MICRO FOCUS

Product Flyer

Retain Unified Archiving
Retain Mobile
Retain Social

SMTP vs Integrated Archiving

In the world of email retention and discovery, message fidelity is an important topic. Organizations, legal experts, and courts want to ensure that the archived version of a message contains the best representation of the original.

SMTP and Integrated Archiving at a Glance:

- **SMTP:**
  Internet email is received by the archiving system and then sent along to the destination, while outgoing customer email is relayed off this same SMTP server or journaling rules are created inside the email server and the resulting journal reports are automatically forwarded via SMTP to the archiving solution.
- **Integrated Archiving:**
  This approach actively connects to and archives individual mailboxes.

Getting the best representation includes not only preserving the message contents of an email, but also the metadata, such as the sender and recipient addresses, subject line, header information, the date and time the message was sent and received, the date and time the email was read, the folder in which the email was filed, and the category that was applied to the email. This metadata, which is extensive, can be as important as the content of the email itself. Being able to prove that an email was actually read sometimes trumps the fact that the user merely received it in his or her mailbox. As we will discuss, being able to capture all of this metadata, and ensuring the highest degree of message fidelity, is a function of the archiving methodology.

Two different archiving methodologies have become dominant in today's marketplace: SMTP or gateway archiving and Integrated or Mailbox archiving. They differ significantly in their approach and implementation. With this high level understanding of the differences between the two approaches, here are the key areas in which SMTP archiving falls short and integrated archiving excels.

SMTP Archiving

Simply stated, an SMTP-based archiving system intends for its customers to send the email to the archiving system via the SMTP protocol. This is typically accomplished in one of two ways. The simplest way is to place this SMTP archive in front of the customers email system. In this scenario, Internet email is received by the archiving system and then sent along to the destination, while outgoing customer email is relayed off this same SMTP server. The second method involves using the Journaling feature of the email server. To implement this method, journaling rules are created inside the email server and the resulting journal reports are automatically forwarded via SMTP to the archiving solution.

Integrated Archiving

While an SMTP archiving system waits for a messaging system to send it emails, an integrated archiving system actively connects to and archives individual mailboxes. The exact method used varies on the messaging platform. For example, Exchange server archiving involves using the EWS (Exchange Web Services) protocol to connect to and securely archive messages at rest inside the individual mailboxes.

The Difference

With this high level understanding of the differences between the two approaches, here are the key areas in which SMTP archiving falls short.

Folder structure. Since SMTP archiving relies on emails being either automatically forwarded or caught before they are delivered to the recipient, there is no understanding of which folder the end user sorted the email. This is a key piece of metadata, especially if end users desire access to the archives themselves. Typically, an end user will search for an email by browsing the folder structure.

Headers. Some SMTP archiving systems, such as Symantec Enterprise Vault, do not capture these key pieces of metadata. The Headers are desired by forensic specialists because they contain the addressing information and routing information of all the servers that the email passed through before being delivered.

Timestamps. Since the typical SMTP archiving system archives the emails before they were actually delivered to the end users' mailbox, there is no record of the date and time the email was actually received. Even worse, there is no record of when the email was read. This is key to many investigations that must prove whether or not a piece of email was read. There is no way to do this other than retrieving the emails directly from the end user mailbox.

Junk mail. By definition, archiving at the gateway, means that every single email that is destined for a certain email address will be archived. This includes all the spam as well. By archiving mailboxes after the email has been delivered, sorted and categorized by end users, the spam that would have been archived by the SMTP system has already been removed.

SMTP is not secure. The SMTP protocol was first defined in 1982. Although it has gone through revisions, it has never been redesigned. In 1982, there was no conception of malicious behavior online, and everyone was trusted. As a result the SMTP protocol suffers from some security issues. One such issue is encryption. While extensions have been added to SMTP to encrypt the message contents, a lot of the valuable metadata is still sent in the clear and is vulnerable to interception and loss of privacy. Another related issue is how easily SMTP servers can be exploited to send spam. SMTP does not use the same PKI infrastructure of HTTPS that can guarantee the proper authentication of connections. As a result, spammers have historically used impersonation techniques or flat out compromised the identity of legitimate users to send spam emails on their behalf. The issue was so widespread that network operators today typically block outgoing TCP port 25 connections on many consumer networks. This could break an archiving system's ability to receive messages from a user's mobile device or mobile computer that is using a network which blocks SMTP traffic. Furthermore, since SMTP archiving systems wait for data to be sent to them, the possibility exists for a bad actor to poison the archive by injecting false emails over an SMTP connection.

Summary

It's all in the metadata. This portion of an email is easily overlooked but it can be as important as the message body itself. Being able to preserve as much of the metadata as possible and being able to preserve the state of the email as it was last touched by the end user is essential for compliance and eDiscovery. Being able to accomplish all this is only possible when employing an archiving system that is able to read the data as it is inside the messaging system.

RETAIN UNIFIED ARCHIVING

Micro Focus® Retain™ Unified Archiving provides unified archiving of all business communication, including email, social media, and mobile communication data for case assessment, search, and, eDiscovery. It can be deployed on-premises or in the cloud. This includes email archiving for Microsoft Exchange, Office 365, Gmail, IBM Notes, Bloomberg, and Micro Focus GroupWise® platforms, and instant messaging archiving for Skype for Business. Retain Mobile archives mobile device communication data for Android, BlackBerry, and iOS, including SMS/text messages, BBM Messages, BBM Enterprise, phone call logs, and PIN Messages. Retain Social provides monitoring and data insight into message context and tone of all posts for Facebook, Twitter, YouTube, LinkedIn, Instagram, Vimeo, Flickr, Pinterest, and Google+ (on and off network).

www.microfocus.com

Micro Focus
UK Headquarters
United Kingdom
+44 (0) 1635 565200

U.S. Headquarters
Rockville, Maryland
301 838 5000
877 772 4450

Additional contact information and office locations:
www.microfocus.com