




Trend Micro, Incorporated 

 **Boost Productivity,
Save Money, and Avoid
Legal Liability with
Message Archiving**

A Trend Micro White Paper | February 2008

Boost Productivity, Save Money, and Avoid Legal Liability with Message Archiving



TABLE OF CONTENTS

EXECUTIVE SUMMARY.....3

IS THERE A JUGGERNAUT IN YOUR EMAIL INBOX?.....4

FIVE QUESTIONS TO ASK YOURSELF ABOUT EMAIL MANAGEMENT.....5

TREND MICRO MESSAGE ARCHIVER MEETS YOUR NEEDS.....6

CONCLUSION.....8



Boost Productivity, Save Money, and Avoid Legal Liability with Message Archiving

EXECUTIVE SUMMARY

The widespread use of email to conduct business has created challenges for companies that affect employees, IT managers, human resources executives, even the CEO and board members. Analysts estimate that 80 percent of a company's intellectual property is contained in its email¹, which includes business-critical data on contracts, purchasing, product specs, corporate policy, and all the other information that employees generate when they communicate by email.

Finding this information when it is needed to solve business problems can be a major source of frustration for employees, one which can consume hours per week. IT managers become involved because they have to find suitable and cost-effective methods for storing this data. By 2011, a typical employee will generate and receive 28 megabytes of email per day²—that's more than three terabytes per year for a 150-employee organization. Such a large volume of inbox data slows down system performance.

However, requiring employees to delete emails to reduce the size of their inboxes destroys valuable business information and creates liabilities from a regulatory perspective, because messages that pertain to business are legal documents and must be retained. IT managers must provide archiving solutions that are searchable and that protect the company from such liabilities as well as spiraling costs—not an easy task. Being able to prove that emails have not been tampered with is a key factor in retaining them for regulatory and e-discovery purposes, as is being able to provide audit trails for searches to protect employee privacy and the chain of evidence.

Considered together, these problems are creating serious issues for companies and need to be resolved. Trend Micro™ Message Archiver efficiently manages secure email storage. It provides fast, easy search capability and reduces storage costs, while enabling e-discovery and compliance with data retention regulations. Message Archiver lowers email storage costs by reducing data on the mail server by as much as 80 percent. The tamper-proof archiving solution allows authorized personnel to search and retrieve emails and attachments quickly throughout an organization, using time stamps and encryption to ensure the authenticity of email. Message Archiver also protects employee privacy by logging transcripts of privileged-user searches that can be sent to a designated “data guardian.”

1. Law Technology Today, “EDD Tips for Email from the Front Line,” March 2007, Frank Chambers www.abanet.org/lpm/lit/articles/vol1/is1/an5.shtml

2. Radicati “E-mail Archiving Market, 2007 - 2011.” May, 2007, Masha Khmartseva and Sara Radicati, Ph.D.

Boost Productivity, Save Money, and Avoid Legal Liability with Message Archiving

IS THERE A JUGGERNAUT³ IN YOUR EMAIL INBOX?

No one can or should resist the convenience that email brings to daily business life. At the same time, however, it can threaten productivity, drive up operating costs, and create legal liabilities. How can this be? Simple. In the old days when letters were typed in triplicate, carbon copies were kept in the appropriate files in file cabinets to make the information contained in communications accessible should questions arise.

With email, the primary means of storage is the employee's inbox, and while email makes it easier to communicate, it doesn't solve the problem of storing and retrieving information later. By 2011 the typical email account will send and receive 28 megabytes of email per day—that's more than three terabytes per year for a 500-employee organization.

The email inbox has become a repository of every conceivable format that can be digitized and sent electronically, regarding every possible topic from casual conversations to legally-binding proposals and contracts, specifications for projects, and policies issued by human resources. Simply managing one's inbox can drain productivity. Between searching for messages, documents, presentations, spreadsheets, graphs, and other images, and trying to reduce the size of their email accounts to stay within size limits, users lose as much as US\$120 per month in wasted time, according to one study⁴.

Meanwhile, this huge volume of data sits on email servers, slowing down traffic, and pushing up storage costs by forcing IT managers to buy additional mail servers. Compressing and archiving messages, such as in Microsoft .PST files, is only a partial solution, adding extra time for archiving and retrieval.

Plus, companies need to be able to produce historic emails promptly during compliance audits. The increasingly pressured regulatory environment has created a focus on records retention, especially with regard to email. In the U.S., laws such as the Sarbanes-Oxley Act and requirements from federal regulatory agencies such as the Securities and Exchange Commission (SEC) and the Food and Drug Administration (FDA) have companies in a host of industries scrambling to get email archiving systems in place—and not just in the U.S., since multinationals and any company with U.S.-based customers must address these requirements in addition to their own country-specific regulations. The Sarbanes-Oxley Act requires sweeping corporate disclosure and financial reporting reform, which means companies have to implement better record-keeping.

In the U.S., under the new Federal Rules of Civil Procedure (FRCP), all organizations (public and private) need to be able to quickly find electronic information including email in the event of a lawsuit. Companies that can't find information or cannot find it quickly enough risk fines from judges. They may also appear to be withholding evidence which weakens their case. Other countries including Australia and Thailand are considering similar rules.

This is making the task of managing mail systems more complex for system administrators and opens companies to fines and other penalties. In addition, without proof that an email has been kept safe from tampering, it cannot be used as irrefutable evidence in court should a company need it as proof in the e-discovery initiatives for a civil lawsuit.

3. Webster's New World Dictionary defines "juggernaut" as a terrible, irresistible force. The tremendous convenience that email brings makes it irresistible, but at the same time it can lower productivity, send storage costs upward, and create the potential for huge fines and penalties.

4. "Meet compliance, manage records with email archiving" MPC Government Resource Center May 2007 edition, by Jesse Fadel

Boost Productivity, Save Money, and Avoid Legal Liability with Message Archiving

FIVE QUESTIONS TO ASK YOURSELF ABOUT EMAIL MANAGEMENT

In dealing with the problem of protecting your organization against lost productivity, rising storage costs, and legal and regulatory liability due to the vast stores of email collecting in employees' inboxes, be sure you can answer the following five questions:

1. Why not use backup tapes as an archive?

Typically backup preserves data with nightly snapshots. Backups will not capture emails sent and then deleted between snapshots. In addition, finding email in backup tapes is expensive and time-consuming because the correct backup tape must be located, restored, and searched. And then you may discover the tape is corrupt.

2. Why not use the archive function in Microsoft Outlook (.PST files)?

These files are locally stored, usually not backed up, slow to access, and prone to corruption. Corporate retention policies cannot be enforced with these files. It is difficult and costly to search throughout an organization if particular email archives are needed for a regulatory audit or legal search.

3. Why not delete email to reduce risk?

Many companies do have email deletion policies, but even if they are followed to the letter, they are not sufficient protection. Once an email has been sent, there will always be at least two copies (sender and recipient). After deletion, copies may still exist on CDs, USB drives, or printed paper, as well as on the recipient's system or the Internet. You might never realize an email exists until it is used as evidence against you.

4. How can I prove an email is authentic?

Digital fingerprints and time stamps on each email can prove email has not been altered—otherwise, there is no proof. Emails stored with encryption also help prevent tampering and protect privacy. Secure logs can track all network and administrative activities. Administrators should be able to configure the system but should not have access to view or modify other users' email. If a user modifies an email in his or her inbox, the original copy should not be changed. Even with these features, external databases required by some email archiving solutions can provide a back door to hostile access.

5. How should I decide what to save?

Sorting email to keep only relevant messages is difficult. It matters who decides what policies are imposed and who is enforcing those policies. Manual sorting is unreliable and expensive. But automatic sorting can also be unreliable because emails and their attachments are usually unstructured documents. Letting employees use their judgment in archiving emails can result in inconsistencies. A single missing email needed for a lawsuit can lead to accusations of withholding evidence, or even financial and administrative penalties.⁵

5. Several of the most notorious examples are cited here: <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1197496448619>

Boost Productivity, Save Money, and Avoid Legal Liability with Message Archiving

What You Need

Ideally, an email archiving solution should offer features that:

- Improve productivity through advanced search capability.
- Reduce data storage by compressing emails and reducing the number of duplicate attachments, saving you costs.
- Authenticate and prevent tampering with email documents.
- Ensure compliance with regulatory requirements.

TREND MICRO MESSAGE ARCHIVER MEETS YOUR NEEDS

Trend Micro Message Archiver manages secure long-term email storage with powerful search capability, while enabling legal discovery and compliance with data retention regulations. It addresses the problems created by high volumes of email traffic in today's workplace in the following ways:

- ④ **Querying large volumes of archived data by content, including attachments, keywords, and meta-data.** Emails and attachments are indexed for quick search based on keywords and metadata. A self-service capability for on-demand searches gives employees the ability to easily find their own email, and power search capabilities enable corporate counsel to respond quickly to requests for evidence related to any email sent to/from/within the company.

With Message Archiver, a simple search can be performed right in Outlook™, or you can pull up the user interface to get more advanced search options. To enable users to find information quickly and easily, Message Archiver performs proximity searches, meaning it finds results with keywords that are located close to one another to get more relevant results; it can perform “sounds similar” searches to find words that are similar or misspelled words such as “attendance” and “attendence.” Also, it performs stemming, which is, for example, looking for the word “run,” and retrieving documents that contain not only “run,” but also words with the same base root such as “running” and “runner.” Wildcards are also permitted in any search field.

- ④ **Lowering email storage costs and improving performance by reducing the volume of data on the mail server.** Integration with Microsoft® Exchange Server® offloads messages from the mail server, reducing inbox storage as well as backup size. Single-instance storage saves just one copy of a message (with attachments) if sent to multiple recipients. The advanced compression techniques of Message Archiver reduce the size of data stored by 50 percent. “Stubbing” further reduces volumes by replacing messages and attachments with shortcuts based on the age of the message. In all, Message Archiver can reduce your total email volume by 80 percent.
- ④ **Providing tamper-proof archiving to ensure email documents are authentic.** Message Archiver encrypts email storage to prevent tampering; privileged user settings prevent unauthorized access. Meanwhile, secure logs track all network and administrative activities, so it is easy for authorized individuals to see who has had access and what they have done.

Boost Productivity, Save Money, and Avoid Legal Liability with Message Archiving

In addition, whenever an email is archived by Message Archiver, the software decodes the recipient information to create a permanent record of to whom the email was sent. The software captures information about who was in the distribution list and who was blind-copied. Then Message Archiver puts a time stamp on the email, which is like a digital fingerprint. Technically speaking, it is an MD5 hash, which ensures that the email is authentic and unaltered. This can stand up in court as legitimate evidence⁶.

- ⊕ **Allowing authorized personnel to search and retrieve emails and attachments quickly throughout an organization.** Since Message Archiver indexes everything within an email and its attachments, it's easy to carry out search requests that comply with regulatory standards. Searches by privileged users, such as a human resources manager, compliance officer, or corporate counsel, are audited, logged, and stored in an encrypted form. This protects employees against invasions of privacy and ensures that someone with access to the system cannot abuse that privilege. This protects both the organization and the employee. Message Archiver will then immediately send copies of the audit trail transcript to nominated "data guardians" to ensure privacy and confidentiality of the stored data.
- ⊕ **Protecting employee privacy.** How important is employee privacy? Employee privacy is the law in the U.K and many other countries, spelled out by the Data Protection Act (UK) and privacy laws. It's a top concern in the U.S., as well. In a recent survey conducted by Trend Micro, 75 percent of U.S. executives polled said that safeguards to protect employee privacy from privileged user search are very/extremely important.

To ensure employees' privacy, organizations must protect employees' email, limit access to it, and audit access to it. Message Archiver encrypts all stored emails and attachments, which protects it from unauthorized use. In addition, access to an employee's email is limited to the employee or to a privileged user. (The person who is managing the archiving does not have access to the email in it.) When these personnel do a search, they have to give a reason for the search. An audit including the reason and the search terms that are used are sent out to the data guardian, who may be a union representative, a privacy overseer officer or another executive whose job it is to safeguard employee privacy to make sure privileged user searches are not abused.

- ⊕ **Achieving ROI within weeks.** Employees are losing US\$120 worth of productivity per month trying to manage their inbox size, or searching for information within their inboxes or, PST archives. That's US\$1,440 per year. A company with 500 employees is losing US\$732,000 per year—money you're already wasting if your organization does not have an adequate email archiving solution. Mid-sized companies are often faced with the same compliance and e-discovery issues as large companies, but cannot afford the cost of enterprise-class email archiving solutions. Message Archiver is designed to solve this problem. You can recoup the cost of Message Archiver quickly, and after that enjoy higher productivity along with lower storage costs while avoiding potentially millions of dollars in fines and penalties.

6. <http://technology.findlaw.com/electronic-discovery/electronic-discovery-guide/processing/audit/analyzing-data.html>

Boost Productivity, Save Money, and Avoid Legal Liability with Message Archiving

CONCLUSION

Despite the benefits delivered by email, the vast volume of data collecting in employees' inboxes creates threats of lost productivity, spiraling storage costs, and legal liabilities. Your company needs an email archiving solution that retains all email and attachments, and enables fast, easy searches to find important business information. Your email archiving solution should save emails in a compressed form that keeps down the cost of storage and optimizes email systems. It should also be able to authenticate emails and attachments and prevent tampering, so that regulatory and legal concerns are met. Trend Micro Message Archiver meets these criteria with a fast, scalable, and powerful email archiving solution that frees employees from the burden of dealing with message archiving and helps your company achieve fast ROI. It works for your organization by improving productivity and protecting it from fines and penalties.

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: +1 800.228.5651

phone: +1 408.257.1500

fax: +1 408.257.2003

www.trendmicro.com

