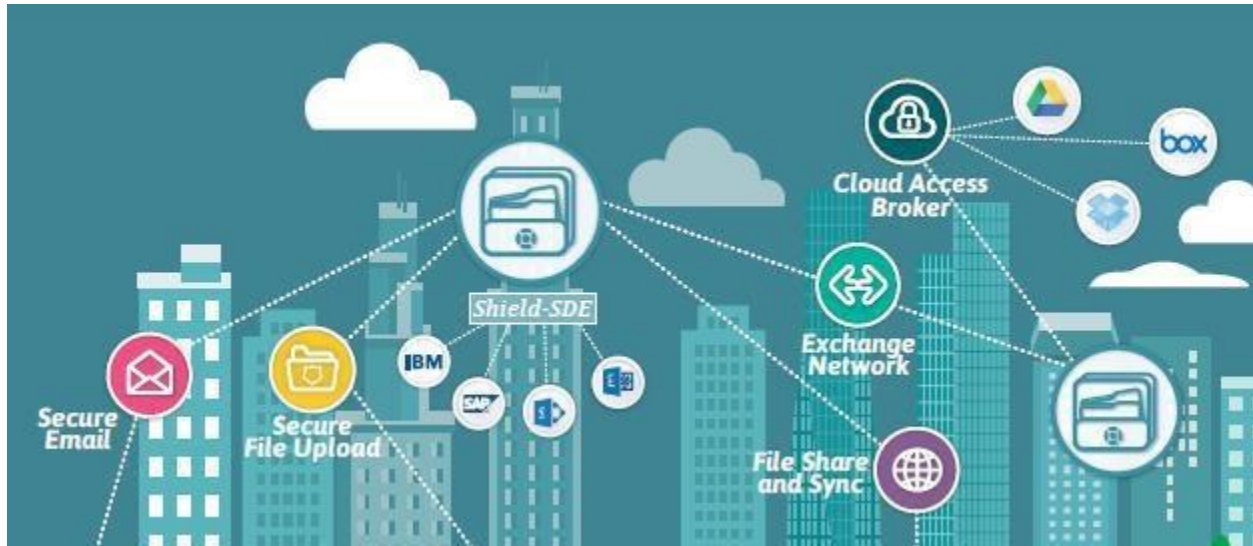# Shield-SDE: Secure Data Exchange Broker

Data Sheet

The High Cost of Uncontrolled Data Exchange

Many businesses do not effectively control or monitor their sensitive and valuable business communications and file transfers. This creates the risk that either confidential information will fall into the wrong hands or that data infected with a malware will enter the business. Exposure of confidential information can result in failure to meet regulatory standards (such as HIPAA and PCI DSS), legal action, fines, theft of intellectual property, bad publicity, and loss of strategic customers.

Email is the most common method of exchanging data between users, business partners and customers. More than 100 billion business emails are sent and received daily. Business users also transfer files using a variety of other methods including FTP and cloud storage solutions such as Box.com, Dropbox, Google Drive and OneDrive.

Confidential files such as financial data, medical records, tax returns, human resources data, intellectual property, and medical images are uploaded and exchanged within and external to government and company offices – in the majority of cases with almost no security.

Although not all messages and transferred files are strictly confidential, statistics show that almost 40 percent of business users have violated company rules by maliciously or inadvertently sharing sensitive

data using email or other file transfer methods. This means that many organizations today are unknowingly in breach of regulations and are potentially at risk of large liability claims due to sensitive data leakage.

Overview: Shield-SDE Platform

Shield-SDE enables organizations to broker, control, and secure data exchange of any type and size between people, applications, cloud solutions, and businesses. Built on the industry's widest range of pre-configured application and cloud connectors and powered by an automated security policy enforcement engine, Shield-SDE is designed to rapidly add layers of security and control across a wide variety of data exchange patterns for enterprises of all types including to and from the cloud.

Shield-SDE strengthens control of sensitive data exchange at a relatively low cost. Shield-SDE's unique modular architecture and integration capabilities ensure that it seamlessly integrates into legacy data platforms in the enterprise and cloud, providing policy enforcement and secure data transfer.

Multiple Innovative Solutions

Shield-SDE offers multiple innovative solutions to securely grant access and transfer shared data. All solutions provide key "where, what, who, and when" tracking data for each transferred file. These solutions are ideal for B2B and C2B transactions.

	Cloud Access Security Broker Utilize cloud storage and services while maintaining full visibility, governance, and control of all data uploaded and downloaded from the cloud.
	Secure File Sync and Share Secure enterprise collaboration solutions, enabling business users to safely share files from any device (desktop, mobile, web) and from any location.
	Secure Managed File Transfer Securely transfer sensitive files of any type or size into and outside the organization with a user-friendly file upload and FTP replacement solution.
	Secure Data Exchange Network Grant access to securely share and distribute any file type and size securely between remote company branches, to business partners, and customers with an intuitive user-friendly interface.
	Secure Email Send encrypted emails of any size and type to registered or ad-hoc recipients, providing a simple, easy to use, fully auditable alternative to PGP.
	SecureFax Service Send encrypted emails of any size and type to registered or ad-hoc recipients, providing a simple, easy to use, fully auditable alternative to PGP.

Cloud Access Security Broker (CASB) Features and Benefits:

- Shield-SDE integrates with leading consumer cloud storage and SaaS solutions such as DropBox, Box.com, Google Drive, OneDrive, Microsoft SharePoint Online, and Microsoft Azure.
- Secure, govern, and monitor all data exchanged with the cloud.
- Automated security policy enforcement on all cloud exchanged traffic.
- Files are encrypted and require a password to access. Full auditing, tracking, and reporting of all cloud file transfer activities.
- Increases compliance with a range of information security regulations including HIPAA, PCI-DSS, FISMA, GLBA and GDPR.
- Can be deployed on-premises, in the cloud, or hybrid allowing both regulated and non-regulated organizations to benefit from the most secure cloud access broker solution.

Secure File Sync and Share Features and Benefits:

- Secure enterprise file and data collaboration solution.
- Adds security layers to standard file share and file upload solutions including authentication, data scanning and data encryption.
- Share business partner data from any device without the need for a VPN. Secure, control, and monitor shared data in motion and at rest.
- Provide end-to-end governance of shared sensitive data.
- Ensure high adoption of secure data sharing solutions through a simple and natural interface.
- Enterprise Dropbox alternative.

Secure Managed File Transfer Features and Benefits:

- Deploy highly automated and secure file upload solutions.
- Provides an FTP replacement solution.
- Transfer any file type and size securely between remote corporate branches, business partners, and customers.
- Integrate seamlessly with business applications, legacy systems and proprietary tools.
- Increase compliance with a variety of regulations including HIPAA, PCI-DSS etc.
- Enables organizations to maintain comprehensive records of their file transfer and download activities, documenting key tracking data for each transferred file.

Secure Data Exchange Network Features and Benefits:

- Transfer any file type and size securely between remote corporate branches, business partners, and customers.
- Use any of the Shield-SDE connectors to integrate Safe- Box with Microsoft SharePoint, Oracle, IBM, HTTP/S based applications, S/FTP, SQL, NFS, DLP, A/V, and more.
- Applications can easily check-in and check-out sensitive data to / from folders across the network.
- Reduce costs of sensitive data distribution and enhance staff productivity and efficiency. Files placed within a folder in one location can be automatically transferred to a remote location.
- All data shared within the network is scanned using the organization's DLP and anti-virus engines.
- Shield-SDE authenticates each recipient before granting access to shared folders and files, ensuring that only the intended end user is able to view or download the sensitive data. Integration with enterprise applications, storage, and security tools such as Microsoft SharePoint, Oracle, IBM, HTTP/S based applications, S/FTP, SQL, NFS, DLP, A/V, and many more.
- All data shared within the network is scanned using the organization's DLP and anti-virus engines.

Secure Email Features and Benefits:

- Send encrypted emails and file attachments of any size and type to registered or ad-hoc recipients.
- Email recipients do not have to install software or exchange cryptographic keys.
- Secure email can be seamlessly integrated with an Outlook plug-in and web interface.
- Users can click Safe Reply enabling email recipients to send back files of any size securely. Set one-time password for recipient to download secure content.
- Set a limit to the number of file attachment downloads.
- Set an expiration date that prevents recipients from additional file attachment download.
- Sender benefits from detailed tracking information such as time and date of file download.
- PGP replacement solution.
- Client deployment manually using a wizard or unattended installation.

Shield Secure Email Outlook Plug-in
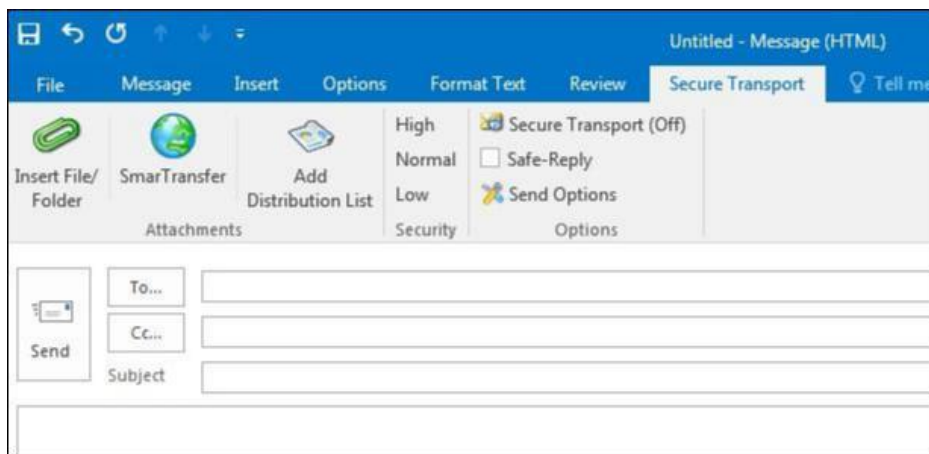
LNK Connector Email

- LNK connector works behind the scenes with no user (i.e. email sender) interaction with the system.
- LNK connector is a SMTP gateway deployed as the next hop email server "before" or "after" the organization's existing mail server.
- Once LNK connector "catches" an email message, it scans the message attributes including the message subject, body, header, attachment type and size; then, based on pre-defined rules, LNK connector performs the required action for example, encrypt, drop, forward, etc.
- Operates with Microsoft Outlook and any other email clients.

Secure Digital Vaults

- Encrypted files are placed in Shield-SDE secure storage. This ensures data is secure at rest until files are downloaded for file sharing or inserted into an email as a file attachment. The files in transit to authenticated recipients are also secured during download by using secure protocols such as HTTPS, FTPS, SFTP and SSH.
- Shield-SDE digital vaults are called: Safe Spaces. A Safe Space contains data from a source transparent to users. A Safe Space can reside on the Shield-SDE server, network file storage location, FTP/SFTP site, or MSSQL database.
- Users may be granted permission to access multiple Safe Spaces that in aggregate host data from various sources transparent to users.
- When a user sends an email with file attachments and sets a secure transport level to High or Normal, the file attachments are not sent by email, instead they are uploaded to a designated Outlook Safe Space from where they will be downloaded securely by the email recipient.

Shield-SDE's SecureFax Service Features and Benefits:

- Send faxes from email (Outlook plugin), web interface or Mobile app
- All fax files (sent and received) are encrypted and placed in Shield-SDE secure storage.
- Simple and secure fax solution that eliminates both administrative overhead and old technology but maintains existing workflows
- Ensures accurate and secure delivery of faxes, while improving workflow and reducing costs
- When a user sends a fax, and file attachments if necessary, they use an address like faxnumber@domain.com (i.e. 17783743219@faxmessage.net). This informs the server it has a fax and not to send it by email. Instead the SecureFax service parses the message and address to obtain the destination number and any attachments. The conversion and processing happens locally on the Shield-SDE server. The fax and its metadata (fax number & accounts details) are transmitted over SFTP to our SecureFax cloud for delivery to the fax recipient.
- Received faxes come into our SecureFax cloud and are delivered to the client's Shield-SDE via SFTP. This maintains compliance while data is in transit and at rest within the Shield-SDE server.

Automated Security Policy Enforcement

- A Shield-SDE administrator can create group policies and procedures for secure data sharing and exchange that can be integrated intuitively into existing work flows.
- Shield-SDE supports more than 100 configurable policy parameters that enable and enforce features. A few examples: Senders must always use a High or Normal security level, safe replies from email recipients are allowed, attachments can be downloaded a limited number of times, attachments cannot be accessed after a certain number of days, emails with attachments more than 2MB must be sent securely.
- The Shield-SDE platform supports integration with industry-leading enterprise security solutions and data scanning engines. A file can be scrubbed by any number of engines. For example: file true type scan, anti-virus, data leak prevention, security sandbox, scrubbing engines, file level permission, user rights management, anti-spam, and any other third-party security solution.

Data Encryption

- Shield-SDE encrypts files in Shared Spaces before they are shared with recipients. Encryption is done using the built-in AES and PDF encryption modules, or by processing the files with third party encryption engines.
- Shield-SDE has an option to encrypt Shared Spaces that prevents the Shield-SDE administrator from being able to decrypt files.
- The Shield-SDE Outlook plug-in has a feature that enables a user to encrypt file attachments within a password protected zip file. The password needs to be exchanged to the recipient when using this feature. In conjunction with security level settings High and Normal a recipient would need to authenticate using a OTP, download the sent file attachments, and then enter a separate password to unlock the encrypted zip wrapper.

User Authentication

- Authentication can be performed as part of configurable policies applied to inbound and outbound data traffic. Shield-SDE supports authentication mechanisms including:
- Active Directory and LDAP authentication.
- A One-Time Password (OTP) sent in a separate email or SMS to an email recipient granting that person access to a message and file attachments.
- SQL-based databases including MYSQL, Oracle, Access.
- CSV/XLS files.
- Open ID / SAML.
- User's authentication for social network such as Facebook, Google+, Live ID.

End User Clients

Shield-SDE supports several user friendly clients including:

- Outlook plug-in.
- Web user interface.
- SmarTransfer desktop client.
- Shield-SDE mobile applications for iOS and Android.

🚩 Tip: The Shield-SDE end user clients are designed to ensure high work-place adoption of all the available solutions.

Path to Secure Information Regulatory Compliance

Shield-SDE has been designed from the ground up with compliance as a top priority, enabling enterprises from various sectors including financial, healthcare and federal institutions, to increase compliance with regulatory requirements such as: HIPAA, PCI-DSS, FISMA, and GLBA & GDPR.

Generate Detailed Reports

Shield-SDE reports key "where, what, who, and when" tracking data for each transferred file. You can generate reports by type such as user, group, policy, Shared Space, packages, and history. Reports can be triggered by events such as login, upload, download, or share files, send email, create or delete file or folder, and more.

Integration With Enterprise Applications

Shield-SDE has dozens of pre-built connectors enabling integration with leading business applications, data repositories, and cloud services. Shield-SDE offers the only true enterprise secure data exchange broker solution.

Shield-SDE connects to business applications and cloud services such as IBM, Microsoft SharePoint, Salesforce, DropBox, Box, etc, and enables applications and cloud services to securely transfer data to users, other applications, and businesses. APIs

About Shield

Our team of security specialists are here to help you identify and implement secure and compliant cyber services. With over 25 years of experience, we are veteran industry leaders that have been at the forefront by providing secure messaging solutions.

Faster. Easier. Focused. The world of cybersecurity is complex. Our services are simple to use, easy to implement, and effective.

To evaluate and test Shield-SDE please contact:

Michelle Owenby
mowenby@shield4uc.com
Toll Free: 1-855-787-7253 ext. 356
www.shield4uc.com

You Be The Hero… We've Got Your Back!