globalscape™
securely connected

Whitepaper

Reducing the Costs and Risks of Email Attachments

How Strategic Secure Managed File Transfer Adds Value and Drives Business

According to a survey by the Radicati Group, the typical corporate email user sends 40 messages a day and receives 100 each day—24 of which have attachments.

[Source: Radicati, Survey: Corporate Email, 2011-2012]

Email is the main collaboration and communications tool in most businesses today. When users want to share files internally or with customers, partners, and others outside the businesses, they typically use email attachments.

But the pervasive use of email attachments is a problem for many enterprises for two primary reasons:

> *Email Storage and Bandwidth*
Attachments are typically much larger than the messages themselves, clogging bandwidth, and consuming a disproportionate amount of space on email servers.

> *Security and Compliance:*
Sensitive files can leave your network without any visibility or control as email attachments. This can endanger compliance with the many regulations that require audit trails for regulated data and communications.

This paper discusses how companies can address each of these problems by transparently using secure file transfer technology for email attachments and describes how the Mail Express™ solution from Globalscape® addresses the specific problems of security/compliance and mail attachment costs.

Sending and Storing all of Those Attachments is Costly

If a sender copies five people on an email with a 1MB attachment, they're sending five copies of that attachment within or outside their network, which increases network traffic and consumes significant storage space on email servers where storage is always at a premium.

As the typical file size continues to grow, and as emails are retained longer for compliance purposes, the storage consumed by all of these attachments also grows. IT must continue to store, manage, back up, and protect the ever growing mass of email data.

IT organizations might offer employees alternatives, such as:

> Creating FTP accounts for ad hoc, one-off file transfers
> Educating and training users on secure, cost-effective alternatives for file transfers
> Enforcing and answering questions about email storage limitations

Each of these strategies requires an investment in IT resources, and potentially has hidden costs in lost employee productivity.

Limiting Attachment Sizes isn't an Answer

Some organizations limit attachment size to alleviate this problem. When employees need to transfer larger files, they look for other methods, which may include:

- Using personal email accounts on Yahoo, Gmail, Hotmail, or other services, which are unlikely to have the same password security as internal email servers
- Copying files to USB devices and sending them to the recipient
- Using other web services outside of IT control to transfer files
- Requesting IT's help for using an FTP server

Some of these methods (such as using personal, potentially insecure email accounts) can expose your enterprise to risk. So how do you manage security and compliance?

Attachments Aren't Tracked and Audited

One of the problems with the status quo of email attachments is the lack of centralized control over file transfers happening within the organization and with partners and customers. IT organizations can set policies regarding attachments and security, but it's up to individuals to adhere to those policies.

If files contain data that is subject to privacy regulations or other industry regulations, then you need to track and audit access to those files. Ideally, you'd like to ensure that only the intended recipient receives the file. The lack of visibility into email attachments creates a glaring hole in security and compliance measures.

But People are Attached to Attachments

Despite these problems, the email attachment isn't going away as a way of doing business. It's very easy to simply attach a file to an email; email is pervasive, and people don't easily change their daily patterns.

The challenge is to better manage email attachments without getting in the way of employees who are collaborating and simply doing their jobs. If you want people to use a more secure file transfer mechanism, you need to make it as easy and transparent as what they're already doing. If it isn't, you're fighting an uphill battle.

Replacing Email Attachments with Secure File Transfers

Using Globalscape Mail Express, IT can take control of the email attachment problem without interfering with employee productivity or file sharing.

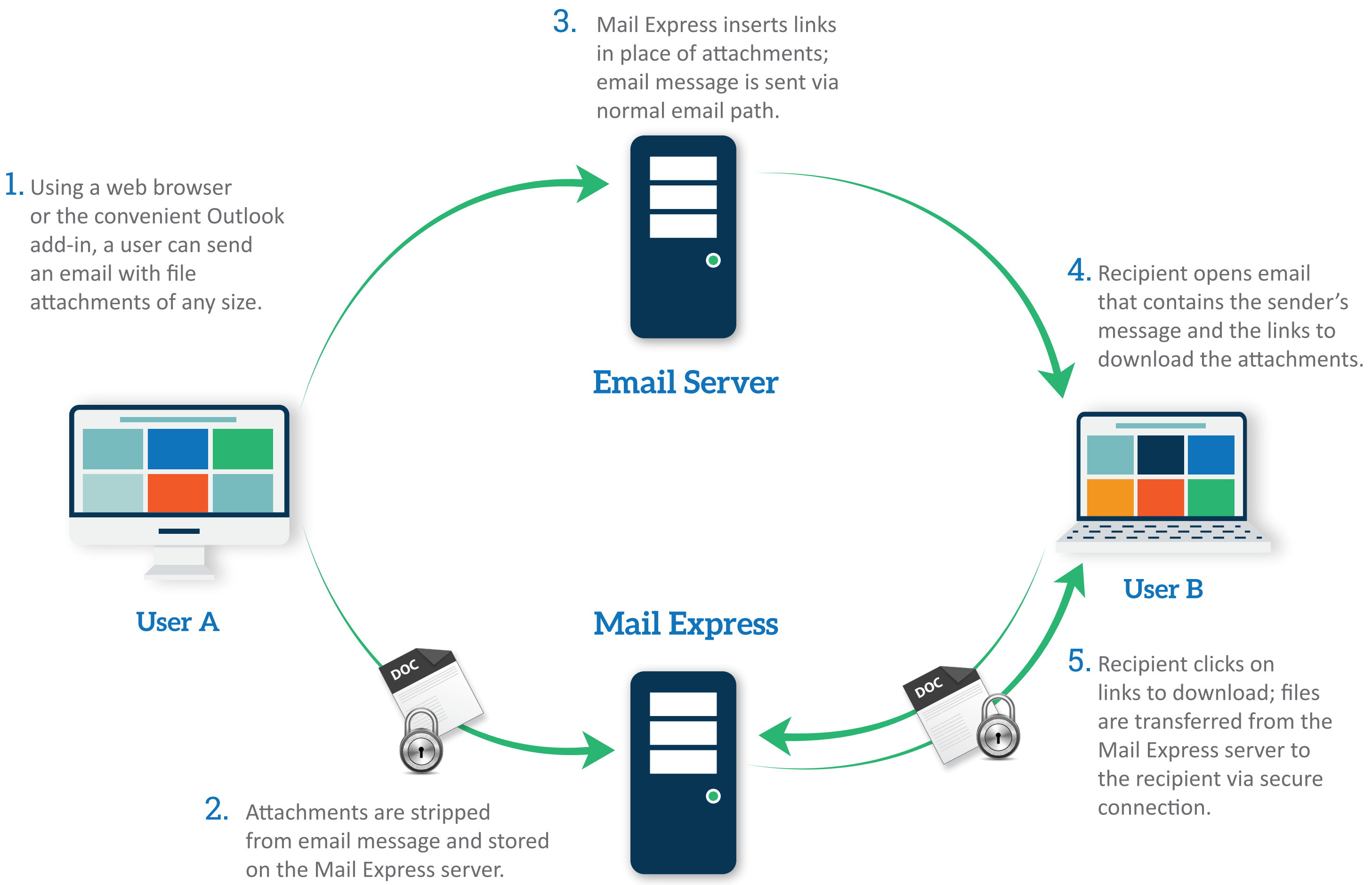
Globalscape Mail Express replaces email attachments with secure file transfer, while maintaining the mechanics of the email attachment from the sender's perspective. Available as a Microsoft Outlook add-in as well as a secure web portal, Mail Express lets individuals keep sending attachments as they always have, while adding audit/reporting, policy-based control, and efficient behind-the-scenes storage.

Mail Express secures the entire file exchange process in both directions; recipients can send files back to the sender from outside the company using an external-facing web portal. This ensures secure communications and tracking from the outside in.

How Mail Express™ Works

When a user attaches an email using the Mail Express Outlook add-in, Mail Express automatically examines the attachment. Depending on the rules that the business has established for email attachments, it transparently removes the attachment from the email and stores it on the secure Mail Express server. It then replaces the attachment in the email with a link to the file on the Mail Express server.

Mail Express then notifies the sender when the file is downloaded and tracks/audits all file access. IT can set policies for which attachments are managed and how long links remain active. IT can also monitor and report on which files are leaving the enterprise.



1. Using a web browser or the convenient Outlook add-in, a user can send an email with file attachments of any size.

2. Attachments are stripped from email message and stored on the Mail Express server.

3. Mail Express inserts links in place of attachments; email message is sent via normal email path.

4. Recipient opens email that contains the sender's message and the links to download the attachments.

5. Recipient clicks on links to download; files are transferred from the Mail Express server to the recipient via secure connection.

For employees that do not use Outlook, Mail Express offers a web portal where internal users can create emails and attach files using a web browser, with the same tracking and auditing features and business rules.

The power of Mail Express is that it fits easily, even transparently, into existing practices for employees.

> *From the Sender's Perspective:*
Employees using Outlook just keep doing what they're already doing, except that they don't have to find alternative means to send large files. Senders can add extra layers of security to the file, such as requiring a password for access. And, unlike regular attachments, the sender receives a notification when the recipient downloads the file.

> *From the Recipient's Perspective:*
Rather than an attachment, the recipient receives a link to the file within the email, thus freeing up his allotted email storage space. By simply clicking the link, they can download the file when it is most convenient for them. (The expiration date of the link, if specified, is included in the email.)

No one has to attend training on how to use Mail Express and, because it fits seamlessly into existing ways of working, Mail Express adoption is rapid and thorough.

Policy-Based Control Over Attachments

Mail Express adds a new layer of control and visibility for IT and security/compliance officers. First, organizations can define the rules by which attachments are managed by Mail Express (and hence secure file transfer), according to:

> File type (e.g., PDF, DOC, GIF)
> File size (aggregate of all files attached to the email)
> Number of attachments allowed per email

In addition, organizations can set the default expiration period for link availability. Note that link expiration can (and should) be distinct from file retention policies. That is, the link for accessing the file may expire while the file itself is retained.

Better Security for Sending and Receiving Files

Using secure file transfer instead of email attachments reduces the risk of information being intercepted or misappropriated.

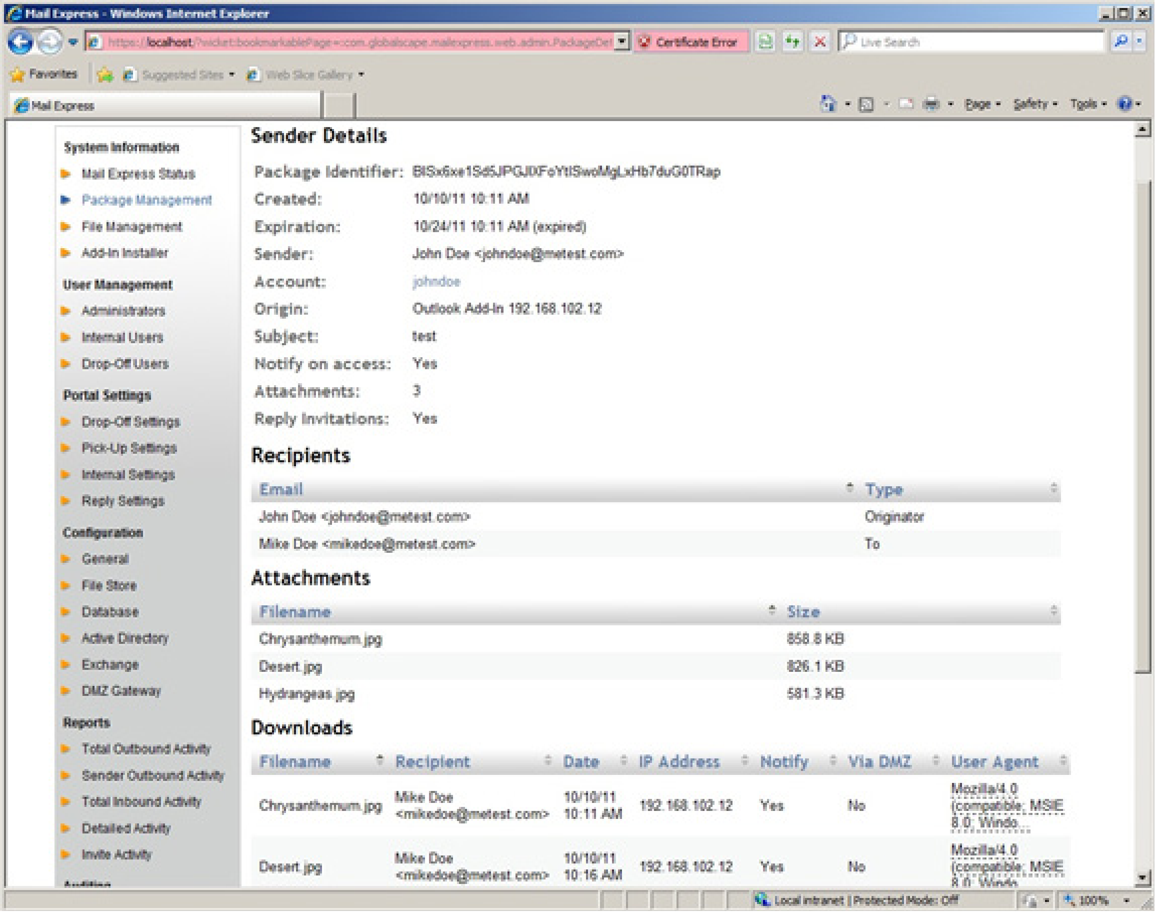
> Files are uploaded and downloaded from the Mail Express server using HTTPS, replacing potentially insecure email paths.
> For sensitive files, the sender can add a password to the file which the recipient then provides when they download the file
> Links expire after a defined time period: the sender can explicitly set a shorter expiration period if they choose.
> Recipients outside of the organization can use Mail Express's Drop-Off portal to return files to the sender, reducing the use of unapproved or insecure file transfer methods, and providing the same level of audit/tracking as outbound transfers. This method provides secure file exchange with partners.

Globalscape offers an optional DMZ Gateway module, which resides in the DMZ and offers secure communication with the Mail Express Server behind intranet firewalls. Using this approach, no sensitive data is stored in the DMZ.

Audit Trails and Reports for Compliance

For regulatory compliance purposes, organizations need to monitor and review email attachments for policy compliance. When called upon in an audit, they may need to respond to requests for information by searching email attachments and demonstrating compliance.

Mail Express helps with both of these compliance tasks. For each email attachment, it automatically tracks information about the sender, the recipient, the file, and access to the file on the Mail Express server.



Sender Details

Package Identifier: BISx6xe1Sd5JPGJIXFoYtISwoMgLxHb7duG0TRap
Created: 10/10/11 10:11 AM
Expiration: 10/24/11 10:11 AM (expired)
Sender: John Doe <johndoe@metest.com>
Account: johndoe
Origin: Outlook Add-In 192.168.102.12
Subject: test
Notify on access: Yes
Attachments: 3
Reply Invitations: Yes

Recipients

Email	Type
John Doe <johndoe@metest.com>	Originator
Mike Doe <mikedoe@metest.com>	To

Attachments

Filename	Size
Chrysanthemum.jpg	858.8 KB
Desert.jpg	826.1 KB
Hydrangeas.jpg	581.3 KB

Downloads

Filename	Recipient	Date	IP Address	Notify	Via DMZ	User Agent
Chrysanthemum.jpg	Mike Doe <mikedoe@metest.com>	10/10/11 10:11 AM	192.168.102.12	Yes	No	Mozilla/4.0 (compatible; MSIE 8.0; Windo...
Desert.jpg	Mike Doe <mikedoe@metest.com>	10/10/11 10:16 AM	192.168.102.12	Yes	No	Mozilla/4.0 (compatible; MSIE 8.0; Windo

Sample Detailed Report

Compliance and security teams can monitor outbound (and inbound) file transfer activities, drilling down to specific transfers, as needed. And, in response to audit requests, they can generate reports by file type, time period, and/or sender.

Using Mail Express also reduces email storage costs by reducing the number of attachments stored on email servers.

Summary

Email messages are a primary means for file exchange in the business world; however, email attachments have outgrown traditional email software. With growing file sizes, increased online collaboration, and escalating privacy and security concerns, businesses need more visibility and control into the files leaving their organizations. Globalscape Mail Express solves the email problems for businesses without interfering with productivity for employees.

> Employees can continue using basic attachment techniques to send large files of unlimited size. And they can see when the recipient actually downloads the file they have sent.

> IT organizations can reduce the cost of storing many copies of attachments on already overloaded email servers.

> Security and compliance officers can easily track and audit files leaving the organization. Email is no longer an open window through which regulated or sensitive data can leave the enterprise undetected.

About Globalscape

Globalscape ensures the reliability of mission-critical operations by securing sensitive data and intellectual property. Globalscape's suite of solutions features EFT Server, the industry-leading enterprise file transfer solution that delivers military-grade security and a customizable platform for achieving best in class control and visibility of data in motion or at rest, across multiple locations. Founded in 1996, Globalscape is a leading enterprise solution provider of secure information exchange software and services to thousands of customers, including global enterprises, governments and small businesses.