TOSHIBA Strategic Alliance Program

PREMIER PARTNER

opentext™ | XM SendSecure™

- Streamlines workflows by securely sending any file, in sizes up to 5TB, as easily as sending an email
- Increases security through encryption, 2-factor authentication, virus scanning and ephemeral storage
- Facilitates compliance with key regulations—HIPAA, GDPR, FERPA, PCI DSS, SOX, etc.
- Simplifies communications of sensitive data with outside organizations through fast, intuitive, and secure messages that don't require special training

Data security has become a critical priority in business, healthcare, education, and government. Research shows that a corporation has a significant likelihood of experiencing a major data breach. The expansion of privacy regulations means that the risks aren't just of data theft and lost revenue, but also government-levied fines. Organizations need a solution that is powerful and secure, but doesn't hamper staff's ability to work efficiently.

Secure file exchange is the future of document communications, but many solutions on the market introduce significant hurdles to efficiency. OpenText™ XM SendSecure™ has been designed to balance high security with extreme accessibility and ease of use. It is adaptable to any industry because it allows transfers of files in any format, each up to 5TB in size.

BENEFITS

STREAMLINES WORKFLOWS

XM SendSecure makes securely sending files as easy as sending an email. The solution can be used on computers (including via Outlook integration, web client, and APIs), mobile devices (with purpose-built apps for iOS and Android) and with connectors to some MFPs. This ensures employees can send and receive sensitive documents, videos, database files, and more from almost anywhere. Collaborative tools allow teams to share access (when authorized) so the solution can be deployed to shared inboxes like “billing@company.com”.

INCREASES SECURITY

Files sent through XM SendSecure are protected with encryption in transit and at rest (including optional double-encryption), 2-factor authentication (via phone call, SMS text message, or email), and automatic virus scanning. Files are uploaded and downloaded from an encrypted virtual safe called a SafeBox. SafeBoxes are ephemeral storage, meaning that they are automatically deleted after a user or administrator-set period of time. This ensures they cannot be discovered later by unauthorized people (a common concern with file exchange solutions).

FACILITATES COMPLIANCE

XM SendSecure has been designed from the ground up for compliance with key privacy and industry regulations—HIPAA, GDPR, FERPA, PCI DSS, SOX, etc. All uploads and downloads to SafeBoxes are tracked to the last byte. When the SafeBox closes, a full record is automatically generated and sent to the owner for audit & compliance purposes.

XM SendSecure can be deployed either on-premises or in ISO/IEC 27001:2013 and PCI DSS certified clouds hosted in the US, Canada, or EU to ensure your organization’s data sovereignty requirements are met.

SIMPLIFIES COMMUNICATION

A major challenge with secure file exchange systems is their tendency to be overcomplicated. Because each transfer is a two-sided transaction, the right solution needs to be easy for the intended outside recipients to access. XM SendSecure does not require that recipients (partners, customers, etc.) create an account, and is intuitively designed so they do not need special training or troubleshooting. If outside customers or organizations want to send you files securely, they can do so as guests on your account via easily-shareable links.

XM SendSecure provides the essential security organizations need for communicating sensitive data without introducing new barriers or workflow inefficiencies. The solution is fast, cost-effective, and intuitively designed. It can be used to exchange billing information, medical imaging, contracts, financial reports, evidence videos, prototyping information, and just about anything else. Whatever your organization does, it’s likely there’s a place for XM SendSecure in your processes.

Simple to use

FEATURES

ENCRYPTION IN TRANSIT AND AT REST

All files are encrypted during uploads and downloads, as well as when stored in the SafeBox. For extra security, optional double-encryption can be enabled.

2-FACTOR AUTHENTICATION

SafeBox invitations are sent via email, with 2nd authentication credentials sent separately via either SMS text message, automated phone call, or email. Which method is used can be set by users or locked-in by administrators via customizable security profiles.

EPHEMERAL STORAGE

File sharing solutions upload copies of sensitive files to servers. If those files are then forgotten about, they can be a serious security liability. Ephemeral SafeBoxes do not continue to exist after they've outlived their usefulness. At time of creation, each box has a ticking timer (length controlled by the user or locked-in by administrators). When that timer ends, the SafeBox deletes itself and sends a record of all transactions to the originating user.

EXTENSIVE AUDIT TRAIL

All interactions within a SafeBox are tracked—uploads and downloads are both reported with the level of success or failure of the transfer down to the last byte. This makes it extremely easy for organizations to know who accessed what data when during later audits (security, regulation compliance, etc.).

Figure 1—Outlook Integration

EASY TO USE, INTUITIVE DESIGN

Many file exchange solutions have overly complex designs that make them slow and difficult to use. XM SendSecure has been designed from the ground up to be as easy to use as email. This not only saves time on staff training but makes the solution more accessible (and thus more likely to be used) for staff at outside organizations.

ACCESSIBLE ANYWHERE

XM SendSecure can be used to send and receive files from any computer (including via an Outlook integration), mobile devices (iOS and Android apps), and some MFPs (via connectors). This means staff can work anywhere they have an internet connection.

COLLABORATION FUNCTIONALITY

XM SendSecure allows access to specific SafeBoxes to be shared across authorized accounts. This enables easier teamwork within the secure environment (including encrypted chat), including using SendSecure with shared inboxes like "billing@companyname".

SECURE HOSTING

SendSecure is available hosted on-premises or via cloud data centers in the US, Canada, or the EU to suit your security strategy and data sovereignty requirements. SendSecure cloud hosting is ISO/IEC 27001:2013 and PCI DSS certified.

AUTOMATIC VIRUS SCANNING

All files uploaded to SafeBoxes are automatically scanned for viruses.

OPENTEXT XM SENDSECURE

Figure 2—Mobile App

Figure 3—Web Client

Copyright ©2022 Toshiba America Business Solutions, Inc. Electronic Imaging Division