overlook or never see relevant messages, depending on where they are stored. When the data is stored in PSTs, users may delete incriminating messages—which is frowned upon by the courts. Ultimately, PSTs cost companies a lot of time and money when it comes to gathering them for an eDiscovery request. Industry experts report that organizations typically spend millions in legal discovery costs for every billion dollars in sales.

Storage space—If PSTs are stored within your infrastructure, the cost is huge. This is because the file format is bloated and consumes more storage than if it was stored in Exchange. In addition, many employees save duplicate copies of PST files to network hard drives to ensure they are backed up, which exacerbates the problem. Some companies estimate 25–60 percent of shared drive storage and backup comes from PST files. Uncompressed PST files can cause very inefficient storage, since they consume significantly more space than compressed files—in some cases consuming 40-plus percent more.

Increased backup windows—An abundance of PST data places additional load on backup applications, resulting in increased backup times and delaying the backup of other important corporate data. A survey conducted by Osterman Research found that 45 percent of organizations view increasing backup and restore times as a serious or very serious problem.[1] In addition, every time a PST file is opened

1-"Messaging Server Market Trends, 2010-2013," Osterman Research, Inc., August 2010

(whether it is modified or not), it "looks" like a changed file to incremental backup programs. Translation: PST backups are highly redundant and inefficient.

Data loss prevention—Locally stored messages (i.e., PST files) may contain sensitive data that can lead to a breach if a user's laptop is lost or stolen. In addition, PST files are the most common way users take mailbox data with them when they leave a company. They simply put it on a portable device and walk out the door with your company's valuable intellectual property (IP). These scenarios pose serious threats to companies as well as major headaches for IT (and end users, when data in PST files is lost).

Lost end user productivity—End users often spend considerable time managing PST files because they are reluctant to delete email. When they hit their mailbox limits, they create PST files to save valuable messages and attachments. If you add up the time users across your organization spend managing PST files, it can very likely amount to thousands of hours of lost productivity on an annual basis.

Potential data corruption—The PST file format itself is unstable and prone to corruption. Large files tend to get corrupted easily, and the larger the file, the more performance wanes. Microsoft doesn't support PST files that are linked over a network connection, because they can become corrupted if there is a network issue or packet loss.

Better PST management

Eliminating the use of PST files isn't simple, but Symantec Enterprise Vault.cloud™ employs a simple seven-step process and addresses these important questions:

- What am I going to do with the data that currently resides in PST files?
- What happens to my mailbox stores if I prohibit users from saving messages in PST files?
- If users must keep certain messages long-term, what takes the place of PST files?
- How can I enforce the decision to eliminate PST files?

The following overview highlights some recommended best practices for limiting PSTs and ingesting them into an email archiving solution:

1. **Enable journaling**—The process of eliminating PSTs begins with enabling journaling. Journaling is a process that forwards a copy of all email communications (including incoming, internal, and outgoing messages) to a third-party service provider like Enterprise Vault.cloud in real time over the Internet, using a secure connection (TLS/SSL). Enterprise Vault.cloud is specifically engineered to index all data for streamlined searching and authenticity purposes. All messages are time and date stamped, serialized, and stored in secure, geographically dispersed data centers. With all email being copied and stored in a central, online repository, it's easier to implement the subsequent steps for PST elimination.
2. **Enable access to personal archives (Outlook integration)**—Most modern archiving solutions include Outlook integration, which gives end users access to their personal email archives (i.e., every email they have ever sent or received) directly from their Outlook interface. In addition, many solutions can ingest legacy data (i.e., emails sent and received before archiving began) with the simple transfer of PST files, so those communications are also indexed and searchable in the archive. Some archiving solutions even preserve the folder structure of the PST files upon ingestion into the archive.
3. **Educate users**—Once end users understand that all of their PSTs have been ingested into their personal archives, they can get comfortable with deleting emails from their inboxes. If they need them, they can quickly and easily access the archived emails and restore them back to their inboxes, often with just one or two clicks. In addition, there's no reason for end users to continue saving PSTs, since email archiving essentially gives them unlimited mailboxes.

4. **Find all existing PSTs**—Crawl your networks, desktops, backup tapes, and other storage devices to locate all user-generated PST files. IT staff can be more proactive about PST management by having information about the current status of these files, such as where they are located, the types of data they contain, how much compaction they require, etc.
5. **Ingest PSTs into online email archive**—As part of the data ingestion process, your archiving solution should index the emails and attachments stored in PSTs, so they are immediately searchable in the archive. If you choose a service provider that can preserve the folder structure of your PSTs in the archive, your users can search them just as easily as they search their Outlook inboxes. **Note:** You may decide not to ingest all PSTs, since some may be older or personal emails that do not need to be archived (depending on your retention policies).
6. **Turn off users' ability to create PSTs**—Microsoft Exchange administrators can disable users from adding data to their PST files. They can even disable PST file creation by leveraging Microsoft Exchange group policy settings in Microsoft Active Directory®. The actual steps to keep users from adding data to PST files vary, depending on which versions of Microsoft Exchange Server and Outlook your organization uses. **Note***:* Once users understand that the emails and attachments contained in their PST files are searchable in the archive, they no longer have to create PSTs to circumvent mailbox quotas, because the email archive essentially gives them unlimited mailboxes they can access directly from Outlook.
7. **Implement retention policies**—Once you ingest your PSTs, you should develop a workable email retention policy that defines which messages you need to keep and for how long. You may already have a retention policy in place (as dictated by some industry regulations), and you can apply it to your legacy PSTs. Make sure you retain only what is required and nothing more. Most modern email archiving solutions can help you enforce your email retention policies with automatic deletion procedures, which you can set based on the age of the emails in your archive.

How email archiving can help

The growing need to archive email, including content from PST files, makes it increasingly important to implement an archiving solution that can automatically index incoming content, place it into an archive and make it easily accessible on demand.

Enterprise Vault.cloud provides a number of important benefits for organizations struggling with PST files, including:

Search PST content by customizable criteria—Once ingested into the archive, designated reviewers can quickly search and recover relevant email without having to extract data from each file individually. For example, an eDiscovery request might require an organization to provide all email to or from 10 people with specific keywords to opposing counsel. Finding and searching hundreds or thousands of individual PST files for this information is difficult, time-consuming, and costly under normal circumstances, but it literally takes only minutes with Enterprise Vault.cloud. Even if PST files are stored in shared folders, it is not easy or convenient to search within all of those PST files to find specific emails and attachments. Since Enterprise Vault.cloud houses all PST files in a single repository, designated reviewers can quickly and easily search across all emails (including PSTs) from all users.

Compliance made easy—Enterprise Vault.cloud makes policy management dramatically easier for Microsoft Exchange administrators, because they can manage corporate policies for all users, content, and locations from a central management console. Administrators can apply certain policies to particular users or types of content, such as senior managers' communications with external auditors for Sarbanes-Oxley compliance, instead of adopting a one-size-fits-all approach.

Preserving chain of custody—Chain of custody refers to chronological documentation or a paper trail that shows the collection, custody, control, transfer, analysis, and disposition of electronic evidence. In the event of an eDiscovery request, parties to the lawsuit must prove that the information has not been tampered with in any way. Sometimes an IT manager (or the person supervising the data collection process)

may have to testify in a deposition or in court about how they executed the data collection. Enterprise Vault.cloud time stamps, serializes, and gives a unique signature to each email as it is ingested into the archive, which ensures its authenticity in court. Organizations can quickly and easily search the archive to find email that may be relevant to a particular case or internal matter.

Enhanced server performance—Email servers simply run faster when they have less data to manage. Archiving reduces the amount of data on mail stores, so it no longer needs to be managed, virus scanned, accessed, or backed up on a daily basis. As a result, your Microsoft Exchange Server runs faster and more efficiently. Plus, backups run faster and more reliably with less data—and with less data in your backups, you can restore your systems much faster and far more reliably in the event of a disaster, saving you days of downtime and thousands of dollars in disaster recovery costs and lost revenue. In addition, an archiving solution prevents you from having to buy newer and faster hardware as often, which also generates significant cost savings.

Built-in data loss prevention—Companies need to control the information that leaves their organizations via corporate email and PST files. Enterprise Vault.cloud gives you the ability to monitor and document the use of corporate messaging systems—and intervene if necessary—to mitigate risk and protect corporate knowledge, transaction records, confidential customer data, and intellectual property (IP).

Fewer storage headaches—Enterprise Vault.cloud offers unlimited storage and retention, which helps offload significant IT management time, resources and server space from your messaging environment. Enterprise Vault.cloud frees up the space consumed by PSTs, deduplicates the files and makes them searchable. Once your PSTs have been ingested (and disabled from being created), email administrators see significant time savings, server performance improves, and backup windows shrink.

Comply with legal and regulatory requirements—Enterprise Vault.cloud facilitates much more rapid compliance with discovery orders, audits, internal data requests, and other demands for information. Companies can quickly search for relevant messages to meet legal discovery requests with minimal IT involvement by giving your legal counsel access to your archive.

Enforce retention and deletion policies—Enterprise Vault.cloud helps organizations enforce policies regarding data retention and deletion. Since different types of data are subject to different retention requirements, it is important to manage these policies efficiently with as little impact as possible on IT staff and end users. Administrators can setup specific retention and automatic deletion policies to meet their organizations' needs.

Simple self-restore of lost or deleted messages—Enterprise Vault.cloud makes the retrieval process easy with Outlook integration. It gives end users unlimited mailboxes and allows them to quickly and easily access their archived email directly from Outlook (or Lotus Notes®). Plus, end users can restore lost emails themselves—even things they may have deleted—from their desktops, laptops, or BlackBerry® devices.

Grant access rights without a client installation—Enterprise Vault.cloud offers granular permissions to archives via Outlook, OWA, and BlackBerry devices, which makes accessing data easier and more flexible. Administrators can quickly and easily create, configure, and push out Web folders to all of their end users in one fell swoop. The convenient Web folders allow end users to access their personal archives directly from Outlook without having to sign in every time. Plus, administrators can also deploy mailbox quotas without end-user backlash, since they can still quickly and easily access every email and attachment they send or receive in their archives.

How Enterprise Vault.cloud alleviates the burden of PST files

Features	Benefits
Optional deletion of PST files from source PC/server	Supports a PST file elimination strategy benefiting storage optimization and capacity reduction, and reduces risks from IP leakage.
PST ingestion	Allows intuitive, self-service access to all PST data to easily search archived messages via Outlook; user training is not required.
Global search and retrieval	Searches all PST message data quickly and easily in a single pass, unlike Microsoft Exchange, which only searches individual PST files one at a time.
Intuitive PST folder display	Preserves file structure in the archive, for users who rely on folders and the hierarchy contained in their PST files.
Integration with retention and disposition policies	Applies retention and disposition policies to archived emails, including PST files.
All PST message data stored in Enterprise Vault.cloud	Stores all PST message data in Enterprise Vault.cloud; no shortcuts or message stubs are placed in Microsoft Exchange.

Conclusion

Information is the most important asset organizations possess, and most of it is stored in individual mailboxes and other message stores (including PST files) that are not located in the same place or centrally managed. Organizations that use Microsoft Exchange Server typically cannot access this information easily or quickly, unless IT staff spends a significant amount of time and energy locating, indexing, and accessing the content. When organizations are required to find information in support of legal discovery or regulatory requests, for example, conventional data access methods are highly disruptive to IT staff, expensive to implement, and consume a significant amount of time.

Enterprise Vault.cloud provides capabilities to find all information stores (including PST files) used throughout organizations, search across these dispersed information stores for required information, report on the content housed in these data stores, archive data according to corporate policies, and reduce overall storage requirements. Consequently, email management is dramatically improved and IT staff is freed to perform other tasks that offer greater value to organizations.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com

Symantec.cloud Australia
Sydney

Level 14
207 Kent Street
NSW 2000 Sydney
Australia

Sales:1800 080 759
Support: 1800 088 099
Main:+61 2 8220 7000
Fax:+61 2 8220 7075
www.symanteccloud.com

Melbourne

Level 3
437 St Kilda Road
VIC 3004 Melbourne
Australia
Sales: 1800 080 759
Support: 1800 088 099
Main: +61 3 88668000
Fax: +61 3 8648 5855