In today's business environment, ensuring data security has become a priority. Recent surveys show that a corporation has a 26% likelihood of experiencing a major data breach within any given 24-month timeframe[1]. And it may come as a surprise to know that careless management and employee practices are the cause of most security breaches — even more than criminal or malicious attacks. The consequences of a security breach for a corporation can be both financial and reputational, and can ultimately lead to a lack of trust in its brand.

If you exchange sensitive, confidential or mission-critical information with customers and partners, and use unsecure communication technologies such as emails, FTP servers, Enterprise File Synch and Share solutions without providing proper protection and a rigorous compliance strategy, you may be running serious and unnecessary risks.

DO YOU USE ANY OF THESE UNSECURE METHODS FOR EXCHANGING SENSITIVE INFORMATION?

Email

Email was not designed with privacy or security standards in mind. Emails are transmitted in clear text over the Internet and are stored in multiple locations with many service providers, which exponentially increases hacking possibilities.

Password-protected zip files

Numerous free tools and tutorials exist that make cracking passwords on zip files in mere minutes an easy task.

Sending two separate email messages

Often, a person will send an email that contains sensitive information and a second email that contains complementary sensitive information. This practice is not in any way secure. Anyone who has gained access to an inbox has access to both the first and second emails.

Uploading files to an FTP server

Many corporate email systems and Internet Providers prevent the exchange of large files. As a result, employees often turn to standard FTP servers or file sharing services. These solutions do not protect sensitive data, and can be complicated to use.

Sending CDs, DVDs or USB keys by mail or courier

Sending data by mail or courier is actually one of the most dangerous methods for sharing sensitive data and could also become expensive. The potential for the package containing the data to get lost or stolen is significant. trail of all communications.

[1] Source : Ponemon Institute LLC, 2016

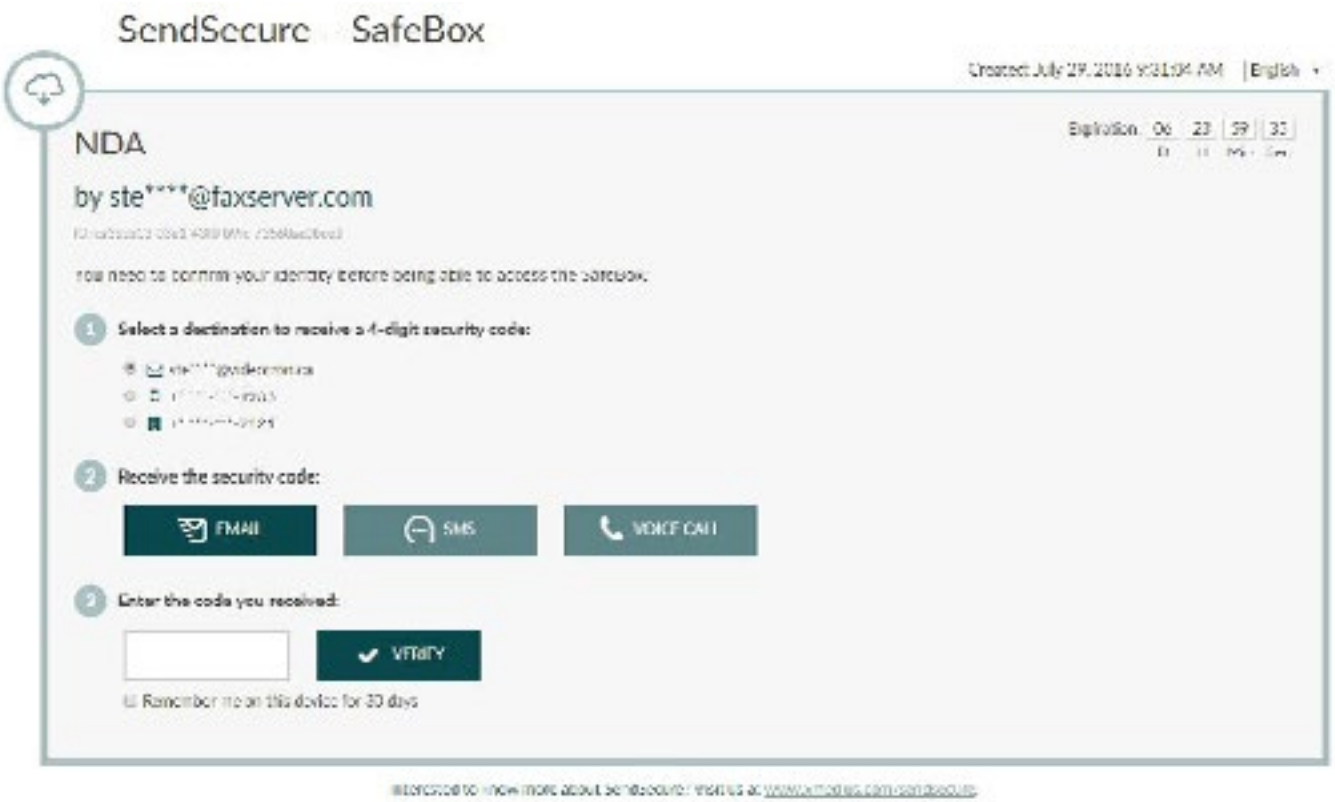
WHAT IS THE XMediusSENDSECURE ON-PREMISES SOLUTION?

SendSecure is a state-of-the-art file exchange platform that is both highly secure and simple to use. It is expressly designed to allow for the safe exchange and ephemeral storage of sensitive files in a virtual SafeBox. Any files exchanged are encrypted in both the upload and download processes. Furthermore, SendSecure requires authentication from the sender, and double authentication for the recipient. Finally, it automatically purges old files based on a retention policy that is customized when the ephemeral SafeBox is created and provides an audit trail of all communications.

SendSecure was initially only available as a cloud-based service for cloud deployment applications. This required no onsite hardware equipment as it resides in Amazon Web Services (AWS), one of the most secure server infrastructures in the world.

In an ongoing effort to offer flexible deployment options, XMedius now offers SendSecure On-Premises. It is an ideal solution for organizations that:

- Want to maintain control over data location and ownership
- Want a fast, seamless deployment
- Are looking for a highly secure file exchange alternative to their telecom infrastructure



Highly Secure

- ### Secure Links

  A secure link is a URL that can be distributed to anyone to initiate a SafeBox for secure inbound generated exchanges of files and messages.

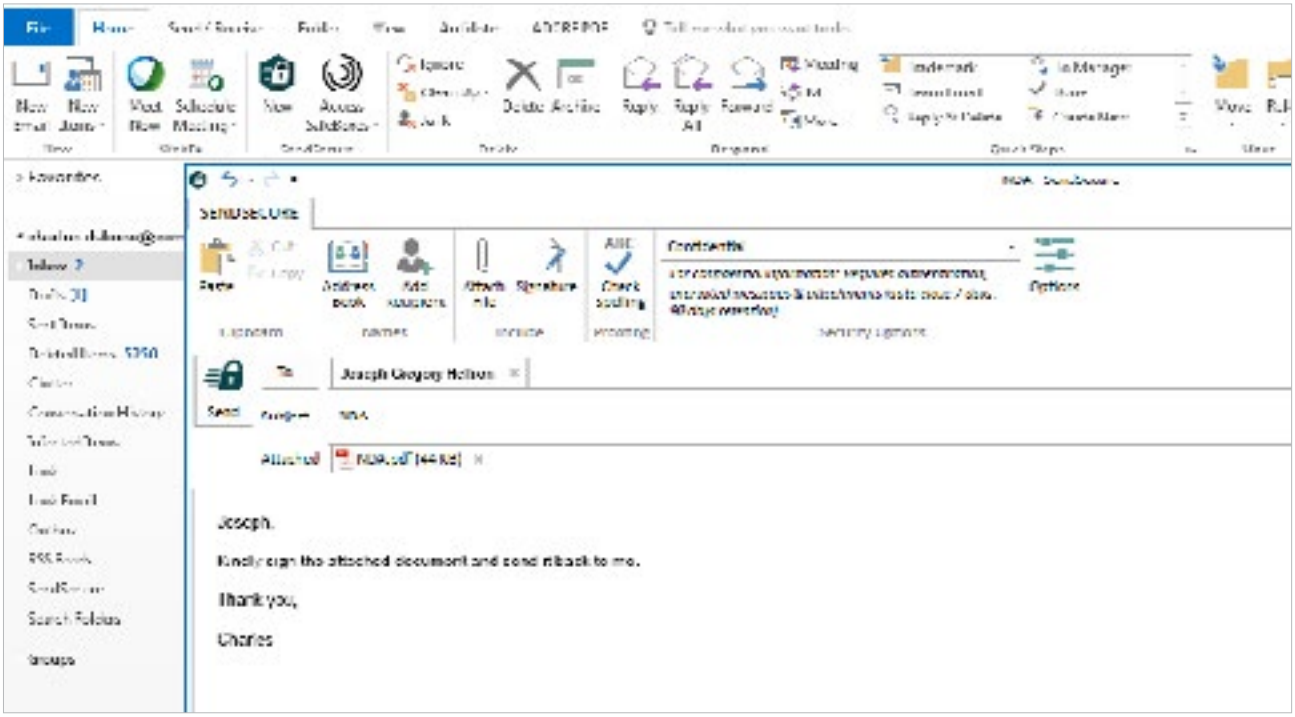
  - Administrators can initiate and distribute multiple enterprise secure links
  - Individual users can create their own (singular) secure link

- ### Two-Factor Authentication (2FA)

  Once the sender has created the SafeBox, the recipient receives an email with the download link, at which point he must input a secondary one-time code (2 factor authentication), which is received via either an SMS, a voice call or an email.

- ### Strong Encryption

  SendSecure uses encryption methods recommended by banking and security experts. All communications are encrypted using TLS 1.2 (with forward secrecy). At rest, all files are encrypted using AES 256-bit encryption.



- Double Encryption

  SendSecure protects the SafeBox from intruders or unauthorized employees by double encryption. One of the two required keys used to decrypt the SafeBox content must be provided by the sender or the recipient before accessing its content.

- Built-in Antivirus Protection

  As an additional security layer, files being uploaded to a SafeBox will automatically be scanned for potential threats. If a virus is detected within a file, it won't be added to a SafeBox.

- Ephemeral SafeBox

  SendSecure allows you to customise the lifespan of a SafeBox. Once that lifespan expires, all files in the SafeBox are deleted and no longer accessible by any party. The sender can also terminate a SafeBox at any time and select the level of security.

Simple to Use

- Superior User Experience

  SendSecure's intuitive design makes it as easy to use as sending an email. In addition, the recipient does not require a subscription, nor are any hardware or software downloads necessary. All you need to use SendSecure is a communication device—such as computer, mobile phone or tablet--and a web browser. Its elegantly simple design means that employee training is no longer an issue, and adopting SendSecure as the solution of choice is effortless.

- Simple Integration

  SendSecure's seamless integration with Outlook (Office 365) lets you send small or large files of all types directly from Outlook without having to open another application. Users can also send secure encrypted files both large and small from a mobile phone or tablet to individuals or groups with a web browser.

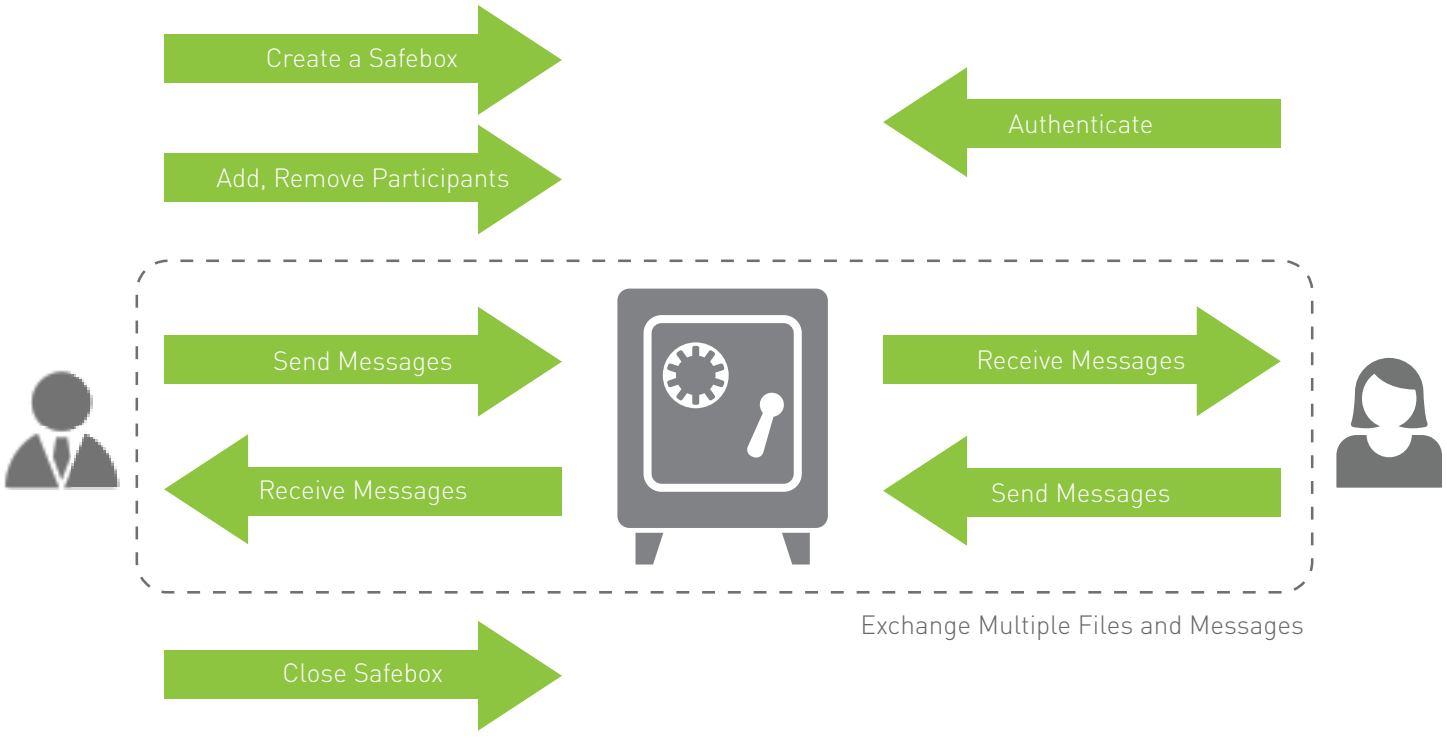
- 32-bit and 64-bit Support

  The SendSecure Outlook add-in is compatible with both the 32-bit and 64-bit versions of Microsoft Outlook 2010, 2013, and 2016.

  - Additional Language Support: Users can set their default language as well as choose from 6 languages (EN, FR, DE, SP, IT, PT) that SendSecure will use to notify recipients of a message.
  - Upload progress bars: Users can see the displayed percentages of completed bytes per file when sending a message to SendSecure.
  - Users have the option to enable/disable the message summary saved in Sent Items, and can also choose whether or not to include the double encryption key in this summary.

- A True Mobile Solution

  SendSecure enables authorized users to exchange files of any size securely from any business or personal device (including smartphones and tablets) whether at the office or on the road. As a result, it's a superior productivity tool.



- No File Limitations/Large File Support

  SendSecure allows the exchange of any type of file (text, image, audio & video) of up to 5 TB/message as well as an unlimited number of messages per month. Most email servers limit file attachments to less than 10 MB.

- Collaborative Work

  SendSecure enables file recipient to participate in a two-way conversation in addition to receiving a secured document transmission. This collaborative feature is enabled by simply clicking on the "Reply" button.

- Manage Participants

  SendSecure lets you easily recall and delete a message and file before your recipient sees it. Moreover, it allows you to invite additional recipients to the exchange while a conversation is taking place.

- Security Profile Per User/Group

  SendSecure gives administrators the flexibility to assign specific security profiles to a particular user or department within their organization. This allows administrators to predetermine higher or lower security and accessibility settings for profiles on a per department basis.

- Restrict file size

  Enterprises can set the limit of file sizes for files uploaded to a SafeBox to help manage bandwidth. Users will receive a notification message when a file can't be uploaded if it exceeds the permitted file size settings.

Audit Trail

- Proof of Delivery

  SendSecure retains digitally signed transmission records of any and all access to a SafeBox. It automatically sends emails to the sender confirming all actions performed by the recipient during the different steps of the process. A Transmission Detail Report is created following the closing of the SafeBox and this report can be printed, downloaded or emailed as a PDF.

- Archiving

  SendSecure can archive all documents that were exchanged on the platform or to an external repository or drive.

WHY ADOPT XMediusSENDSECURE?

Protect Disclosure, Minimize Reputational Risk

Over the last few years many organizations have seen sensitive internal information stolen, lost or purposely leaked. Their reputations and brands may have suffered extensive damage that is impossible to value and may have negative impacts for years to come. SendSecure helps to minimize these risks.

Limit Possible Litigation and Fines

Certain industry regulations – such as Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (SOX), the Gramm-Leach-Bliley Act, etc. – require companies to keep private information safe. SendSecure meets the highest Compliance Standards. The XMedius platform is also certified ISO/IEC 27001:2013. This certification provides independent assurance that XMedius' employees operating the XMedius SendSecure can effectively run a comprehensive security program and manage information security risks.

AN ENTERPRISE GRADE SOLUTION

White Label

SendSecure service can be provided under the XMedius brand, or can be customized to fit a unique brand and identity (white label).

Administration and Reporting

SendSecure administrators can use the secure web-based interface to manage users, generate reports and more.

Worldwide Coverage

Languages supported for customer interactions (emails, user interface, PDF reports) include English, French, German, Spanish, Italian, and Portugese.

WHO SHOULD USE XMediusSENDSECURE?

Healthcare

Medical professionals and institutions--including doctors, nurses, administrators, clinics and hospitals can use SendSecure to:

- Securely send messages, medical records and files to patients, insurance companies, clinical research, etc.
- Share MRI, CT scan, and other large diagnostic files between physicians and patients

Finance

Frequently, clients of financial institutions are limited to using the electronic communications systems that the financial institutions have available. These systems often require software downloads or account creation. Worse yet, documents cannot always be returned using the same system.

Banking

- Ease the workload of loan officers who need to sign banking documents with customers
- Ensure that legal documents are kept confidential when working with regulators, outside legal counsel, or business partners
- Secure the communications of executive teams who need to share information with their Boards of Directors, one another, outside counsel, and regulatory agencies

Mortgage Companies or Brokers

- Help loan officers who need to send or receive sensitive documents
- Facilitate the workflow of departments that need to receive documents from appraisers, title companies, government entities, banks and other outside parties

Insurance Companies and Brokers

- Assists with the exchanging of information for insurance claims
- Facilitates receiving detailed building plans or other pertinent data to provide accurate quotations to customers

Legal

Lawyers deal regularly with confidential client information and have an obligation to protect that information from being intercepted, either accidentally or deliberately.

Common uses for SendSecure include:

- Sending contracts to other lawyers inside and outside of their firms
- Sending sensitive messages and files to personal and business clients
- Using Delivery Confirmation to prove that recipients received and opened secure messages

Government agencies

Government agencies deal with large amounts of sensitive personal data from citizens that must be protected.

- Securely communicate social security numbers
- Exchange Tax report information without risk

Distributor/Reseller:

XMedius

info@xmedius.com
Americas: 1-888-766-1668
EMEA: +33 1 70 92 13 10
XMEDIUS.COM