



# McAfee<sup>®</sup> SaaS Email Archiving

## Solution Guide



McAfee, Inc.  
3965 Freedom Circle  
Santa Clara, CA 95054  
888 847 8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee and/or other noted McAfee related products contained herein are registered trademarks or trademarks of McAfee, Inc., and/or its affiliates in the U.S. and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. Any other non-McAfee related products, registered and/or unregistered trademarks contained herein is only by reference and are the sole property of their respective owners. © 2009 McAfee, Inc. All rights reserved.

## Table of Contents

<b>Executive Summary</b>	<b>3</b>
<b>The (Business) Case for Email Archiving</b>	<b>4</b>
<b>McAfee® SaaS Email Archiving – A Wide Range of Benefits for Every Business</b>	<b>5</b>
<b>Easy Setup and Administration</b>	<b>8</b>
<b>Secure and Efficient Email Transport, Storage, Search and Retrieval</b>	<b>10</b>
<b>McAfee SaaS Email Archiving Packages and Service Suites</b>	<b>13</b>
<b>About McAfee SaaS</b>	<b>15</b>

## Executive Summary

Take a tour of any accounting or finance department and you're bound to find file cabinets and boxes filled with everything from payment receipts to bills to payroll records. These financial files provide a history of money in and money out, and they are particularly helpful in protecting the business during audits, where gaps and irregularities can raise suspicion and the prospect of fines.

Today, smart businesses are taking the same approach with the growing number of email messages that flow in, out and through their organizations. For some industries, particularly financial services and healthcare, the retention of electronic communications is more than a best practice – it is mandated by Federal and industry regulations. Businesses that fail to comply can face substantial fines, and in some cases, jail time for the responsible parties. In addition, all businesses, regulated or not, face workplace compliance issues like discrimination, harassment, and the loss or theft of proprietary information and intellectual property, all of which can often be accurately documented through a trail of email messages.

Thus, it has become increasingly important for businesses to implement an email archiving solution that can efficiently store all inbound, outbound and internal emails, while also providing a fast, accurate method of retrieving individual messages - whether the business is subject to government or industry regulations or if it could potentially come under fire for failing to produce an email as part of a judicial e-discovery mandate.

The McAfee® SaaS Email Archiving service helps businesses to control the ever-increasing volume of email messages in order to satisfy compliance and business data storage needs, while also facilitating rapid, centralized electronic discovery. The fully managed service, which requires no hardware or software integration, enables customers to automatically and securely archive their internal, inbound and outbound email messages to a centralized, secure location. Through an intuitive, easy-to-use administrative platform, the McAfee SaaS Control Console, messages can quickly be searched for and retrieved, using either “Simple” (for novice users) or “Advanced” (for technical users) search screens.

This overview reviews the features, functionality and foundational technologies that power the SaaS Email Archiving service, and explains why choosing a SaaS solution from McAfee over an in-house solution or on-premises appliance is the right choice.

- Ease of administration and use through secure Web-based platform
- Unlimited storage with definable retention periods
- Simple or Advanced Search options
- Wide range of features to support compliance
- Complimentary 24x7 telephone, email and online support
- Convenient, recession-friendly month-to-month contract terms

## The (Business) Case for Email Archiving

While email has become the preferred communications medium between businesses and their employers, partners and customers, it has also added complexity and risk to day-to-day business. Aside from the network-crippling effects caused by malicious threats like spam and viruses, many businesses today are also struggling with storing their growing volume of legitimate email messages, whether spurred on by regulation, workplace compliance issues, or simply by instituting a best practice for proper retention and retrieval of important business information.

- Regulatory and compliance requirements:** Governmental agencies, such as the U.S. Securities and Exchange Commission (SEC) and other regulatory organizations, have established strict requirements for message retention, accessibility, and security. To comply, organizations must establish secure archiving systems which retain electronic communications for a specific time period, while guaranteeing that requested materials can be retrieved and presented in a timely manner.

### Key regulations include:

Regulation	Key Requirements
SEC 17a-3 and 17a-4	<ul style="list-style-type: none"> <li>Broker/dealers must provide 6 years retention, the first 2 in a readily accessible repository</li> <li>Business must maintain redundant copies of message data</li> <li>Reveal tampering or unauthorized deletion</li> <li>Unalterable storage</li> <li>Message must be readily accessible</li> <li>Automatic verification</li> <li>Provide a Letter of Undertaking that can be put on file with the SEC</li> </ul>
Gramm-Leach-Bliley Act	Companies must ensure security and confidentiality of customer data
Health Insurance Portability & Accountability Act of 1996 (HIPAA)	Members of health care industry must retain patient information and safeguard its privacy
Sarbanes-Oxley	Accounting firms that audit publicly traded companies must retain all related documents for 7 years

- Legal discovery and investigations:** Organizations must be able to preserve and retrieve messages relevant to a legal proceeding when ordered to do so by the courts, especially as mandated by recent amendments to the Federal Rules of Civil Procedure (FRCP). Generally one of the first steps in any lawsuit is the discovery process, in which evidence is located to support legal claims. When discovery involves electronic information, the process is referred to as "e-discovery" or electronic discovery. Failing to comply with e-discovery orders can result in harsh court sanctions (punishment for non-compliance imposed by a judge). The SaaS Email Archiving service assures that evidentiary-quality records are systematically stored in a central tamperproof repository.

- **Business continuity and disaster recovery:** Recent research indicates that the number one threat to business continuity is hardware failure. Organizations can mitigate this threat by switching from an unreliable, high maintenance, internal solution to the SaaS Email Archiving service, which securely stores messages in two redundant data centers.
- **Storage management:** As the volume of messages continues to increase on local Exchange databases, an archiving solution lets organizations offload messages from their corporate servers to the SaaS Email Archiving service. Once this is done, historical messages can be safely removed from the customer server, reducing the storage burden and increasing performance.
- **Workplace compliance:** All businesses are at risk from issues like discrimination, harassment, and the loss or theft of proprietary information and intellectual property. The SaaS Email Archiving service enables businesses to automatically store and access all email messages, and can easily produce them if so ordered by a court in the event of a lawsuit. Administrators can also identify outbound messages that include proprietary information via keyword searches, which helps to identify any violations of company information handling policies.

### **McAfee® SaaS Email Archiving – A Wide Range of Benefits for Every Business**

While helping to protect your organization from the many legal ramifications that can result from improper storage and retrieval of email messages, the SaaS Email Archiving service can also help you to reduce costs and increase operational efficiencies.

- **Free IT from on-going service management** - With SaaS, there is no hardware or software to install, integrate or maintain, and continual updates to features and functionality ensure that the service never grows obsolete.
- **Reduce internal requirements for storage** – With the SaaS Email Archiving service you can consolidate .pst files in order to secure company knowledge, and shrink your Microsoft Exchange databases to a more manageable size.
- **Empower end-users** – The SaaS Email Archiving service enables authorized end-users to search for their own archived messages directly on a familiar interface, the McAfee SaaS Control Console, thereby relieving IT from having to perform the task on their behalf.
- **Ensure that message stores are up to date** - McAfee provides near-real time email archiving, which is more accurate and less prone to data loss than delayed point-in-time snapshot backups which only capture messages that are present in at the moment the backup runs. Messages deleted before the backup are skipped and messages that have been modified by end users are recorded in an altered state without an audit trail of the modification.

- **Affordably store all emails** – McAfee provides unlimited storage capacity, which offers freedom from overage charges. Customers can determine how long their emails need to be retained to meet business, compliance or legal requirements, and can choose from 1-year, 3-year, 5-year, and 7-year retention plans. McAfee offers both online and offline options for the secure transport and storage of historical email data. Most businesses can opt to transfer historical email directly to the SaaS Email Archiving system, while organizations with extra-large stores of historical mail can opt for the Managed Import Service.
- **Reduce costs and risks with rapid message retrieval** – Using either the Simple or Advanced Search options, customers can retrieve messages in a matter of seconds, cutting hours, days and even weeks from the time necessary to locate messages compared with many in-house solutions. The speed and accuracy afforded by the SaaS Email Archiving service translates into drastic reductions in the often exorbitant legal fees associated with e-discovery.

### SaaS Email Archiving vs. In-house Solutions

SaaS Email Archiving from McAfee can eliminate the management issues common with in-house archiving solutions - including tape, disk, appliances or software - while greatly improving the ability to quickly and easily retrieve particular messages.

- **Cost effective e-discovery** – With both Simple and Advanced Search technology, the SaaS Email Archiving service enables customers to retrieve messages in a matter of seconds. With tapes, restoring and viewing a single email, or a set of email, across many years of data can be time consuming and costly – and often nearly impossible.
- **No coverage gaps** – The SaaS Email Archiving service records and stores emails in near real-time, as opposed to point-in-time backups, which can result in message loss. Relying on tape backups can result in non-compliance if the backups are made after emails are deleted from the system.
- **Pristine archiving guards against tampering** – The SaaS Email Archiving service verifies that the original message and copies are identical. Conversely, messages can be edited or deleted altogether prior to storage on tape, with no audit trail available to document the changes.
- **Secure message transport and storage** – Messages are transported to the SaaS Email Archiving service securely via TLS or SSL and are stored using 256-bit encryption.
- **Full email disaster recovery** – With the SaaS Email Archiving service, messages are stored at dual, secure off-site locations. Less than a third of companies currently back up their on-site tape archives to an offsite device, which increases the risk of data loss.

- **No single point of failure** – The SaaS Email Archiving service offers off-site redundancy, while few in-house solutions are ever duplicated off-site in real time, making them another device that must be maintained and backed up.
- **No vendor conflicts** – The SaaS Email Archiving service is a complete managed solution that eliminates having to deal with conflicts between application, hardware, and platform vendors whenever technical issues arise.
- **No corrupt indexes, poor reliability** – The SaaS Email Archiving service is always up and running and is not subject to the types of hardware failures common in black box appliances. Hardware failures are cited as the number one threat to business continuity.
- **No declining performance or scalability** – With the SaaS Email Archiving service, messages are always available within a matter of seconds. In-house solutions are often plagued by declining search performance as the amount of stored data grows.
- **No complex implementation and maintenance** – The SaaS Email Archiving service offers easy implementation and can be up and running in a matter of hours once provisioning is completed. In addition, the service removes the burden of on-going management off of IT, helping businesses protect their valuable resources.

### **McAfee SaaS Email Archiving Compliance Features**

Organizations that are mandated to comply with Federal or industry regulations covering email communications can rely on McAfee for the support they need to be fully compliant with today's strict guidelines.

- **Tamperproof read-only storage** – Messages and message metadata are protected in its original state
- **Dual data centers** – Eliminates threat of “single point of failure” and ensures that no message is ever lost
- **Automatic quality verification** – Verify that stored message copies are identical to the original
- **Dual commit message capture** – Messages aren't deleted from customer server until accurate copies are made and verified
- **Auditable message serialization** – adds a unique numeric identifier to each message to comply with SEC requirements prohibiting tampering or deletion of messages
- **Search data, attachments and metadata** – Message can be located quickly and easily through either advanced or simple search technologies
- **Transport and storage encryption** – Messages are transported to the SaaS Email Archiving service securely via TLS or SSL and are stored using 256-bit encryption.

## Easy Setup and Administration

As with all McAfee SaaS email and web security services, the SaaS Email Archiving service was designed from the ground up to deliver enterprise-grade service and performance, without enterprise-level complexity and cost. The service offers a wide range of features and functionality that are delivered via an easy-to-use, highly intuitive user interface.

### Rapid Service Activation and Setup

The SaaS Email Archiving service offers a quick, easy setup and activation process which requires no hardware or software integration. It is also highly scalable to meet the needs of your business without the threat of technology obsolescence.

To begin the service setup, users whose mail will be archived are loaded into the McAfee system. In order to streamline this step, service administrators can use Directory Integration, a user management tool for all McAfee SaaS email and web security services which syncs automatically with the customer's Active Directory. Service administrators can easily synchronize account information, including primary and alias email addresses and distribution lists, thereby eliminating the need to manually make changes in both the corporate directory and the McAfee SaaS system.

Going forward, administrators can use Directory Integration to synchronize information on an automated schedule, ranging from one to four times per day, or they can choose to initiate a manual sync. Once the sync is complete, administrators can view the list of changes prior to giving final approval for the altered directory. Administrators can also review previous synchronization activity to identify all prior changes to user accounts and distribution lists.

With the user information in place, service administrators then setup up transport security on the Exchange server(s) and connect their systems to McAfee. The final activation step is to activate the envelope journaling function of their Microsoft Exchange server(s) (2000, 2003 or 2007 versions).

The journaling feature records a copy, or journal, of all sent and received email messages processed by the Exchange Server. Envelope journaling ensures that BCC and distribution list recipients are captured and archived. The Exchange Server sends this copied email to a dedicated mailbox called the journal recipient mailbox, which resides on the Exchange Server. The service then retrieves the email from this journal recipient mailbox and archives it.

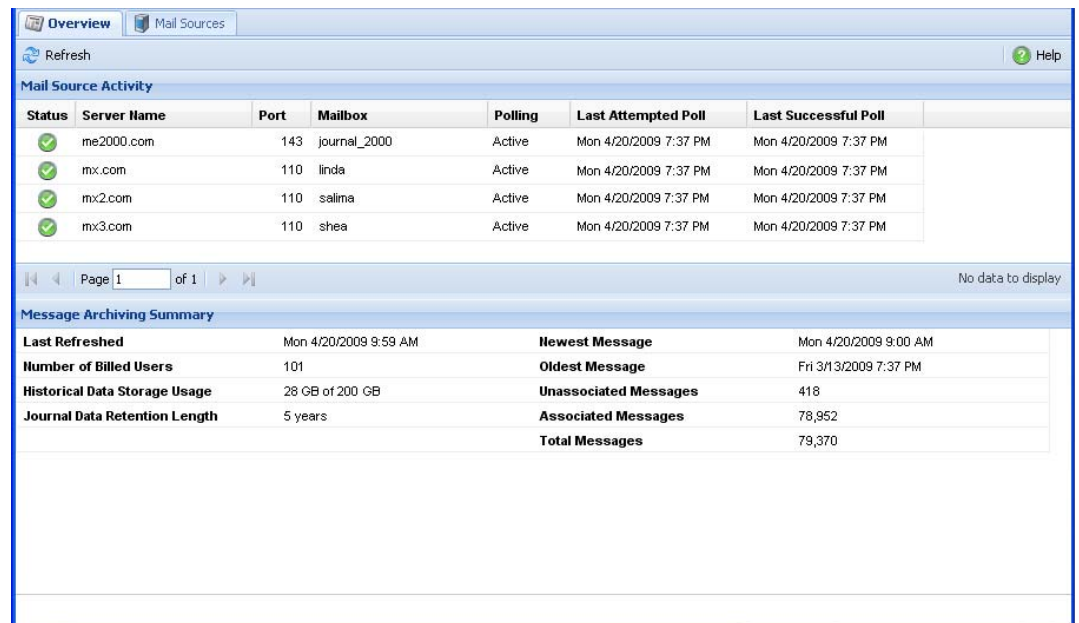
Each Exchange database can have its own journal mailbox, and the SaaS Email Archiving service allows the customer to create a mail source entry for each journal mailbox. Once activated, McAfee will poll each mail source every 15 minutes to check for available messages, which are then pulled into redundant, off-site archives. By using "pull" technology, McAfee is able to eliminate the reliability and security issues that are inherent with solutions that require the customer to "push" mail into an archive. The service supports up to 64 individual mail sources, which can each have unique settings for encryption and quiet periods.

The mail source process is also used in the optional Historical Data Storage feature. Customers can designate a mail source specifically for historical data, designated Historical mail source, from which historical email will be securely transferred to McAfee in much the same manner as current mail is ingested into the SaaS Email Archiving service.

**Streamlined administration through the industry’s most intuitive management console**

The initial setup and all on-going administration of SaaS Email Archiving are performed through the McAfee SaaS Control Console, the highly-acclaimed and innovative administrative platform that supports all McAfee SaaS email and web security services.

The Email Archiving area on the McAfee SaaS Control Console is first service area to incorporate a newly designed user interface, which was developed to improve workflow and reduce the time it takes to perform common tasks ranging from message restores to e-discovery. The advanced interface looks and responds very similar to a desktop application, making it familiar and easy to use.



(Fig. 1 – McAfee SaaS Control Console, Email Archiving Overview)

The Email Archiving Overview page includes a wide range of important at-a-glance information, including:

**Mail Source Activity**

- The current status of system connections is quickly viewable based on the color-coded Status icon. This system health monitoring feature provides on-going status information for each active mail source, helping administrators to identify and troubleshoot connectivity issues.
- Configuration parameters for each connection are displayed, as defined in the Mail Sources screen.

- The time of the last attempt to connect to each mail server in order to archive messages.
- The time of the last successful connection to each mail server.

#### **Email Archiving Summary**

- The last time the administrator logged into the McAfee SaaS Control Console.
- The last time the administrator refreshed the Overview page.
- The total messages that are currently archived
- The retention length for archived messages, as configured on the Customer Management screen.
- The date and time when the oldest and newest messages were archived. Administrators can use this information to determine when older messages might start dropping from the Message Archiving database.
- The number of users whose messages are being archived, as created using the McAfee SaaS Control Console User Synchronization screen and/or the Create User screen.
- The number of associated, unassociated, and total messages archived from the mail source.

### **Secure and Efficient Email Transport, Storage, Search and Retrieval**

Whether your organization chooses to archive its inbound, outbound and internal email messages due to compliance or legal issues, or simply as a best business practice, SaaS Email Archiving from McAfee is the smart choice, with:

- Secure, end-to-end email transport
- Definable retention period
- Simple and Advanced Search options
- Fast message retrieval

#### **Secure email transport to McAfee**

Once your mail sources have been configured and activated, McAfee begins polling each one on a regular basis to import new messages. As noted above, this import process eliminates the reliability and security issues inherent with solutions that push messages from the customer to the archive.

During each import attempt, the service will attempt to import a pre-set number of messages, determine whether each message was imported successfully, then remove each message that was imported successfully from your mail source. Messages that cannot be imported are left in your mail source, ensuring that messages are never lost. While this is occurring, more messages will arrive in the journal mailbox, which will not be imported until a future attempt. The time it takes to complete an import cycle depends on your e-mail volume, server load, server performance, and available upstream bandwidth.

The SaaS Email Archiving service uses powerful encryption when messages are in transit and at rest. All messages and metadata, including the index, are stored using 256-bit encryption. Customers can require that all data is transported via a secure connection as part of the Mail Source configuration to import messages from their server(s), using either Secure Socket Layer (SSL) or Transport Layer Security (TLS) encryption methods.

### **Efficient off-site email storage**

Any organization can quickly eliminate the burden placed on its IT department related to the management and maintenance of in-house email message stores by utilizing our SaaS service. Businesses that rely on McAfee for message storage can drastically reduce their hardware related costs, as well as the soft costs for resources involved in day-to-day system management.

The SaaS Email Archiving service provides unlimited storage and is available with various durations of message retention in order to better meet the specific needs of an organization. More information about service packages can be found in Section 5.

- **Stand-alone SaaS Email Archiving packages** – available with 1, 3, 5 or 7 years of retention
- **Service Suites including SaaS Email Archiving** – available with 3, 5 or 7 years of retention

To increase security and aid compliance, we implement tamper-proof, read-only storage, which ensures that all messages and message metadata are protected their original state

Unlike other solutions, the SaaS Email Archiving service does not offer message stubbing, a process that strips an email of its attachments, replaces them with a stub file or link within the message, and then stores the actual attachment in an archive. The main disadvantage to stubbing is that it removes message content data from Exchange, which prevents users from easily searching for that data with Outlook or Exchange search tools. In addition, stubbing usually only works on attachments, and leaves behind all other message data including the header and body. The SaaS Email Archiving service addresses these limitations by allowing customers to import entire messages from Exchange, while providing end users with open access to those messages and their attachment content via an Outlook 2003/2007 add-in.

### **Fast, precise message search and retrieval capabilities**

The key to any email archiving solution is not the actual storage of messages, but how easily and quickly individual messages can be retrieved from the storehouse. The importance of message retrieval cannot be overstated, as email messages are often the “smoking gun” that can prove guilt or innocence in the courtroom, or by serving as evidence that a business is fully compliant with Federal or industry regulations covering the proper handling of electronic communications.

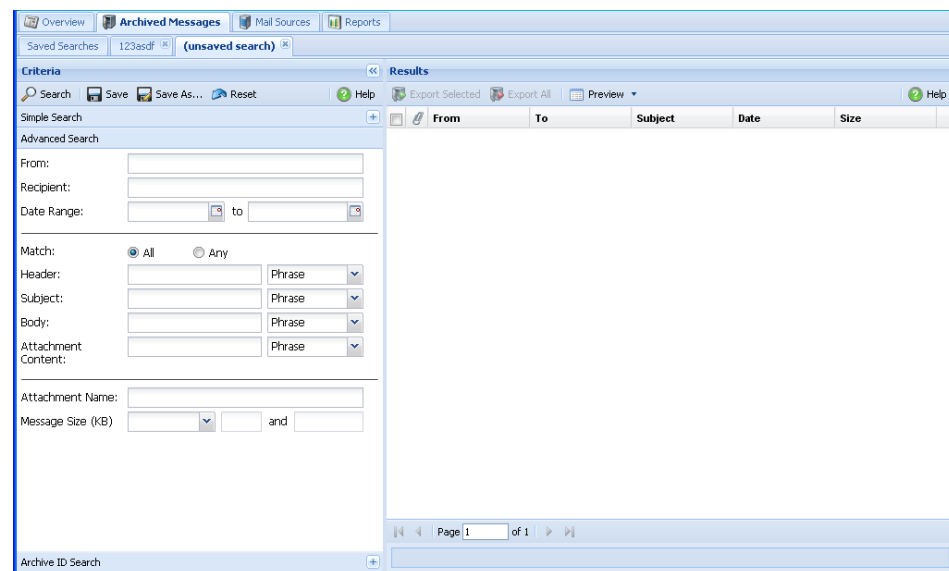
Often compared with finding a specific needle in a stack of needles, message search capabilities can vary vastly from provider to provider. The SaaS Email Archiving service is based on search engine technology and not relational database technology, and is therefore able to scale much more

efficiently than a traditional database. The McAfee search architecture is based on technology similar to that used by Internet search engines, and is therefore able to index vast amounts of data while maintaining excellent search performance. Traditional relational databases have excessive overhead and do not scale as efficiently.

Through the McAfee SaaS Control Console, authorized staff members are armed with quick, accurate search capabilities for retrieval archived messages, based on search criteria that include:

- Message headers
- Subject
- Body content
- Over 300 attachment file types
- Common fields such as Sender, Recipient and Date

Authorized staff can choose to initiate a search via Simple, Advanced, or Archive ID search interfaces.



(Fig. 2 –

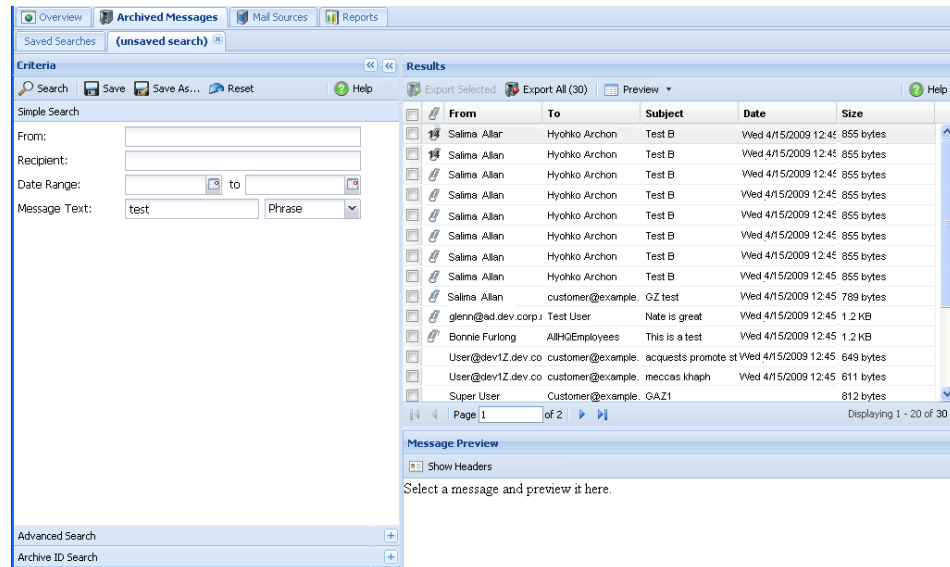
**Advanced Search)**

The search capabilities of the service are unrivaled, and include several features designed to take the hassle out of message management for service administrators:

- **Parallel Search Technology** – McAfee enables efficient multitasking by allowing administrators to view multiple search parameters and results conveniently on one screen.
- **Saved Searches** – Authorized users can save searches for later use, saving time and effort wasted on redundant tasking

- **End-user support** - Enables authorized users to review their own archived messages without requiring assistance from an organization's IT staff.
- **Outlook 2003 and 2007 integration** – An add-in that allows authorized users to search for, view and save copies of archived messages directly through their Microsoft Outlook 2003 or 2007 email client.

The streamlined McAfee SaaS Control Console makes reviewing of search results quick and easy.



(Fig. 3 – Search Results)

The SaaS Email Archiving service includes several configurable options for reviewing search results, including enabling administrators to sort message based on From, To, Subject, Date and Size. A selected message can be viewed in a simple preview pane by scrolling down the list of results, or the entire message can be viewed simply by double-clicking on it. In addition, administrators can also view message header information, which includes technical details about the message.

Using the Export feature, authorized staff can download copies of archived messages to their computers, leaving the original pristine copy in the archive. Individual messages can be exported, as well as up to 150 MB of messages within the Search results pane.

## McAfee SaaS Email Archiving Packages and Service Suites

McAfee offers two SaaS Email Archiving packages, each offering a different message retention length, including:

- SaaS Email Archiving – 1-Year Retention
- SaaS Email Archiving – Multi-Year Retention

McAfee SaaS Service Suites combine the power and protection of our industry-leading email security, Web security and email archiving managed services – all backed by live 24x7 support, innovative technology and our experienced team of threat experts. You can choose the following service suites to meet the unique needs of your organization:

**Complete Security<sup>SM</sup>** - A comprehensive suite that protects your business from spam, viruses and worms, email attacks, fraud and spyware, while enabling you to efficiently store and retrieve all inbound, outbound and internal emails. In addition to McAfee® SaaS Email Protection & Continuity, Complete Security includes McAfee® SaaS Web Protection Total Control and McAfee® SaaS Email Archiving with either 1, 3, 5 or 7 years of data retention.

**Email Security & Archiving<sup>SM</sup>** – This suite combines our award-winning SaaS Email Protection threat and disaster recovery services with SaaS Email Archiving for organizations looking to protect their vital email communications. This suite is available with 1, 3, 5 or 7 years of data retention.

**McAfee Service Suite Features**

SaaS Email Protection	SaaS Web Protection	SaaS Email Archiving
<ul style="list-style-type: none"> <li>• Advanced spam blocking</li> <li>• Triple virus and worm scanning</li> <li>• Content and attachment filtering</li> <li>• Email attack protection</li> <li>• Fraud protection</li> <li>• SaaS Email Continuity</li> <li>• SaaS Control Console</li> <li>• Sophisticated, 14-day spam quarantine</li> <li>• Group policies management</li> <li>• Enforced TLS security</li> <li>• 24x7 threat monitoring and protection</li> <li>• (Optional) Outbound filtering</li> <li>• (Optional) Email Intelligent Routing</li> </ul>	<ul style="list-style-type: none"> <li>• Anti-spyware scanning</li> <li>• Anti-virus scanning</li> <li>• Anti-phishing protection</li> <li>• URL filtering</li> <li>• Safe Search protection</li> <li>• Peer-to-peer site blocking</li> <li>• Streaming media site blocking</li> <li>• Group policies management</li> <li>• IP and user-level authentication</li> <li>• SaaS Control Console</li> <li>• 24x7 threat monitoring and protection</li> </ul>	<ul style="list-style-type: none"> <li>• Unlimited storage</li> <li>• Advanced search options</li> <li>• Definable retention for 1, 3, 5 or 7 years</li> <li>• Secure data transport and storage</li> <li>• Transactional data acquisition</li> <li>• Parallel Search Technology</li> <li>• Outlook 2003/2007 integration</li> <li>• Saved searches capabilities</li> <li>• Mail source health monitoring</li> <li>• SaaS Control Console</li> <li>• 24x7 online or phone Customer Support Services</li> <li>• (Optional) Additional historical data storage (25GB increments)</li> <li>• (Optional) Managed Import Service</li> </ul>

All McAfee SaaS stand-alone packages and Service Suites include complimentary phone, email and online Customer Support Services, and all are available through convenient month-to-month terms, with no setup fees.

In addition, customers can turn to McAfee for both online or offline transport and storage of their historical message data, a feature available in 25 GB increments.

### **About McAfee SaaS**

As part of the world's largest security-dedicated vendor in the world, McAfee SaaS is a leading developer of cloud-based security solutions, providing real-time protection to more than 575,000 businesses. McAfee SaaS offers the industry's most comprehensive, cloud-based security portfolio, including email and web protection, message continuity and archiving solutions. McAfee's true multi-tenant, massively scalable SaaS architecture delivers enterprise-grade performance and reliability without enterprise-level complexity and cost. Additionally, McAfee SaaS solutions provide unrivaled protection, leveraging McAfee's Global Threat Intelligence Network of 350 researchers and threat centers in 30 different countries.

McAfee SaaS Email & Web Security Sales Team  
9781 South Meridian Blvd., Suite 400  
Englewood, CO 80112 USA  
T +1.877.695.6442  
F +1.720.895.5757  
E [sales@mcafeesaas.com](mailto:sales@mcafeesaas.com)