email2 SECURITY PLATFORM

www.email2.com | 1.888.362.4520

email2 Secure Email & Content Delivery Platform

Feature Sheet & Technical White Paper

The email2 Secure Email & Content Delivery Platform helps corporations address National (HIPAA, SOX) and State email and content delivery security safeguard standards. It enables smart compliance controls and powerful productivity features, using existing email programs that users are familiar with such as Microsoft Outlook®, Webmail, and Smartphones such as the Blackberry® and iPhone®. It works with all email addresses and consumer and corporate email such as Microsoft Exchange and Google Apps, offering the highest level of security, integrity and productivity. It employs highly effective encryption, without requiring complex programs, PKI certificates or TLS servers to manage.

Cloud-based Deployment:
Safely bring the platform into the organization without infrastructure changes or complex server configurations. Cloud-based On-demand (SaaS) model enables quick and easy corporate deployment, minimal training with an affordable subscription model, while leveraging your current IT infrastructure. The platform eliminates the need to store encryption keys and avoids traditional legacy technology problems of complex software deployment.

Secure Email & Content Delivery:

- **Ease of Use:** Securely communicate with thousands of internal & external users with a 20-second automatic account self-provisioning. The Platform 'wraps around' your existing email infrastructure and is customized with your branding, positively identifying the sending organization.
- **Universal Access:** Unique non-invasive, patented technology; closed-loop 2-way Outlook integration, Webmail, Smartphone & Desktop App (PC / Mac) Full WCAG3 AAA & Section 508 Accessibility.
- **Cloud-based SaaS:** Compatibility with all email addresses and consumer and corporate email such as Microsoft Exchange® and Google Apps®. Easy per seat or enterprise licensing with complete support.
- **API Secure Content Delivery:** Automate secure information delivery such as statements & invoices. Improve Green image by reducing paper consumption, realize an immediate cost saving of 80% and decrease collection time by 10+ days.
- **Patented Interchangeable Cryptographic Engine:** Unique customer-defined encryption certificate eliminates cross-contamination of data and ensures your privacy & confidentiality.

Smart Compliance Controls:

- **Risk & Compliance Management** Stop worrying about sensitive information falling in the wrong hands and directly address National (HIPAA, SOX) and State technical security safeguard standards.
- **Non-repudiation:** Real Time Tracking & Audit-trail of all content delivered, and unique 'For Your Eyes Only' feature ensures non-repudiation between parties.

- **Permission-based Intellectual Property Protection:** Complete message recall & content forwarding permission controls (ForwardFreeze); prevent content to be printed or saved locally (unique 'ScreenFreeze' viewer).
- **Outbound Smart Content Filtering:** Avoid brand-damaging and financial liabilities caused by improper data leaks. Integrates with existing DLP engines with our SMTP Emulator Appliance.
- **Spam Throttle**: Users are approved by your organization and can be banned at the first sign of abuse, combined with a throttling engine that prevents inappropriate use of the system.
- **Archiving, Indexing and Searchability**: 'Bolt on' approach to your existing infrastructure leaves zero footprint. Content can be stored within existing email server; indexing and archiving systems continue working without any special configurations. 'Disable Local Store' technology can prevent local storing of secure content in recipient's local email client or server.

Powerful Productivity Features:

- **Securely Deliver & Receive Files / Attachments of Any Size**: Securely Deliver & Receive Files / Attachments of Any Size directly in Outlook or through the Desktop App, no links to click & does not require FTP, nor unsafe separate website navigation.
- **Secure e-forms Data Workflow Automation**: Make sharing confidential information with your organization easy & secure by sending a secure message to the desired recipient(s) from any webpage.
- **Desktop App:** The Desktop App acts as a secure productivity agent & notifier. It displays an icon in your PC system tray or Mac Finder and lets you know instantly when you have new messages or when your secure messages are read, replied to, forwarded, all without having to open a web browser. The Desktop App also offers some convenient shortcuts to create secure messages, or send/share large files securely.
- **Secure Virtual Printer (PC only)**: Send printed data securely from within any third party application such as ERP or CRM, instead of unsecure PDF, fax or overnight courier.
- **Secure & Private Video Messaging**: Communicate via secure & private video messaging. Executives can now record secure podcasts from their desk and share them in confidence.
- **User Group, Email Aliases & Legal Disclaimers Management**: Enable feature access by pre-defined user group and allow multiples email addresses per user. Custom notifications allow legal disclaimers to be added to any secure communication.

Secure Email & Content Delivery

- Securely communicate with thousands of internal & external users with a 20-second automatic account self-provisioning. The Platform 'wraps around' your existing email infrastructure and is customized with your branding, positively identifying the sending organization.
- Send & Receive secure messages as easily as standard email; email2 uses unique non-invasive, patented technology; closed-loop 2-way Outlook integration, Webmail, Smartphone & Desktop App (PC / Mac) & Administrator Console for client-specific configuration. WCAG3 AAA & Section 508 Accessibility.
- Increase customer satisfaction by clearly indicating that you are protecting their information from falling in the wrong hands.

The email2 platform is used today by thousands of users to ensure corporate secure messaging & compliance, ensuring integrity and control over your data. Offered On-Demand (SaaS), it 'bolts on' to your existing infrastructure leaving a zero footprint and can be deployed within minutes with minimal training and no user workflow changes. It allows for seamless conversations, from Outlook to Outlook, without requiring any changes to the current user business workflow. There are no separate interfaces required, no changes to email addresses or email programs, and no need to access secure FTP or to click a link to access message attachments, etc.

From small to mid size law firms, large manufacturing companies, to government and large F100 corporations, the email2 platform's turnkey solution is often used by our clients to 'replace' their traditional email encryption products that fell short on their promises. In fact, the majority of our clients turn to email2 having already realized the importance of securing all their communications but failed to fully deploy security to their entire user community due to the complications involved with competing products.

Secure the line, not just the message: the email2 platform takes secure messaging to a new level, giving you ownership of your secure communication path from sender to recipient through your own, fully branded secure messaging platform. Every message and content delivery is secure, tracked and auditable, allowing you to prove who read your communication and what they did with it. email2 can easily be deployed departmentally or enterprise wide. Start your deployment with only a small workgroup and grow your usage based on your specific needs. Legal, Tax and HR departments benefit from an immediate ROI and increased productivity.

The email2 Platform ‘wraps’ around existing email infrastructure so you do not have to replace any technology that is currently in place like your email addresses or email programs; it acts as a secure message gateway by bringing a more reliable transit and content management system to your existing email infrastructure.

The email2 platform offers corporate email and content delivery security without the complications: no PKI keys or TLS Servers to deploy & manage, and under 20-second automatic user self-provisioning (including external users). The email2 Platform combines database messaging and permission-based document management concepts with Internet banking security-strength to give organizations the confidentiality, compliance and control they require. The email2 platform addresses the shortcomings of basic SMTP email, encrypted or not, while remaining fully compatible with previously-deployed infrastructure like Microsoft Outlook® and Exchange®, Webmail or Smartphones.

Secure messages are stored encrypted using our patented Interchangeable Cryptographic Engine using AES 256-bit encryption for data-at-rest storage on your own branded messaging platform - not all over the Internet on unprotected, public SMTP servers, like with basic email (even if your emails are encrypted). AES is the only

publicly available cipher certified for official government documents classified as 'Top Secret'. It eliminates cross-contamination of data with our SaaS offering and ensures that your data is not tampered with (edited) over time, and is automatically archived.

Communicate with your clients, and give them the peace of mind that comes with knowing that the security of their data is a priority to your organization. Every aspect of the email2 platform can be branded in order to integrate visually with your existing web site, portal and web application. The email2 Toolbar for Microsoft Outlook, Secure Webmail and Smartphone clients can follow your company's strict branding guidelines in order to reinforce your brand image. The patented Delivery Slip offers secure identity verification, so you know that no one has "spoofed" an email account and sent a forged or altered email to you. Because there is sender transparency, personal accountability enforces non-repudiation and ensures a reduction in spam, phishing and the spread of malicious software.

By extending invitations to your Secure Messaging Platform to your client base, you can extend your brand into their local computers as well. Invitations sent to new users and messaging at the login screen of the Webmail can also be customized to reflect your branding and properly explain what is expected of the new user and why your organization is now using a secure method to communicate confidential information with them.

Unlike email encryption programs where only email security is addressed (and often poorly), email2 also adds a layer of functionality not currently available with competing products. In fact, a recent survey with our user based showed that security only accounts for 10% of the satisfaction benefits of the email2 platform. Real time tracking and control of information, true & complete message & content recall function, seamless large file transfers, integrated video messaging and the ability to invite several thousands of 'Guest' users external to the client's organization are the key differentiators that make email2 so popular.

Universal Access:

- Unique non-invasive, patented technology & Delivery Slip; closed-loop 2-way Outlook integration, Webmail, Smartphone & Desktop App (PC/Mac). Full WCAG3 AAA & Section 508 Accessibility.
- Enable security and unique productivity features within existing email programs that users are familiar with, deployed within minutes with minimal training and no user workflow changes.
- The Delivery Slip is a window to the secure message. Recipients can access information about the Private Email Network used, the sender, the recipients and what actions have been performed on the message. Quickly review message metadata, such as real time tracking, with any secure message. Start composing a basic email message and use the Delivery Slip to change to a secure message while composing.
- Web Admin Console dashboard displays important statistics quickly and clearly, in order to analyze usage and user membership settings. All actions are recorded and logged to provide a clear audit trail for reporting purposes.

email2's key differentiator is the seamless integration with your existing email programs like Microsoft Outlook. From sender to recipients, there are no cumbersome 'keys' to exchange and manage, allowing your organization to exchange confidential information with all your stakeholders such as your employees, clients and partners, in a complete closed-loop. For those not using Microsoft Outlook, our powerful secure Webmail and Mobile clients take care of your entire user base seamlessly.

email2 Toolbar for Microsoft Outlook

The Outlook email2 Toolbar allows users to manage their secure messages alongside their basic email messages seamlessly in the world's most widely used business email programs. With the email2 Toolbar installed, any authorized user can use their email program to create, read and respond to secure messages. Secure messages can make use of all existing features such as Spell Check, Address Book, and Organizational Rules. There is no need to navigate to a separate browser, or to manage and rotate complex encryption keys and cumbersome passwords. Users are also able to send files of any size without limitations that are otherwise imposed by traditional email and without being forced to use FTP or navigate to an (potentially) unsafe website.

The email2 Toolbar appears in the default menu and toolbars section of the email program, giving users the option to quickly choose between creating a new secure or basic email message. This selection can also occur mid-way while composing your message: the patented Delivery Slip is added to the right side of the secure message compose window that allows the sender to select the proper Private Email Network, set forwarding, replying, and message tracking permissions as well as create secure & private video messages on demand. The email2 Toolbar provides added flexibility by conforming to the way users work within their email program yet takes advantage of all the security and tracking capabilities of the email2 platform. With the patented Delivery Slip installed in your email program, you have access to more information (message metadata) and actions than you do for basic email messages.

There is no need to reconfigure your mail server or change your email address or Internet Service Provider (e.g. MX records) to start using your Private Email Network with the email2 Toolbar for Outlook. It is designed to be a client-side solution via a desktop client; the email2 Toolbar is easily installed in under two minutes without requiring Administrative rights. Send secure messages through your branded Private Email Network directly without requiring your mail server's interaction; your network works with all mail servers including Microsoft Exchange®, Zimbra®, etc. without needing any integration changes or complicated configurations. All your existing investment in email archiving, compliance, workflow and management remain intact and continue to work with your Private Email Network; there is nothing to change or replace.

email2 Secure Webmail & Smartphone Clients

The secure email2 Webmail client is a full featured AJAX web-based mail client that gives you access to all of your secure messages. It is compatible with most major web browsers, including Firefox 2+, Microsoft Internet Explorer 6.0+, Safari 4.0+ and Chrome 0.2 beta+ on Windows PC, Mac or Linux.

The secure email2 Webmail client allows authorized users to read, reply to, forward and create messages securely. The email2 Webmail client is specific to a Private Email Network, effectively creating a branded, personal private mailbox for each of your members. Only secure messages can be acted upon in this interface; no basic email messages, no spam, and virtually virus-free. Being browser-based, the email2 Webmail client requires no installation on the local machine. It can easily extend itself to accommodate any new features as they are developed; the entire platform allows for the custom design and implementation of network-specific "modules" through our API. These modules can be productivity tools geared to a specific industry vertical such as secure delivery of invoices (e-statements).

Users accessing the secure Webmail client from a Smartphone or other web enabled mobile device (like a Blackberry or an iPhone) are automatically directed to a secure email2 Smartphone client. Create, read and reply to secure messages on your BlackBerry, Windows Mobile, Android and iPhone, or any other Smartphone device.

The best part is that it uses the same secure access; all connections are still made over HTTPS (128-bit SSL encryption) and none of your private data is stored on the handheld device. Your information is protected, even if you lose your device. Smartphone access can quickly be enabled or disabled from the Webmail client. Disabling mobile access after a handheld device has been lost or stolen adds additional protection by preventing access to the member's account through the Smartphone client.

Patented Delivery Slip

The patented Delivery Slip is a window to the secure message where the recipient can access information about the Private Email Network, the sender, the recipients, and what actions have been performed on the message; message retrieved, forwarded, replied, deleted or recalled, etc. The Delivery Slip also contains pertinent information regarding the message details, attachments, secure video messages and policies applied to the current secure message; you can determine whether you want to download attachments or even the secure message itself (with auto-retrieve secure message 'off').

Among other benefits, the Delivery Slip allows the sender to:

- Choose the appropriate Private Email Network for a specific conversation.
- Find out if the Private Email Network used is Certified Secure.
- Set permissions on compose such as the ability to reply or forward your message (ReplyFreeze & ForwardFreeze).
- Mark the message For Your Eyes Only (F.Y.E.O) and set a unique password.
- Mark printed secure attachments to be viewed on screen only (ScreenFreeze).
- Record a secure Video Message

The Delivery Slip allows recipients to:

- Find out who the secure message is from, and who it was sent to.
- Review real time tracking if enabled and if it is shared with every recipient.
- Review the filename, size and type of any attachments before they are downloaded locally.
- Review the special policies applied to the secure message such as 'ForwardFreeze' and 'For Your Eyes Only (F.Y.E.O.)'.

email2 Web Admin Console

Companies or organizations that implement a branded Private Email Network have full control over the administration and management of the network. When the Private Email Network is created, the organization designates an administrator. The Administrator creates membership packages and sets membership levels and invitation policies. Administrators can choose to explicitly set up each new member account, grant invitation privileges to certain members, or make the network open access for all current members to invite new members. The published API can be used to automatically provision member accounts or create new secure messages through another program, like a web service or Active Directory (LDAP).

The Web Admin Console allows IT administrators to set user configuration options and security authentication levels, and whether they want to enforce secure communications for all email traffic. The web-based Admin Console has a dashboard, showing important statistics quickly and clearly. With a glance, Administrators can see

the total number of members, or the total amount of storage for their network, along with a host of other statistics that can be quite useful when analyzing usage. Additionally, all actions are recorded and logged to provide a clear audit trail for reporting purposes. IT Administrators have the ability to:

- Set the proper security settings such as 'open' or 'closed' Private Email Network access environments or 'by invitation only'.
- Design Membership Packages on-the-fly, establishing feature access and security settings for members throughout their entire organization.
- Control membership configuration options such as storage and bandwidth limitations, set who can invite new members.
- Set and manage a unique security option that prevents any programs (e.g. Outlook) or web browsers from storing copies of messages locally (even if using MS Exchange).
- Create grouped views by dragging a category into the grouping bar and export the member list into Microsoft Excel.

Cloud-based SaaS Benefits & Cost:

- SaaS model enables quick and easy corporate deployment, and offers a zero-download approach for all senders and recipients. Easy per seat or enterprise licensing with complete support.
- Compatibility with all email addresses and consumer and corporate email such as Microsoft Exchange® and Google Apps®.

The email2 platform is offered as a service (SaaS/Cloud On-demand). Our licensing is available 'per seat' or as enterprise bundled packages and can accommodate small groups of 5 users up to thousands of internal and external users. Every package includes your own branded Private Email Network, access to all of our security & compliance and productivity enhancements features, and unlimited L1 L2 & L3 support. The same packages can be broken down to remove the productivity enhancements and support, ideal for quickly replacing your existing email encryption product that fell short on their promises and keeping pricing within your current budget.

The email2 Platform is compatible with any email address or mail server such as Microsoft Exchange® and Google Apps®, and offers a zero download approach for all senders and recipients. New recipients are automatically invited to join your network. A 20-second automatic self-provisioning through the Webmail client gives them instant access to your secure messages. Optional free self-configurable plug-ins for Outlook and Desktop App increases accessibility with minimal training. Increase customer satisfaction by clearly indicating that you are protecting their information from falling in the wrong hands.

The email2 Security Platform was designed so that it will not conflict with other email applications, even other security applications. If enabled, members are able to send basic email messages because the email2 platform does not affect any part of basic email. Alternatively, a special set-up can force a specific member's computer to only send secure messages over a specified Private Email Network. When a member sends a secure message, the confidential portion of the message bypasses the regular basic email workflow, instead using the Private Email Network workflow. The email2 platform stops its integration at the client level (e.g. Outlook) and does not interfere with your existing applications, back-up systems of firewalls; it only requires port 80 and standard SSL port 443 to function properly.

Cloud / SaaS Benefits & Cost

Delivered via the SaaS model means that your Private Email Network is hosted in email2's state-of-the-art data centers:

- No need to worry about hardware and upgrades costs. We take care of everything behind the scenes.
- No need for large up-front capital expenditure and weeks of deployment time.
- Corporate deployment time of less than 10 minutes, self-user set-up of less than 20 seconds.
- Available around the clock anywhere in the world.
- Monthly feature upgrades automatically
- Data Protection with our patented Interchangeable Cryptographic Engine & Certification process that generates a unique encryption certificate for your data

At any given time email2 updates its infrastructure to accommodate new customers' requirements and usage patterns. Multiple Application Servers are deployed within the Private Email Network where the load is distributed via a load balance solution. In general the Data Server remains as one redundant server. This allows us to provide the same level of isolation for customers that require it, in which case a dedicated App and Data Server machines are deployed internally, while still taking advantage of the other shared services.

The yearly cost associated with setting up a 'company-branded' Private Email Network is based on the number of 'Premium' and 'Guest' user types. As a user, the cost of accessing and using the Private Email Network is generally covered by the company offering the service.

SaaS / Cloud (10 minute corporate configuration – under 20 second user self-provisioning)

- Small-Medium: 5 to 200 Premium Users, up to 2,000 Guest Users
- Large: up to 350 Premium Users, up to 3,500 Guest Users
- Enterprise: up to 1,000 Premium Users, up to 10,000 Guest Users
- Platinum Dedicated Server: thousands of Premium Users, thousands of Guest Users

Members can have two distinct types or roles within your Private Email Network: 'Premium' and 'Guest'. Types or roles are set as part of a 'Membership Package'. Custom Membership packages can be designed to control feature access, storage capacity, etc. The Member Type is the only variable that drives the monthly billing:

- **Premium Type:**
  A Premium Member has full rights to the Private Email Network, to invite new Members and create new email2 secure messages. Premium (registered) members count as a 'Premium Member' for billing purposes.
- **Guest Type:**
  A Guest Member can only read and reply to secure email2 messages. They cannot invite new Members or create new secure messages. Use this type for customer facing activities, ideal for clients facing activities to exchange confidential information only a few times a month, offered at a fraction of the cost of a Premium Member.

API Secure Content Delivery:

- Our full featured developer API exposes commands to third party developers that wish to integrate the email2 platform with their applications, or even create standalone modules. Easily automate information delivery in a secure manner such as employee statements, invoices, etc. Become greener and reduce paper consumption.
- Improve Green image by eliminating costs associated with printing and mailing or faxing periodic statements, realize an immediate cost saving of 80% and decrease collection time by 10+ days.

Do you have a need to automate information delivery in a secure manner? Perhaps you need to distribute employee statements electronically to each employee confidentially? Need to ship invoices or price books securely to your clients or distributors? Or perhaps you have a mandate to become greener and reduce paper consumption? Our full featured developer API exposes commands to third party developers that wish to integrate the email2 platform with their applications, or even create standalone modules.

Our API Secure E-statement feature delivers the same information previously sent on paper, fax or PDF automatically and securely to your stakeholder's existing email addresses. Examples include (but are not limited to):

- Monthly invoices to your entire customer base
- Monthly employee statements such as paystubs
- Monthly financial reports (banking, wealth management, trading confirmations, brokerage transactions, insurance policies, mortgages, etc.)
- Claims & Records transfers (healthcare, X-Ray files, patient records, etc.)
- Custom OEM solutions, confidential system notifications, etc.)

Secure and fully automated, email2's powerful set of APIs allows your organization to connect any existing application or engine such as your ERP, HR or custom applications. Every transaction currently produced as a PDF, or at worst, printed, can now be delivered electronically, securely, without any changes to your existing internal workflow. Realize an immediate cost savings of 80% or more by eliminating costs associated with printing and mailing or faxing your monthly statements; your transaction price reduces from an average of $1.50 to a few pennies. On average, our clients save more than $11,500 per month for every 10,000 statements.

By eliminating paper consumption related to your monthly distribution of information, you can show your customer base that you are actively participating in protecting the environment. Allowing your stakeholder to 'self print' their information directly from their secure mailbox has shown a reduction in paper consumption by more than 80%. Used for e-billing purposes, you can realize a reduced processing and collection time of about 10 days compared to the process of printing and mailing every invoice. Every statement is delivered securely to every stakeholder's existing mailbox, using their same email address. The email2 platform allows you to fully track not only when the information was received and read, but also track if it was printed. Monitor tracking information collected real time using our 'Campaign' manager, increasing accountability; gone are the days where your clients claim to not have received your overdue invoices! Information sent to the wrong person can quickly be recalled, even if already read by the recipient(s).

Companies concerned about paper consumption have traditionally relied on fax or PDF distribution of monthly statements. With new rules and regulations in place, this information must now be delivered securely. The email2

platform can deliver statements in a traditional PDF format (but securely), or in an HTML format directly placed in the body of the secure message, enabling 'self print' functionality but eliminating such statements from being saved on local computers that might not be safe.

Distributing information to large groups such as employee statements or client invoices and statements incur a significant reduction in fuel and paper consumption over paper-based mail delivery. Enhance your corporate Green Image through reduction in fuel consumption (used by couriers) and paper consumption. This may allow your organization to qualify for an Energy Star rating from the EPA or carbon credits.

Build secure communication support into your web applications or just add a feature that you think is missing. We use a REST-like approach and accept custom formatted JSON requests. Examples of the type of integration that customers have developed for the email2 platform include SAP, JD Edwards, Salesforce.com, and ACCPAC. Contact us or your Reseller to obtain a developer documentation kit that includes several Case Studies.

Patented Interchangeable Cryptographic Engine:

- Unique customer-defined encryption eliminates cross-contamination of data and ensures your privacy & confidentiality.

The email2 platform uses a "Master Key" process in order to ensure integrity of the customer data, and guarantee that no other customer can access your data. The Certification consists of entering a unique long password when the network is certified (Master Key) combined with random information specific to the network and local storage server in order to create a unique and interchangeable encryption process for each branded Private Email Network.

Risk & Compliance Management:

- Directly address National (HIPAA, SOX) & State email security and content delivery compliance standards.
- Designed to integrate seamlessly with email compliance supervision tools.

The email2 platform recreates the full business process of traditional registered mail electronically. All attachments are stored encrypted, certified and available for later retrieval in their original condition. Every transaction is verifiable and protected from tampering, providing a defensible chain of custody for compliance and litigation.

Stop worrying about sensitive information falling in the wrong hands and directly address National (HIPAA, SOX) and State technical security safeguard standards. Since every secure message stays encrypted from creation to retrieval and is hashed with a unique value, there is no feasible way to modify the content of a message or attachment without causing an error that would be evident to the end user or an administrator.

Non-repudiation:

- Overnight mail replacement through secure delivery of messages, content & attachments and real time tracking audit-trail to prove it, using our unique message tracking technology.
- See when recipients have read, replied to and forwarded your messages (and to whom, if allowed). Enforce non repudiation between entities by knowing when messages are read and forwarded.

- Unique 'For Your Eyes Only' allows user to assign secret passwords to specific communications and prevent unauthorized usages of your email account. Turn on the 'Challenge Response Authentication' feature to create a second factor authentication mechanism where new users are required to enter a Client ID, PIN, Account Number, Zip code, etc. before having any access to secure messages or attachments.

Non-repudiation is legally defined as the absence of deniability, meaning that recipients cannot deny their participation in the transaction. The email2 platform offers guaranteed and confirmed delivery of your messages. Track your secure messages on any platform; Outlook, Webmail and Smartphone clients with absolute accuracy. When was a message opened? Who was it forwarded to? Did the recipient print it? These actions and more are recorded automatically for any message sent on your Private Email Network and conveniently displayed through the patented Delivery Slip.

Real time tracking and audit-trail of all secure message and content delivered

Your Private Email Network lets you track the delivery of your secure message and content delivery just like couriers and logistics companies. It provides truly accurate message tracking because all messages are stored on a central, trusted server. All requests for retrieval, replies, and forwards are tracked. Additionally, the server tracks when the message has been printed and the attachments have been downloaded. Secure messages are tracked both when they are received and when they are opened, providing the most accurate non-repudiation possible. Because the tracking information is so accurate, it can be used by organizations to aid in compliance with regulatory requirements, (e.g. SOX, HIPAA, and others): this means that you can track all activity that's happening with 100% accuracy.

Through the patented Delivery Slip, the tracking feature displays a list of message participants, and whether or not they have (for messages and attachments):

- Reviewed the Delivery Slip
- Retrieved the message (read, either in Outlook, Webmail or Smartphone)
- Retrieved any attachments (either opened or store locally on their network)
- Replied to the message (and to whom – information available only to the sender)
- Forwarded the message (and to whom – information available only to the sender)
- Forwarded any attachments (and to whom – information available only to the sender)
- Printed the message though the Webmail client
- Deleted the message permanently though the Webmail client
- If the message Recall is allowed for the message
- Recalled the message, along with all attachments (attachments are no longer available for retrieval)
- If the correct password has been entered when using 'For Your Eyes Only (F.Y.E.O)

Each of these actions is recorded every time they occur with a date stamp and IP address. This information can be shared with other participants through the Delivery Slip, or kept private. Generate audit reports with tracking data on the fly, which will aid in compliance with difficult regulatory requirements such as those found in Sarbanes-Oxley (SOX), HIPAA, etc.

For Your Eyes Only (F.Y.E.O)

For additional non-repudiation of your secure communications, turn on the 'For Your Eyes (F.Y.E.O.)' delivery option. When creating a new secure message, the F.Y.E.O. delivery option is available under the 'Enhanced Security Options' of the Delivery Slip. F.Y.E.O. requires that every recipient re-enters their Private Email Network password or a unique password as set by the sender every time they wish to read the secure message.

F.Y.E.O. provides certainty of identity and certainty of participation in the transaction, especially if a unique password was set and shared verbally with all recipients. Once the secure message is marked as 'retrieved' in the tracking module of the Delivery Slip, you can be certain the recipient(s) have read the secure message.

This feature is also useful, for example, for Senior Executives who share their mailbox with their assistant but still want to selectively keep some conversations private or for added protection when the users leave their computer unattended; no one else can read your secure messages marked with F.Y.E.O. unless they have access to the password. F.Y.E.O makes use of the 'Disable Local Store' feature whereby no content is stored locally and must be re-retrieved every time the message is to be viewed (even when using Outlook).

Challenge Response Authentication (CRA)

The Challenge Response Authentication (CRA) enables an additional level of non-repudiation when new users register with the Secure Network. The CRA feature acts as a second factor authentication where new users are required to enter a Client ID, PIN, Account Number, Zip code, or any other code as required. Once registered, the CRA code must be entered and validated by the system prior to the new user having any access to secure message or attachments. Once the CRA code is validated, a date stamp and IP address is recorded and is available through the Web Admin Console for audit purposes. The DLP whitelist feature allows exemption of specific domains or email addresses, especially useful for internal users to your organization.

The CRA can be integrated through the email2 API for automatic provisioning with any existing database with the organization, including LDAP. Alternatively, the CRA code can be entered manually by members of your organization when inviting new users to the system. This option requires no special integration and can be up and running with a single click through the Web Admin Console. The process entails having the sender manually enter the CRA code at the time of composing a secure message to new users. The CRA code can later be changed or edited if a mistake occurred during the invitation process.

Permission-based Intellectual Property Protection:

- Allow secure messages & content sent in error to be completely recalled and removed from the recipient's local email programs at any point during the life cycle of the conversation, even if the message has already been read.
- Content forwarding permission controls (ForwardFreeze); prevent content from being printed or saved locally (unique 'ScreenFreeze' viewer).
- Exchange confidential information knowing that your data is protected. Disabling printing of content improves the chances of your intellectual property remaining secure.

Complete Message Recall

Email has sped up our workflows, but its irrevocable nature means that highly visible mistakes are often made. You can now completely and 'truly' recall your secure messages and all attachments, even if the message has already been read. All attachments are automatically recalled and deleted. email2's complete message recall feature is different due to the underlying architecture of the platform: permission-based database messaging means that you can recall the 'read' permission at any point during the life cycle of the conversation with no special conditions.

'ReplyFreeze' & 'ForwardFreeze''

The email2 platform uses a centralized, mutually trusted Private Email Network to ensure that policies are always upheld. The platform allows the sender to control a message for its entire life cycle on the network. The unique architecture empowers the sender to limit reply and forward permissions on the network: Exchange confidential information knowing that your printed secure documents are protected with our unique 'ReplyFreeze' and 'ForwardFreeze' features.

It is important to note that these features are not designed to prevent the spread of information on its own, or to replace Information Rights Management (IRM) tools. Users can still take a screenshot or photograph their monitor, or verbally share the data. Most organizations will conclude, however, that from a fiduciary standpoint, best efforts have been made to control the flow of data by using a Private Email Network without additional controls like IRM. Delivery Slip options only restrict what can be done for a specific secure message residing on your Private Email Network, therefore reducing liability issues.

'ScreenFreeze'

Exchange confidential information knowing that your documents are protected with our unique 'ForwardFreeze' feature. Attachments such as PDF or Office documents become viewable only through our specialized Flash viewer (on-screen view only) and disables file printing, text copying or file saving of the PDF documents. Note that this feature does not prevent the user from taking a screenshot of their monitor or taking a picture of their monitor. This feature was designed to discourage inappropriate sharing of confidential information. The ScreenFreeze feature is available with the use of the Secure Virtual Printer where any information can be printed and attached to a secure message, and protected from locally saving the information at the receiving end. Turn on F.Y.E.O under Enhanced Security options to increase non-repudiation and ensure only the intended recipients can view the content.

Outbound Smart Content Filtering:

- Preemptive DLP feature with a powerful function to quickly make global rule changes to all employees. Users are prompted preemptively 'on send' to make appropriate corrections.
- Avoid brand-damaging and financial liabilities caused by improper data leaks such as Personal Identifiable Information (PII) and reduce training costs by 'catching' errors prior to data leaving the organization.
- Integrates with existing DLP engines with our SMTP Emulator Appliance.

Pre-emptive Data Leakage Prevention allows keyword filtering of all messages (secure and non-secure) and black & white listing of all content and recipients before the message is sent (as set by the Administrator). Policy control takes place dynamically – on 'SEND' before the message is transferred to the server. This is drastically different

(and more effective) than solutions which rely on ad-hoc parsing or outgoing message filters. Black listing allows complete blocking of email addresses or emailing domains before they can even be invited or registered with the Private Email Network, and white listing ensures that specific email addresses or email domains are always using the Private Email Network when exchanging messages.

email2's unique white & black listing rule-based DLP feature offers data-leak prevention that works preemptively, before the message is even sent. Prevent SNN and Credit Card numbers, or any other 'keyword' or 'algorithm' base rules from ever leaving your organization. Messages that do not meet your firm's customized criteria can simply be blocked or automatically sent securely using email2's unique 'Send Secure Default' feature.

Easily integrate with your existing DLP engine through the use of our SMTP Emulator / API Connector Server Appliance. When a message or attachment is detected by your DLP engine as requiring security, it can be re-routed instantly to our SMTP Emulator / API Connector Server Appliance. This appliance acts as a SMTP emulator where the content, attachments and headers of the message requiring security is uploaded directly to the Private Email Network using a direct & secure API connection. From there, the secure message is prepared and sent on behalf of the user, in a completely transparent manner. Recipients respond in the same secure manner back to the original sender ensuring that the entire thread is secure.

Spam Throttle:

- Users are approved by your organization and can be banned at the first sign of abuse. Message throttling prevents inappropriate use of the system to send large volumes of email (unsolicited emails). Self executable viruses are not able to infect your network. Authorized users are in, spammers are out.

Your Private Email Network is the "gated community" of the email world. Members are approved by your organization, and can be banned from the community at the first sign of abuse. Message throttling prevents inappropriate use of the Private Email Network to send large volumes of email (unsolicited emails). Automatically block specific users or IP addresses based on criteria specific to your organization.

Your Private Email Network also eliminates unwanted 'spam' email and messages: limit communication to a specific user group. With basic email, anyone who can guess your email address can contact you, with or without your consent. Once a spammer has your email address, they can contact you from as many different email addresses as they like, as often as they like. There have been major advances in the area of spam filtering, but large amounts of spam messages still manage to get through every day, wasting your time and hurting your productivity. Since Private Email Networks are only available to verified members, they are a tool for organizations to control the flow of spam into their network. Bulk 'emailers' are therefore unable to send secure email2 messages to your employees using the company Private Email Network. Since sender identity is always known, there is built-in accountability and an implied trust for all messages being received. Spam does not exist in messages sent via the Private Email Network because spammers do not have access to this exclusive gated email community. Additionally, the email2 Security Platform does not interfere with external email programs; third party anti-spam solutions will still work perfectly alongside the email2 Security Platform.

If your organization receives an enormous amount of email on a daily basis, as is the case with a government organization, you may want to consider simply 'ignoring' basic email and focus exclusively on secure email2 messages. Using the Secure Webmail client, basic email messages are not present, and therefore it is 100% spam-free.

The risk of contracting a computer virus is also mitigated by using the email2 Security Platform. Computer viruses are often transmitted via email attachments, and some are so virulent that even just having them unopened on your computer is dangerous. email2's attachment system doesn't automatically download attachments once they are received (at the member's option); instead members are notified of the attachment and prompted to download it. If an attachment seems suspicious, or is a confirmed virus, users can delete it from the PEN's server without ever having it put their personal computers at risk. Self executable viruses are not able to infect the network and propagate themselves because files are stored broken into parts, resulting in an overall more secure global network. Allowing recipients to manually retrieve messages once the Delivery Slip has been reviewed substantially reduces the probability of being infected by a virus. Additionally, users are guaranteed to retrieve messages from the proper sender / organization, resulting in a 'phishing' reduction.

Archiving, Indexing and Searchability:

- 'Bolt on' approach to your existing infrastructure leaves zero footprint. Content can be stored within existing email server un-encrypted so that users can still search for content in secure messages, and indexing and archiving systems continue working without any special configurations, or exported to any archiving system through our API Connector.
- Unique 'Disable Local Store' technology allows sending organization to prevent local storing of secure messages in recipient's local email client or server. Prevent any user outside your organization from saving and archiving secure messages locally (e.g. Exchange Server), increasing security of your data.

Secure email2 messages can be stored by Outlook into the traditional mail server repository (e.g. Exchange, Zimbra) as any other basic email messages (default configuration). This means that all company data is stored behind the company's firewall and any existing archiving or indexing email systems will still work with secure messages. If at any point a member stops using the Private Email Network and uninstalls the email2 Toolbar, these downloaded secure messages will behave as any other basic email messages, without the added functionality of the Delivery Slip. None of the company data is ever lost even if you stop using your Private Email Network.

Super Secure: 'Disable Local Store':

For an additional layer of security, another option of the email2 platform can ensure that messages are never stored locally on any recipient's computers, even if they are using Microsoft Outlook. Every secure message is securely re-retrieved every time it is viewed by the recipient and only stored locally for the time the message is being viewed. As soon as the recipient navigates away from the secure message, the local content stored in their mail server such as MS Exchange is replaced with the original notification message which contains no confidential information. Recall the secure message and rest assured that no copy of it exists anywhere, unless of course a recipient printed a copy or saved the attachments locally. Note that with this feature enabled your existing archiving email systems will be archiving the notification messages instead of the actual content of the secure messages. If your company policies require that secure messages be archived the same way basic email messages are archived, use the email2 API to periodically export all data to an appropriate storage location.

Securely Deliver & Receive Files / Attachments of Any Size:

- Securely Deliver & Receive Files / Attachments of Any Size directly in Outlook or through the Desktop App; no links to click & does not require FTP, nor unsafe separate website navigation.

- Avoid limitation policies set by receiving organizations and eliminate complicated FTP set-ups or user workflow changes with our unique permission-based attachment library.

Users are accustomed to sending files as email attachments; however email content is getting big and continues to grow at a rapid pace. Documents, spreadsheets, presentations and most other forms of information now in use, now employ rich multimedia content. When you are dealing with large files, you know from experience that your messages are getting bounced, quarantined and are saturating your inbox storage limit. Basic email was never intended for this use. As a result, many organizations now restrict the size of email attachments due to the strain it puts on networking and storage resources.

The email2 Platform offers the ability to manage very large file attachments without taxing your network. You can now quickly and easily send large files (tested up to 20GB / 20,000MB) that would bring a traditional email system to its knees. Since all communications are made using the HTTPS protocol, (instead of SMTP/POP3/IMAP4), large files can easily be sent and downloaded at high speeds (up to 10x faster with email2's acceleration technology), from Outlook to Outlook, without requiring the user to log in to a FTP server or a browser-based application with links to click. We eliminate all the problems people have with basic email as a file transferring tool. Consider the following benefits:

- email2 works directly within Outlook without dealing with size and security limitations.
- No attachment size limits: send and receive large attachments with no problem & eliminate large email storage issues from your email server: you don't have to download attachments every time you download your email messages (pull approach).
- No more FTP and secure FTP headaches: large attachments can be uploaded faster using more efficient protocols: eliminate FTP problems while meeting user needs and security requirements.
- Security Compliance: enforced HTTPS (128 bit SSL encryption) connections and AES server encryption keep your attachments safe during transfer and storage.
- Track attachments and view specific metadata, just like secure messages: used in CPA/Accounting, Law, Architecture, Construction, Engineering, Military & Defense and the Healthcare industries.
- The Attachment Library tab lets you manage, re-download and re-attach files that are already stored on the Private Email Network; when you forward an attachment, you don't need to upload it again (you are only forwarding the permissions to the attachment).
- From an IT management perspective, you are effectively reducing storage bloat on your mail servers and thus reducing IT costs and overhead.

When using your Private Email Network, attachments are not 'pushed' to users. The actual attachments are sent to your Private Email Network, and the recipients must actively retrieve attachments from the network itself. This is considered a 'pull' structure, in which users personally select which content to download to their local environments, resulting in a significant virus reduction.

Pull structures are generally considered superior, but due to the constraints imposed by the original design of basic email, it is impossible for basic email messaging to adopt a pull methodology. Users are subjected to spam, viruses, large (often unwanted) attachments and a number of other headaches associated with push systems. The email2 platform offers a pull structure through your network without invalidating basic email. Basic email attachments are pushed to users along with email messages, which can cause message bottlenecks and waste bandwidth and storage by duplicating the attachment by the number of recipients, or by unwanted attachments. The pull process

for attachments also adds a degree of protection; users do not have to download suspect files that might damage their computers.

Every time a user sends or receives a secure message with attachments, these attachments are automatically added to the secure, searchable Attachment Library. It is accessible from the Webmail client by clicking on the "Attachments Library" tab (can be labeled differently based on your Private Email Network and Membership Package). Users can assign access rights to the same files without waiting for them to upload again or perform a quick search of their attachments when they are looking for that important document. Monitor tracking data for attachments that each user owns, even recall or delete older attachments that are just taking up space. Use the Webmail to easily find and act on all secure messages: gone are the days of sorting through countless messages in your inbox to find an attachment.

The Attachment Library also provides a web-based secure and permission-based online storage for sharing files internally and externally. Files that are exchanged via your Private Email Network from your vendors, partners, and/or clients can be stored in the Attachment Library for later access, instant 'permission' transfer without any additional upload time. For example, if you have a large file that you regularly send to different stakeholders, you can just upload it once and resend it any time you want, rather than uploading that same file each time you want to send it to different stakeholders. Every attachment is protected by an authorized access list of your external guests and internal users with different permission levels. Therefore, you have full control of who has access to your files. Deleting the file from your Attachment Library automatically deletes it for the entire audience you had previously shared the file with, even if that file was forwarded by one of your original recipients.

Secure e-forms Data Workflow Automation:

- Secure e-Forms make sharing confidential information with your organization easy. e-Forms can be located on any webpage and creates a secure transaction by sending a secure message to the desired recipient(s).
- Accept data input from clients directly on your website and allow them to contact your employees securely, including large attachments. Reduce phishing and spam by not posting any email addresses on your website.

Create secure forms and make them available on your website, or directly in your users' Inbox for fast procurement. Every form submission triggers a secure email2 message directly in the Inbox of the person selected to be contacted.

The secure forms feature of email2 does not require that your website use SLL to safeguard the information submitted; instead, a direct and secure API call is made to your Private Email Network, routed directly into the secure mailbox of any and as many employees as you require. Reply to the form submission securely in order to engage in a private conversation with your website visitors, customers, patients, etc. Create secure forms such as 'Contact Us', Surveys, Loan Applications Processing, Benefits Enrollment, Health Insurance Claims, Medical History Forms, or Quote Requests on the fly. Design your forms with your favorite tool and programming language. Increase customer service satisfaction while reducing spam by not publishing email addresses on your website (only the list of available recipient's names are available as a pre-selection to the visitor). Form submission throttling prevents inappropriate use of the public form by web-bots repeatedly submitting false information.

The manual process involved with typical data entry (e.g. paper forms, PDF forms, Word Forms) are error-prone, offer no real workflow and are extremely time-consuming to manage. Web portals or Intranets are expensive to

deploy and maintain, and are slow to deploy. email2'secure e-Forms module combined with our powerful API provides a quick and effective way to deploy forms on any website, and allow your prospects, customers, partners and stakeholders to securely submit information for automatic integration into any third party application such as your CRM, ERP or EMR. Some of the benefits include:

- Both transport and storage of data submitted is encrypted and secure
- Deployed within minutes using any coding or platform
- Offered as SaaS or on –Premise (we can host the form for you or embed into your web pages seamlessly)
- Forms and fields can be designed specifically to your business process needs
- API delivers form data as an XML, EDI, HTML, TXT, CSV, etc. including business intelligence systems
- Eliminate costly paper, phone, fax and courier based processes
- Securely deliver forms directly to employees inboxes, without the need re-route the information or ask employees to switch between systems to accomplish their daily tasks

Desktop App:

- The Desktop App acts as a secure productivity agent & notifier. It displays an icon in your PC system tray or Mac Finder and lets you know instantly when you have new or when your secure messages are read, replied to, forwarded, all without having to open a web browser. The Desktop App also offers some convenient shortcuts to create secure messages and send/share large files securely.

The Desktop App is also responsible for the installation and management of the Secure Virtual Printer (PC only), all asynchronous resumable uploads/downloads of large files, and local desktop API integrations. It can easily be installed from your Secure Webmail client account.

Secure Virtual Printer:

- Send printed data securely from within any third party application such as ERP or CRM, instead of unsecure PDF, fax or overnight courier.

email2's unique virtual printer allows sending traditionally printed material as a secure message, to any recipients. It installs on your computer just like any other regular printer driver and can be used from within any application such as CRM, ERP, EMR, and even directly from your scanner. Additional security options include password authentication every time the virtual printer is used (Server Edition). Send printed data securely instead of unsecure PDF, fax or overnight courier. (Current support for Windows PC).

Secure & Private Video Messaging:

- Communicate internally and externally via secure voice & video messaging, directly through your standard email programs.
- Record personal messages to clients that accompany a message or file attachment, providing a more personal explanation. Executives can now record secure podcasts from their desk and share them in confidence.

The email2 platform offers the ability to send voice and video messages using the integrated attachment-free video messaging, with a webcam. No more additional third-party software or codec installation is required. You can

stream video directly onto your Private Email Network, record it securely, and have your recipients watch the video message using the same streaming, permission-based technology. For example, doctors can record personal messages to patients that accompany a message or file attachment, providing a more personal conversation. Executives can now record secure podcasts from their desk and share it in confidence with part or all of their staff on a weekly basis. Franchisors can also create marketing oriented podcasts to all their franchisees seamlessly.

Simply press the record button in the 'Video Message' section of the Deliver Slip and it will automatically start securely streaming the video directly to the Private Email Network's media server. When your recipient receives the video message, all he or she needs to do is click the Play button to begin watching it. Playing and recording videos only requires the Adobe Flash plug-in (Macromedia Streaming Server RTMPE), which is already present on most computers.

User Group, Email Aliases & Legal Disclaimers Management:

- Enable automatic assignment of special privileges and feature set access based on email domain through custom Membership Packages. Allow secure communications with internal and external parties such as partners, clients and off-site employees with minimal training and appropriate permissions. Disable feature access such as 'Message Recall' per user-group or Private Email Network.
- Email aliases can be self configured by each Member under the 'Tools' section of the Webmail client, or set by the Administrator on behalf of the Member.
- Custom notifications allow legal disclaimers can be added to any secure communication. Meet National and International email standards regulations and reduce liability risks.

User Group Management & Membership Packages

User Identity verification is performed when a user registers with a Private Email Network and becomes a member. Email address ownership is confirmed by a challenge during registration that requires an activation code (optional). Depending on how the user registers, this activation code may be provided transparently. In other cases, it will be provided in an email message. If a member sends a secure message to an individual that is not using the Private Email Network, the recipient will receive a customizable invitation message via basic email to register with the specific branded Private Email Network and then retrieve the message securely. This can be disabled by the Administrator for situations where the Private Email Network is "closed" and new members must be explicitly authorized by the Administrator.

-Every user or member of your Private Email Network is automatically assigned a Membership Package that dictates their level of functions. Each Membership Package can be upgraded or downgraded at a later time by the Administrator or be automatically provisioned via the email2 API. While the email2 platform does not allow deletion of members from the Private Email Network (for auditing purposes), members that do not require access can be set as 'Disabled' preventing them from accessing your Private Email Network. Every single function of the email2 platform is driven through the Membership Packages. Design your own specific Membership Packages to allow your clients to only use the Secure Webmail client, rename the navigation tabs to reflect how your organization works, restrict video messaging, who can invite new members, and more.

Email Aliases Management

Email aliases are often created within an organization so that multiple versions of an email address can reroute all traffic to a final email account. The email2 platform supports email aliases and allows each member of a PEN to define as many email aliases as necessary, and only count as a Guest license for billing purposes.

Email aliases can be self configured by each Member under the 'Tools' section of the Webmail client, or administered by the Administrator on behalf of the Member. Before adding an email aliases for a member, ensure that the user has access to the basic email account for the email address as they will need to manually confirm ownership of the email account.

Legal Disclaimers Management

-Email legal disclaimers are statements that are appended to outgoing messages. The email2 platform offers full management of custom legal and non-legal disclaimers. The content of the 'disclaimer' message is managed by the Administrator from a single source and can be added as a variable several ways (one-to-many relationship):

- Injected automatically 'server-side' to every secure email2 message at the database level so there is no room for error (automatic server side injection to every thread on 'send'), and/or
- Included automatically with every secure email2 message notification (email2 message notifications are what recipients not using the email2 Toolbar see in their regular email inbox, containing a link to access the secure Webmail client), and/or
- Some additional disclaimers can be added throughout the application such as the login screen, invitation message, etc.