DeliverySlip

WHITE PAPER

Enabling Secure, Diverse Communications for B2B & B2C Organizations

Introduction

The ability to communicate with customers and business partners quickly, effectively and securely is crucial to enterprise, SMB and government organizations. Whether for Business-to-Business (B2B) or Business-to-Consumer (B2C) communications, organizations increasingly rely on technology to collaborate and share information efficiently across multiple locations and devices.

At the same time, security concerns are increasing as sensitive data used in B2B and B2C communications transfers among multiple parties. Physicians need to send data to insurance companies; attorneys need to send contracts to clients; product and support teams need to send information to customers, and government agencies need to transfer documents to or receive information from citizens and other agencies. Securing all of this information is imperative to organizations that must comply with regulations and maintain credibility, as well as those that value protecting their intellectual property and private data.

This paper discusses the communication needs of users and their various roles in organizations and different industries, and explains how to secure, track and control sensitive data such as personally identifiable information (PII), corporate intellectual property and patient records without impeding productivity.

The shift to shared communications

Historically, organizations focused internally when it came to sharing information, using resources and security policies to build defenses designed to keep information inside the organization. Over time a shift occurred, requiring companies to respond nimbly to new innovations and increased competition. This meant opening more communications with partners and customers and sharing confidential, private and proprietary information. At the same time, organizations increased outsourcing, began to forge new business partnerships, and sought faster, more effective customer communication.

Now, the high speed of business makes collaboration with consumers and business partners essential for success. To facilitate this communication, organizations are forced to be more open when it comes to sharing information, while accounting for varied locations and devices.

The PWC "2015 US State of Cybercrime Survey" reported that 58% of respondents do not consider supplier risks, and 23% do not evaluate third parties at all.[5]

The risks

As essential as open communications are for organizations, the ability to secure these communications is equally, if not more, critical. Privacy breaches and data leaks continue to increase, damaging companies financially and causing public embarrassment. For example, the Sony email hack cost the company more than $100M, with at least $35M in IT costs.[1] And according to an InfoWatch analytics report, company employees were responsible for 58% of data leaks in H1 2015. More than 262 million records were compromised, and 90% of data leaks were related to personal data.[2]

Adding to the complexity of security management is the potential for data breaches through third-party partners. For example, the Army National Guard reported that 850,000 members' data may have been exposed due to an improper data transfer to a third party, non DoD-accredited data center.[3]

According to Booz Allen Hamilton, third parties posed the top security risk to financial services firms in 2015.[4]

"Business stake-holders often mistakenly assume that email encryption is a single solution, regardless of differences between use cases such as B2B and B2C; as a result, they provide insufficient information to risk and security leaders for product evaluation and selection."

Gartner Market Guide for Email Encryption, 2015

Diverse messaging needs & roles for B2B & B2C organizations

When it comes to business communications and collaboration, there is no one-size-fits-all approach to sharing information with partners and customers. Internally, the types of content and recipients (customers or business partners) differ based on business functions and roles, while the size and/or industry of the business determine the applications and extent of use; benefits, such as improved sharing and collaboration; automated, intuitive interfaces that are easy to use in real time; and equal suitability for SMBs and enterprise organizations.

B2B INFORMATION SHARING

- Financial data
- Product information
- Engineering designs
- Government: inbound communications
- Statements of work

B2C INFORMATION SHARING

- Legal documents
- Customer support information
- Release forms
- Customer product or service collaboration
- Agreements and releases

Secure communication needs by organizational role

Likewise, organizations find that as they work in more lean and nimble environments and need to increase their communications, almost any department or role needs to secure messages, files and information workflows. Below are some examples of needs by organizational role:

FACILITIES

THE NEED To streamline, secure and track facility management communications and agreements, and improve communications with vendors. For example:

- Facilities and vendor negotiations
- Lease agreements
- Facilities contracts and agreements

HUMAN RESOURCES

THE NEED To manage security in a department's internal and external communications and receive real-time visibility and full control of messages. For example:

- Employee policies
- New hires
- Contractor communications
- Separation agreements
- Salary/compensation information
- Employee evaluations
- Offer letters
    i. Internal disciplinary proceedings
    ii. Claims/disputes

FINANCE/ACCOUNTING

THE NEED To manage security in a department's internal and external communications and receive real-time visibility and full control of messages. For example:

- Invoices
- Budgets
- Auditing/communications with partners
- Affiliates
- Sending confidential financial information
- Records

OPERATIONS

THE NEED To share information securely for business operations functions that include budgeting, investor information and contracts. For example:

- Operating plans and budgets
- Company and investor updates
- Contracts and agreements

ENABLING SECURE, DIVERSE COMMUNICATIONS FOR B2B & B2C ORGANIZATIONS

Revelations of nation state surveillance activities and court challenges to "safe harbor" provisions are increasing data privacy and residency concerns."

Gartner Market Guide for Email Encryption, 2015

ENGINEERING

THE NEED To protect valuable intellectual property and engineering processes by sending information privately to associates within a department, customers and partners. There is often a need to share very large files securely and quickly without needing encrypted media drives, FTP transfers, as well as prevent usage of insecure means. For example:

- Product requirements
- Engineering specifications
- Customer requirements and acceptance
- Consulting agreements
- Product schedule updates
- Product planning
- Statements of work
- Patent applications
- Trade secret documentation
- Defective product conversations
- Outsourcing inquiries/workflow

PROCUREMENT

THE NEED To manage communications and sharing of information with suppliers, and better manage contract processes securely. For example:

- Statements of work
- Agreements
- Contracts
- Purchase orders
- Specifications
    i. RFP management

LEGAL

THE NEED To maintain full confidentiality in legal communications and document sharing. For example:

- NDAs
- Contracts and agreements
- Board minutes
- Policy updates
- Confidential information/legal opinions
- eDiscovery (email archive integration capabilities)
- Reporting requirements
- Compliance reporting

MARKETING

THE NEED To share marketing plans, documents, schedules, budgets and updates with customers, contractors and vendors. For example:

- Marketing contracts and agreements
- Marketing plans
- Customer communications
- Partner communications and document sharing
- Designs and images
- Training
- Launch planning
- Share large files such as graphic design documents, website code, etc.

PRODUCT MANAGEMENT

THE NEED To speed up and secure the delivery of new products and enhancements and share product plans and updates with customers. For example:

- Product requirements
- Product roadmaps
- Product releases
- Code reviews
- Customer communications/ updates
- Product updates
- Product recalls

IT

THE NEED To manage security in a department's internal and external communications and receive real-time visibility and full control of messages. For example:

- System changes
- System specifications
- Account information
- IT policies
- Security alerts and updates
- Password resets
- Reports on critical infrastructure/ severity/outages/etc.
- Requests for eDiscovery content

ADMINISTRATION (PAS, EAS, ETC.)

THE NEED To maximize the utility of business messaging and information workflows by ensuring timely responses to requests and sharing large files, while maintaining executive confidentiality. For example:

- Organizing executive travel/ relocation (sharing passport documents, etc.)
- Schedules and agendas
- Private executive communications
- Password management
- Specifications
    i. RFP management

SALES

THE NEED To achieve approvals to close deals faster and maintain company confidentiality with the capability to share emails and files with prospects, customers and partners securely. For example:

- Partner agreements
- Sales quotes and orders
- Integration with CRM (DeliverySlip API integrates secure messaging and file sharing into any CRM application)
    i. RFP management

INVESTOR RELATIONS/ EXECUTIVE COMMUNICATION

THE NEED To maintain reporting and information compliance by securing sensitive financial and company information. For example:

- Reporting
- Financial/earnings updates
- Investor communications
- Mergers and acquisitions

SUPPORT

THE NEED To share account and configuration information with customers privately and track message receipts easily in email client or browser. For example:

- Customer account provisioning
- Customer notifications
- Product updates

Different uses, common requirements

ONE-CLICK, INTEGRATED SECURITY

Despite their varied needs, businesses and individuals share the same requirements when it comes to email security. At the basic level, all users need a secure way to share information, including messages, files and information workflows from other applications with customers, affiliates or business partners. In today's instant-access business culture, users want to be free to share appropriate information without running into legacy security barriers that are difficult to use, slow them down, or block them from communicating. However, the potential for user error and insider threats make security necessary. The key is to make it available in a simple, easy-to-use interface that integrates into existing applications to facilitate adoption and usage.

MESSAGE CONTROL & TRACKING

Business users need to ensure prompt delivery of their messages and to track and control messages after they are sent, regardless of whether business partners or customers are the recipients. Was the message opened? Did the recipient download the file attachment? Was the message forwarded or deleted? Has the document been signed? The ability to control the messages and files by preventing forwarding or replying to all, by setting expiration dates, and by recalling a message, provides a critical extra layer of data protection and helps business reinforce compliance.

E-SIGNATURE SUPPORT

Whether it's signing and exchanging contracts, agreements, medical records, financial information, or other formal acknowledgements, organizations need to exchange signed documents. This is increasingly done through e-signatures, which are digital representations of signatures that are incorporated in,attached to, or associated with an electronic document, designed to replace an actual hand-written signature. E-signatures significantly speeds up the process of obtaining required signatures on documents and dramatically reduces much of the cost since documents can now simply be exchanged digitally.

SUPPORT FOR MOBILE DEVICES & LOCATION

The ubiquity of remote and mobile workers and the necessity to collaborate with business partners and connect with customers has led to the commonplace use of mobile devices for internal and external email communications. Business users need to send and receive messages and files easily from any devices (BYOD and company-supplied), regardless of location, and know that any sensitive information will remain as secure as on-premises communications.

INFORMATION CONTROL FROM OUTSIDE APPS

The sharing of information from cloud-based applications for various business functions has grown significantly in recent years. Organizations want to empower their employees to use these productivity-enhancing tools, but users need to ensure information shared through these apps is protected. By integrating an easy-to-implement API, users can re-route these communications through a secure messaging solution without impeding the efficiency of the application.

SIMPLE INSTALLATION

Messaging security should install quickly and easily without necessitating a change to a business's IT infrastructure or requiring IT expertise. The solution should be flexible enough to be deployed on a project-based basis when appropriate, and it needs to be intuitive and simple to use and manage, so it doesn't interfere with common tasks.

DATA RESIDENCY

Many organizations collaborate with consumers and business partners that reside in other countries, making it essential that they control where their data resides to protect privacy and facilitate compliance.

For a secure, mobile-friendly communications solution, get DeliverySlip

As a flexible, yet total Cloud messaging, file sharing and information workflow security solution, DeliverySlip offers B2B and B2C users the tools and features they need to communicate and collaborate freely without worrying about information security. The solution delivers advanced message encryption, tracking and detailed message control that protects private data, secures communications and ensures compliance. Key benefits include the capability to:

SEND PRIVATE EMAILS TO ANYONE WITH ONE-CLICK ENCRYPTION

Users can send fully secure emails to internal employees, partners, customers or patients without requiring them to download special software. Emails are encrypted at the desktop level, so users simply hit send to secure their emails.

SHARE LARGE FILES RAPIDLY

Users can email large files quickly, bypassing pre-set file size limitations and maintaining workflow.

SECURE E-SIGNATURE

DeliverySlip's E-Signature solution is the simplest, most cost-effective way to securely authorize documents with e-signatures. It includes a simple "click to acknowledge" signing process, broad file type support, integrated security for document and data privacy, and is provided at no extra charge.

ENABLE SECURE MOBILITY

Messages can be shared on mobile devices without compromising security or data integrity.

TRACK & CONTROL EMAILS WITH THE DELIVERY SLIP

Users receive real-time message tracking and notifications to know when their email was received, read, answered, forwarded, deleted or printed.

ADD LAYERS OF PROTECTION FOR EXTRA-SENSITIVE MESSAGES

Critical messages can be assigned additional security with ForwardFreeze,™ ReplyFreeze,™ and FYEO (For Your Eyes Only). Messages and their attachments can be recalled (even if already opened).

REFERENCES

[1] Hack to Cost Sony $35 Million in IT Repairs, Network World
[2] InfoWatch Global Data Leakage Report, H1 2015
[3] Third-Party Security Breaches Sign of Growing Vendor Risk Problem, SecurityScorecard
[4] ibid
[5] ibid

INTEGRATE INTO APPLICATIONS & WEB FORMS EASILY

DeliverySlip can be integrated easily into almost any cloud-based app or web page to protect data to protect other workflows beyond email.

DEPLOY QUICKLY & EASILY

DeliverySlip can be integrated into your existing email systems in minutes and requires no extra hardware and no transfer of MX records, limiting the impact on your IT resources.

CHOOSE DATA RESIDENCY/JURISDICTION

Ensure that data remains in the company's jurisdiction of choice to protect confidential information, ensure regulatory compliance and collaborate with consumers or businesses that are outside of their country of origin.

INCORPORATE SECURE E-SIGNATURES

DeliverySlip offers an easy way for business users to sign documents electronically and send via email.

DeliverySlip

About DeliverySlip

Powered by 10 patents and stress tests by KPMG, you can trust DeliverySlip to keep your communications safe. DeliverySlip is the leader in email encryption and file security. Used and trusted in virtually every industry with over 5 million users and growing every day.

Be Productive, Be Collaborative, Be Secure

TRY IT FREE | DELIVERYSLIP.COM OR 1.877.404.9964