RMail™
By RPOST

Email Security

Email Privacy & Compliance
Feature Spotlight

Explore Our
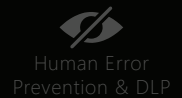Secure Email
Services

»

Email Privacy &
Compliance

Human Error
Prevention & DLP

Targeted Attack
Pre-emption

Certified Proof of
Content Delivered

Outbound AI
Security Stack

APPLIED

▶▶ Customer Stories

Applied Systems is the world's largest insurance agency management platform. Their customers have trusted RMail email security for more than a decade. Now Applied Systems is building the newest RMail innovations – its AI-infused impostor email and human error protection suite plus dynamically simplified email encryption – into its main platforms, OEM-esque.

California	70+	100%	190+	
R&D	Patents	AI-Infused	Countries	www.RMail.com

RMail™
By RPOST

Why We Are Unique

Our features provide the best user experience. Our prices make us the most affordable. And our services connect elegantly inside your existing email programs and business systems.

Email Privacy & Compliance

SMARTR Email Encryption
Dynamically adapting encrypted email ensures elegantly easy; simple for recipient means happy sender. Far beyond opportunistic TLS, RMail encrypted email service smartly adapts to provide peace-of-mind with end-to-end encryption, secure file sharing, auditable proof of fact of GDPR and HIPAA privacy compliance, email thread security monitoring, and more.

Human Error Prevention & DLP

Mutating the DNA of Data Leaks
Automatically sensitize users of their need to treat certain messages differently, seamlessly and in the flow of email and work, with in-the-moment-of-sending, bite sized insights and alerts. Empower your people and prevent data loss with AI-Infused and automated rules-based email compliance and security recommendations.

Targeted Attack Pre-emption

Intercepting the Human Instinct to Please
Nip cybercriminal-induced mis-wires (a/k/a wire fraud) with real-time alerts that expose whose email account is being eavesdropped on, which email addresses have tricky lookalike domains, and when a reply is about to be hijacked--must-have additional layers for your Business Email Compromise defense. Outbound Pre-Crime™ email security at its finest!

Certified Proof of Content Delivered

Proof of Who Said What When, by Email
Gain insights of the overall journey of your email, how popular who read what when, and receive forensic certified proof.

Outbound AI Security Stack

Perfect Harmony, Enhance the Outbound
Keep your existing inbound email security – and even your outbound DLP if you so choose. Add RMail outbound security gateway, in-the-inbox integrated cloud email security, and in-the-ether e-security content controls: all, some or one. RMail harmoniously extends your existing email security systems, adding elegantly-easy encryption user experiences, unique BEC targeted attack detection, and more, with AI DLP automation.

Breadth of Services
RMail empowers you; all of the functionality you need, all in one installation onto the platforms you're already using -- email encryption, certified proof, AI-infused human e-security error prevention, in-the moment personalized e-security training, and much more.

Simplicity
We understand that the power of e-security technology resides in user adoption. That is why RMail is built with AI that automatically sensitizes users to today's e-security and e-compliance needs, subtly nudging them to make the right email-related e-security decisions. Securing your business has never been easier.

Legal Proof®
Each message comes with a Registered Receipt™ email record; the global standard for court-accepted, timestamped proof of secure delivery of emails — and its attachments. This record is durable (it may be forwarded, retaining its self-authenticating integrity), and is self-contained (it does not require any other record to be stored anywhere).

Friendlier Service
Excellent technology is key, outstanding service is gold. Getting both in a single package is pure bliss. Our teams are more knowledgeable and friendlier to work with. That is why our customers rate us with 99% satisfaction scores and 5-star accolades.

Thank you, to the more than **25 million people** the world over, who have put their trust in our team and technology, **since 2000**.

USDA · Allianz ⑪ · BT · Claro · GT GreenbergTraurig · THE DOCTORS COMPANY · Coca-Cola · PANDA EXPRESS · UNITED NATIONS

RMail Security Flow

RMail Outbound Cloud Security Platform most often acts as an extension of one's existing inbound email security filters and outbound DLP services, with specialized Email Eavesdropping™ protection, elegantly easy and automated email encryption, and more.
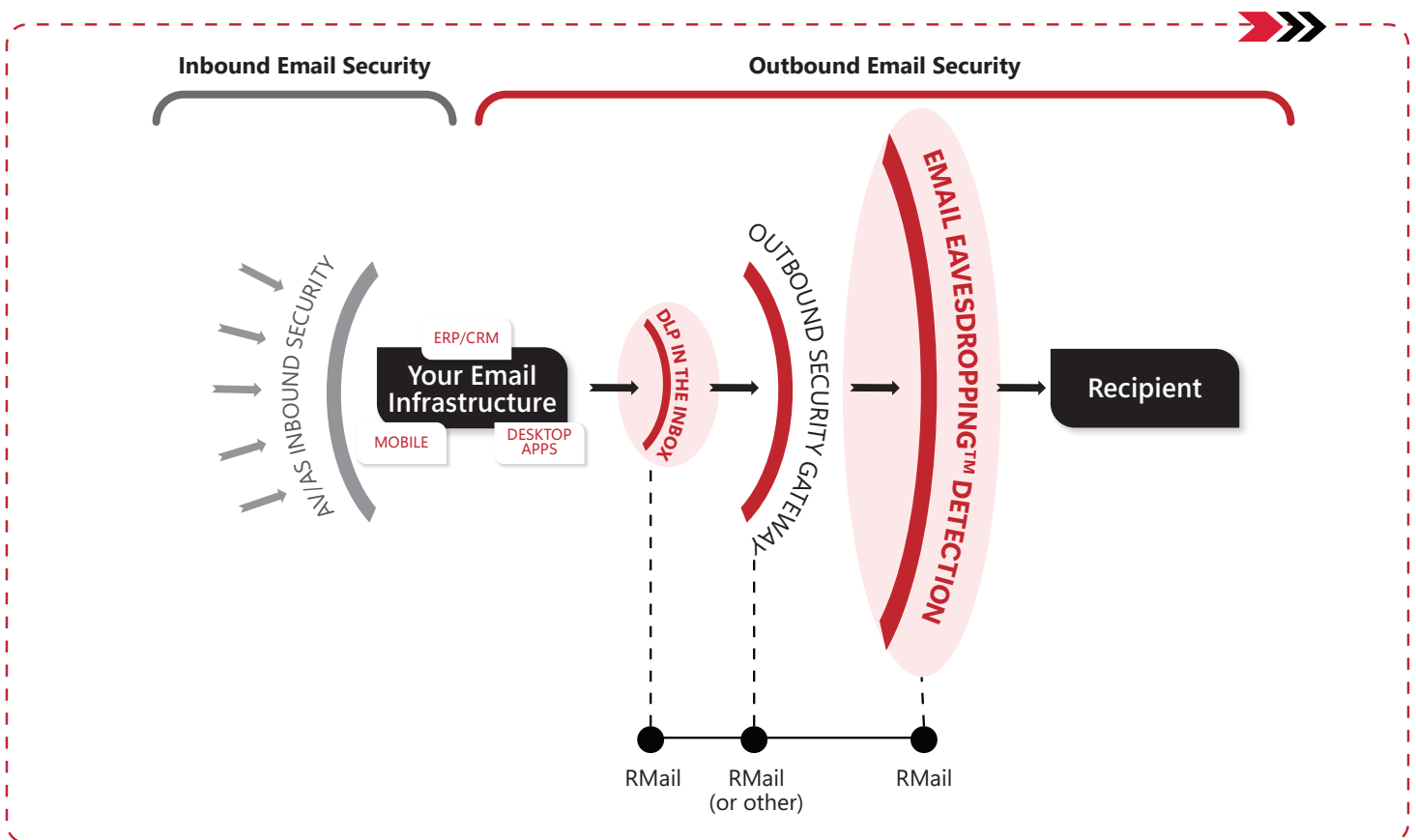

RMail services detect when a message should be sent encrypted and automatically transform it into a secure message that recipients can view with ease.

With Email Eavesdropping™ threat hunting, senders have peace-of-mind that they will be alerted in real time if a cybercriminal has compromised their recipient's email inbox, which is often the main step in lures leading to mis-wires.

RMail then sends aggregate Email Eavesdropping™ red-alerts to administrators and, if desired, to their managed security service provider as well.

All-in-One in the Inbox
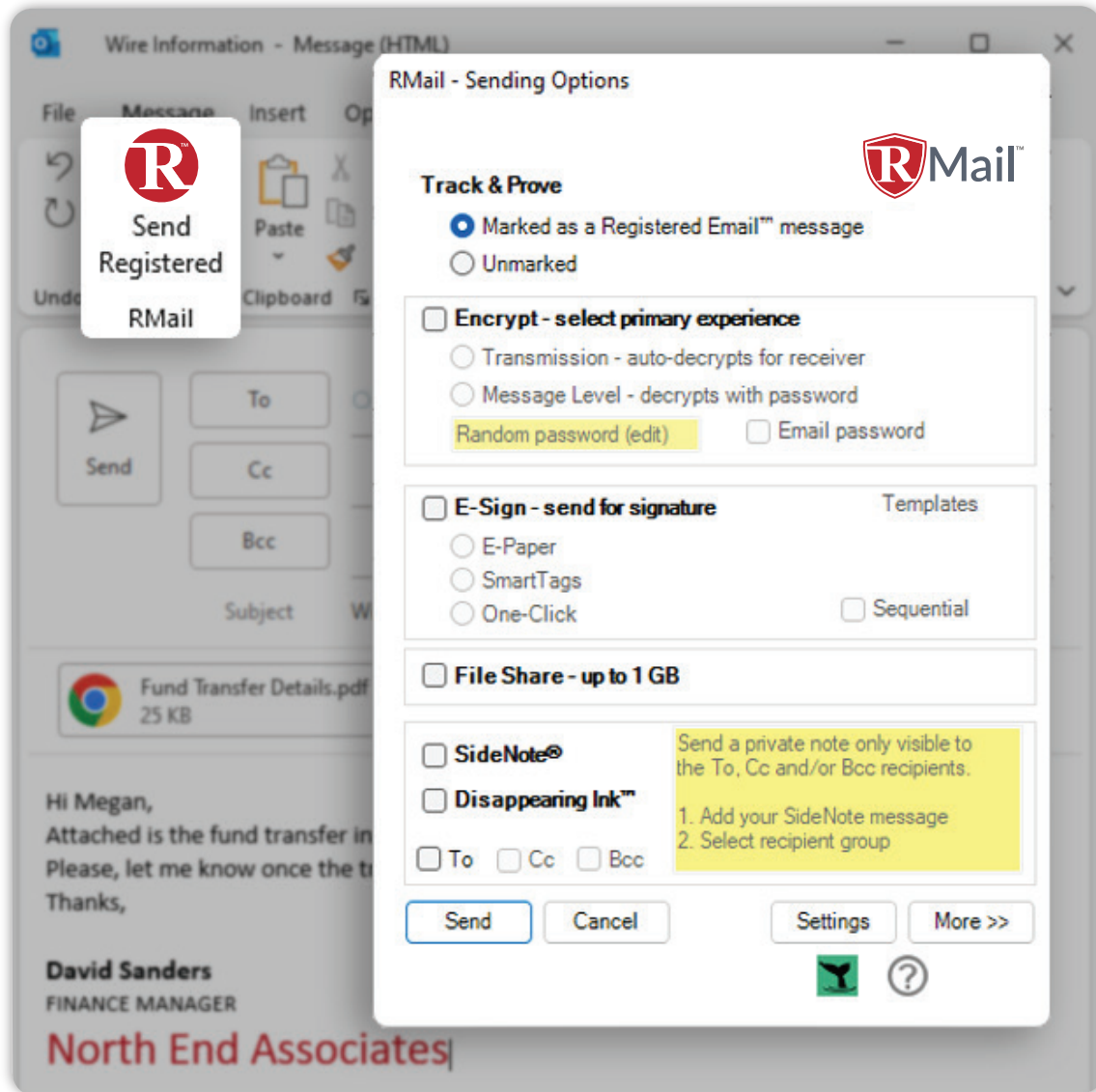
RMail installs seamlessly into Microsoft Outlook, Gmail, Salesforce and more to empower users with its full set of email security, DLP, privacy compliance and productivity tools at the click of a button.

RMail™
By **R**POST

RMail Recommends™ DLP in the Desktop
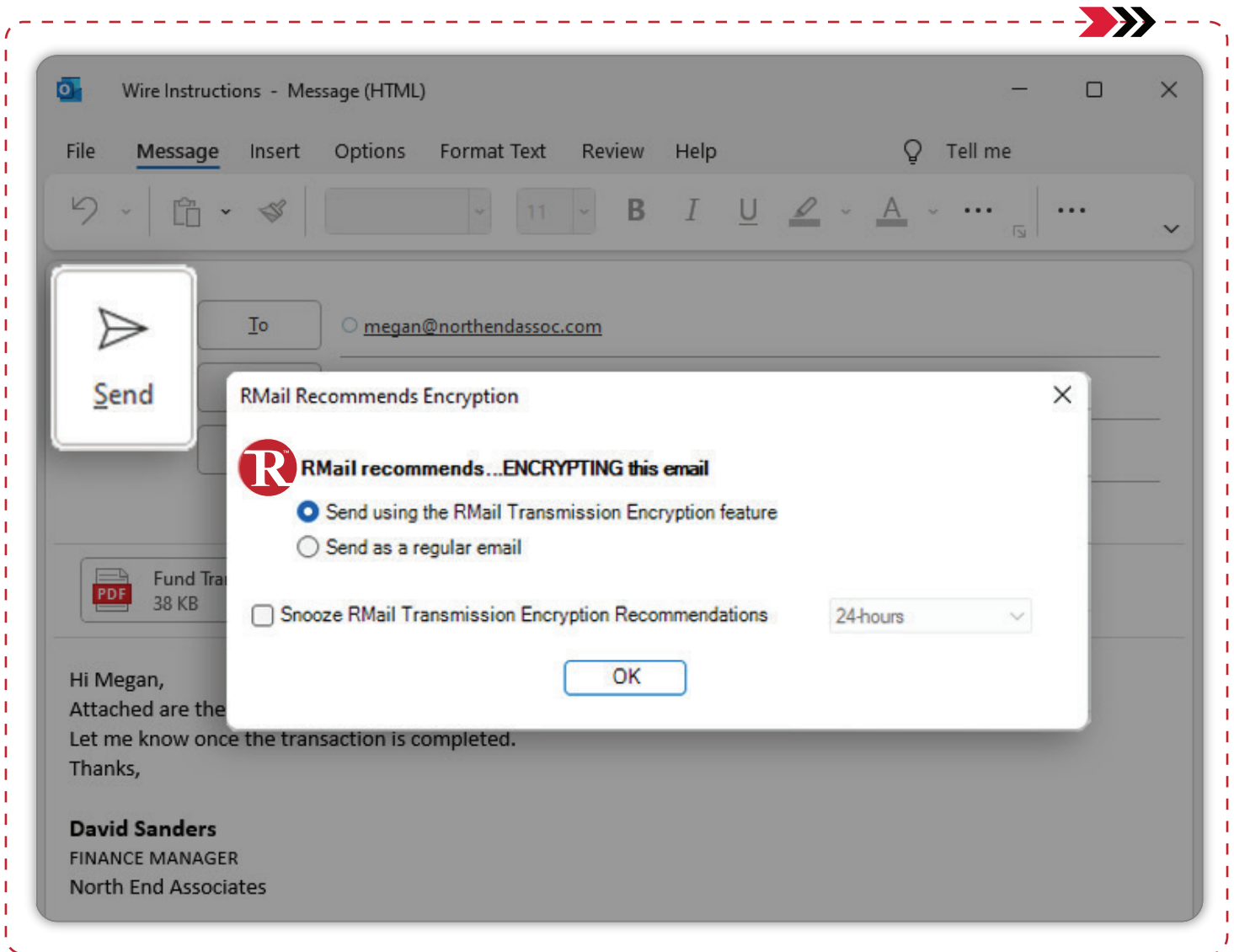
RMail automatically sensitizes users to the need to treat certain email with special care; and then transforms the message with specialized security in mind. This is true DLP in the desktop, no server settings or routings needed. For the sender, it's just like sending any other email. For IT admins, it's peace of mind with pure email security and compliance bliss.

SMART**R**™ Encryption
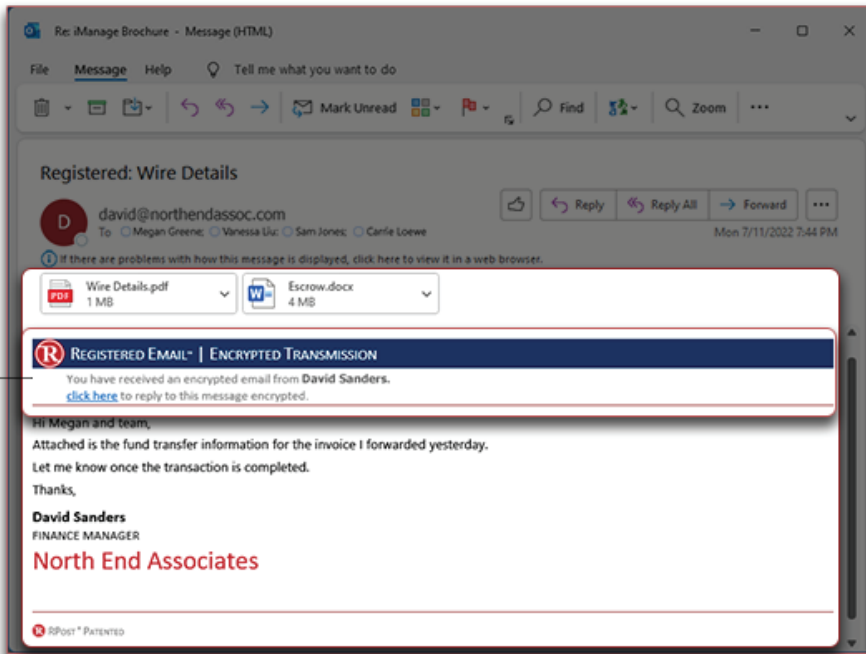
Transmission Preferred Encryption: RMail's default settings first attempt transmission level encryption at the minimum sender-acceptable security level, and deliver the encrypted email right to the recipient's inbox, providing the same familiar user experience as a normal email: **without any logins, links or need to create an account.** Recipients even have the option to reply encrypted.

R REGISTERED EMAIL™ | ENCRYPTED TRANSMISSION

You have received an encrypted email from **David Sanders. click here** to reply to this message encrypted.

Benefits:
- The banner adds confidence for the receiver that the information was shared securely
- Familiar user experience
- No logins, links or need to create an account

click here to reply to this message encrypted.
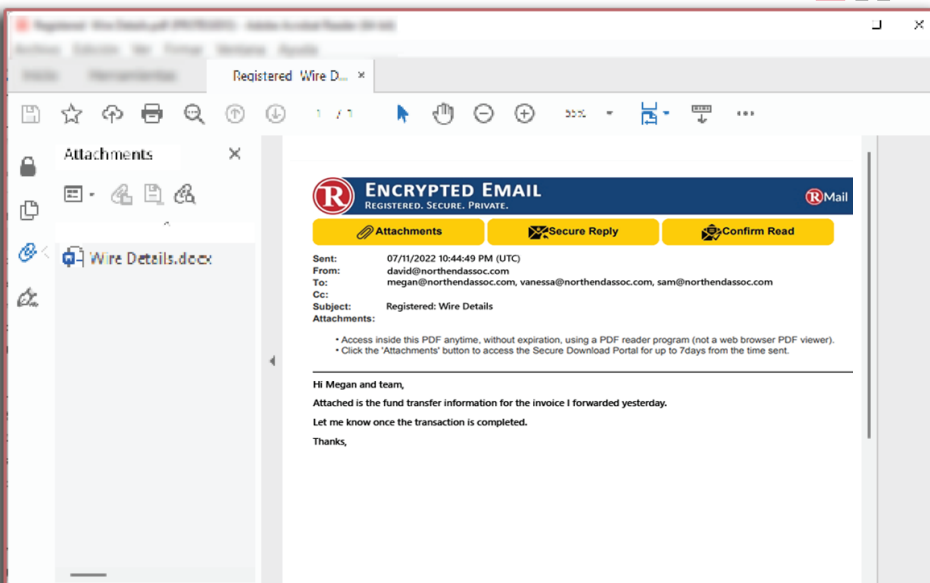
Benefits:
- Recipient can reply encrypted
- Option to attach up to 200MB of files securely in the reply

SMART**R**™ Encryption
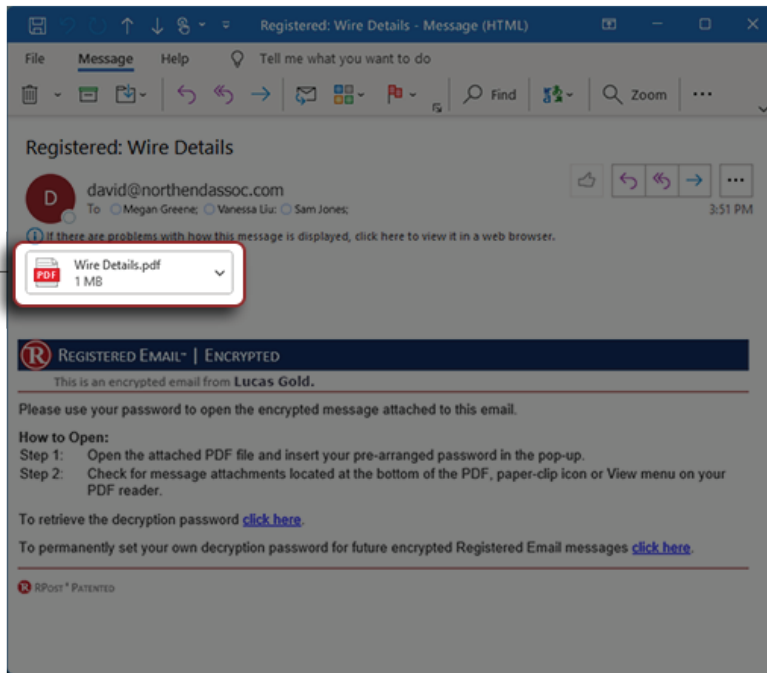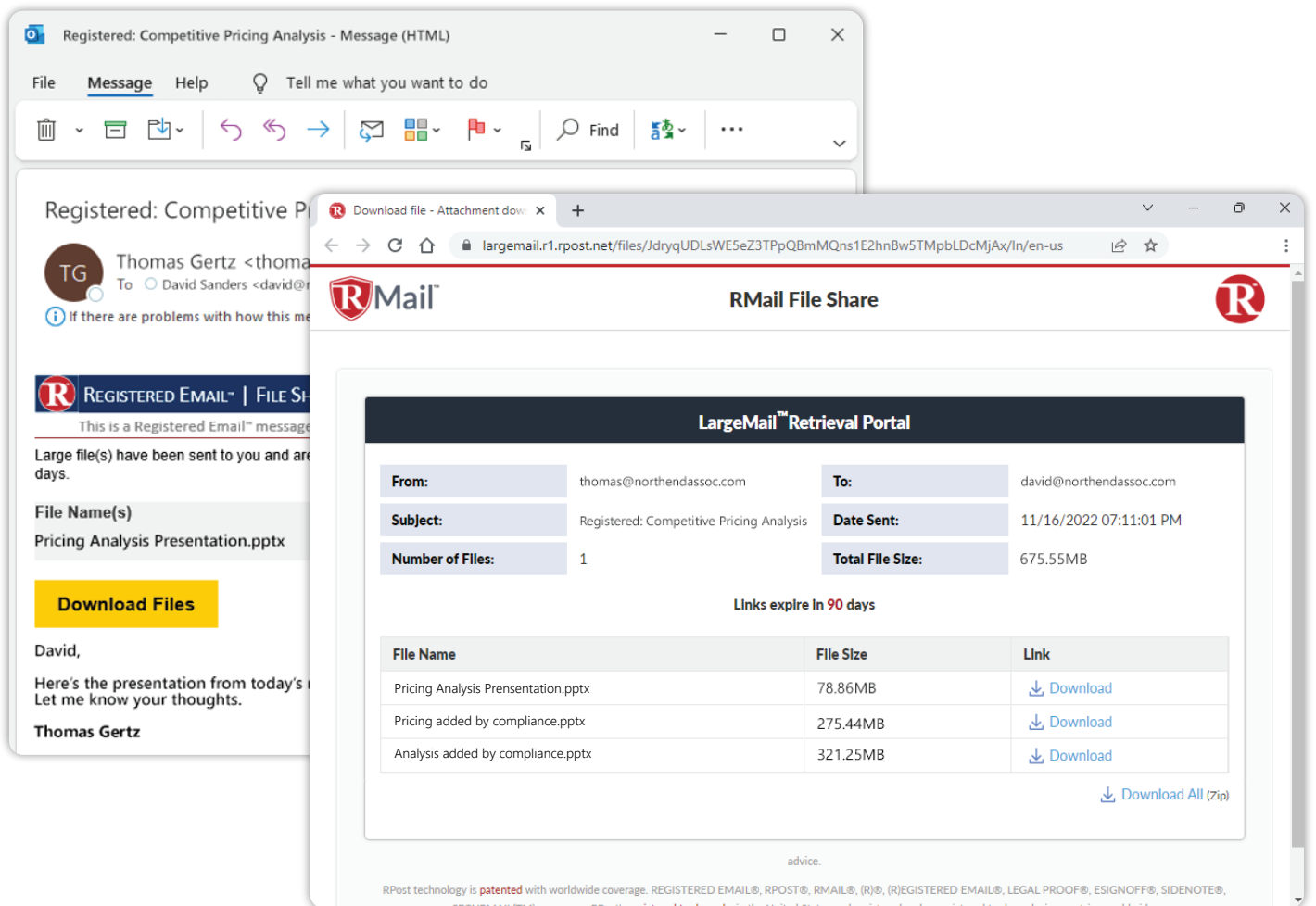

Message Level Encryption
RMail dynamic encryption engine detects whether the recipient's server is able to receive the email at the minimum sender-acceptable security level and, if not, automatically reverts to message level encryption, wrapping the email and any attachments inside an AES-256-bit encrypted PDF package, delivered into the recipient's inbox, with automated decryption password management.

Benefits:
- Message and attachments remain encrypted at rest in the recipient's inbox
- Familiar and easy PDF user experience for reader
- The email opens in any browser or PDF reader
- Digitally signed, integrity visible in the PDF reader
- Recipient can access the attachments in any browser with a simple click, or directly in their PDF reader

RMail By RPost

Email Security

Secure Large File Share™ Send Up to 1GB from within Outlook

Senders can easily attach and track up to 1GB of files right from inside the Outlook compose window -- or any of the RMail web applications. Senders can send large files securely to any recipient with encryption and configurable self-purging options (from 1 to 90 days) through a secure web container that eliminates the risk of download recipients being able to see sender's cloud storage file structure.

Plus, files auto-purge after 1 to 90 days (configurable) and can be killed early at any time by the sender. No files linger on the Internet – pure compliance bliss.

Digital Seal®: Authenticate True Email Content & Sender
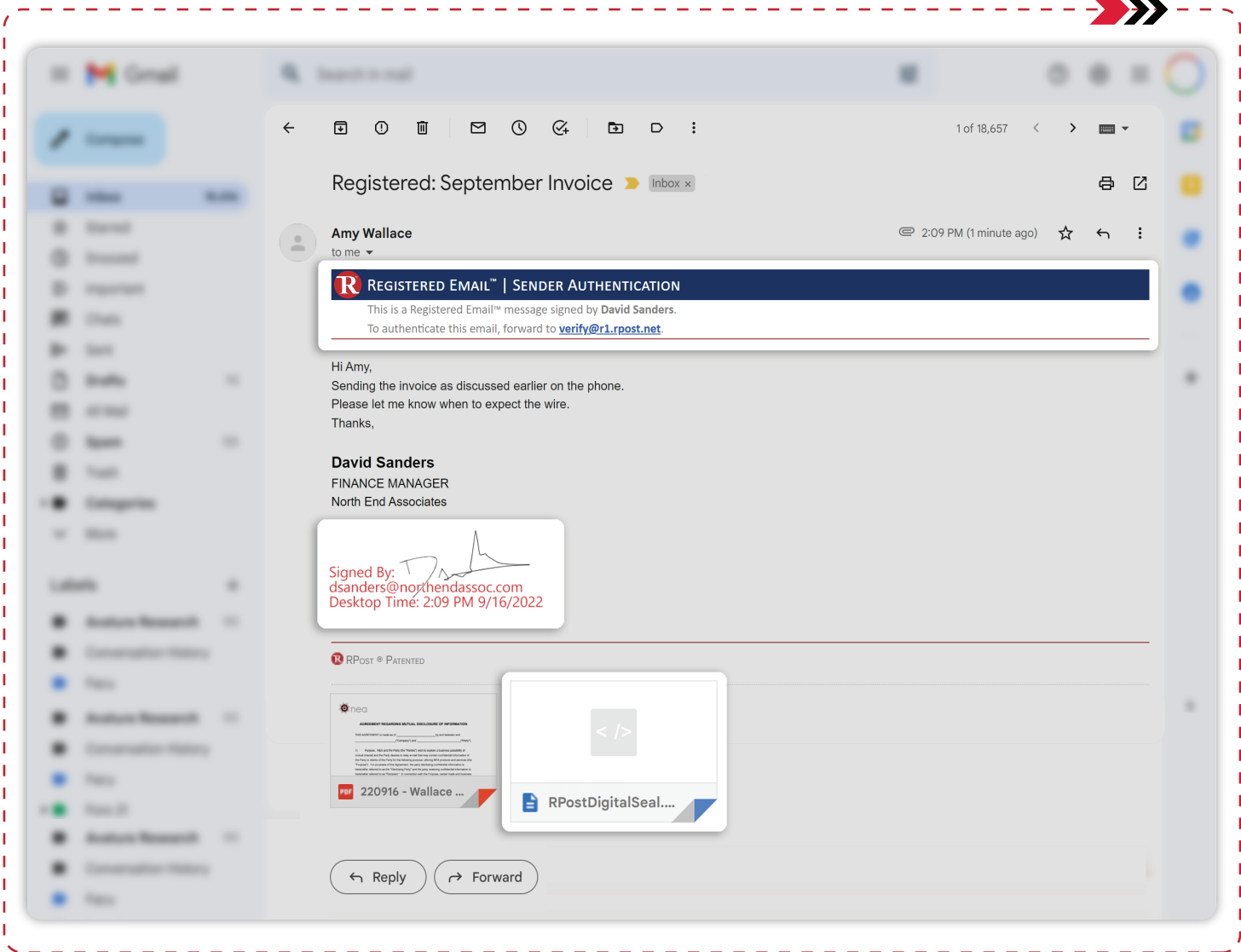
RMail Digital Seal® authentication makes it easy for a recipient to verify origin and authorship of an email (for example, an email carrying an invoice) and re-create a copy of the original message content instantly. This empowers the recipient of the invoice to verify authenticity of payment information in real-time, anytime, before paying.

Security Breach Locator™ Report

REGISTERED ENCRYPTION™
CERTIFICATE EVIDENCING END-TO-END SECURITY

This privacy certificate provides proof of the privacy status of the associated email, from the original sender through to each recipient. Together with the Registered Receipt™ it is attached to, a user may authenticate the data in this certificate along with the original message content and all of the delivery history and timestamp details. To authenticate the information in this certificate, follow the instructions on the associated receipt. Patented and Pending US 16866135.

Message Envelope

Message ID:	C8737FB9CF1519A2053C44E0056FDF5C39DDB645
From:	MelanieJames <mjames@newinsurance.com>
Subject:	Policy Updates
To:	<wanda.mcgrath@holdingsusa.net> <jonathan.ogden@holdingsusa.net> <richard.clark@associatesolutions.net>
Cc:	
Bcc:	-
Received by RMail System:	05/26/2022 07:39:38 PM (UTC)
Client Code:	-

Outbound Details: Sender to RMail Cloud / Inbound Details: RMail Cloud to Recipient

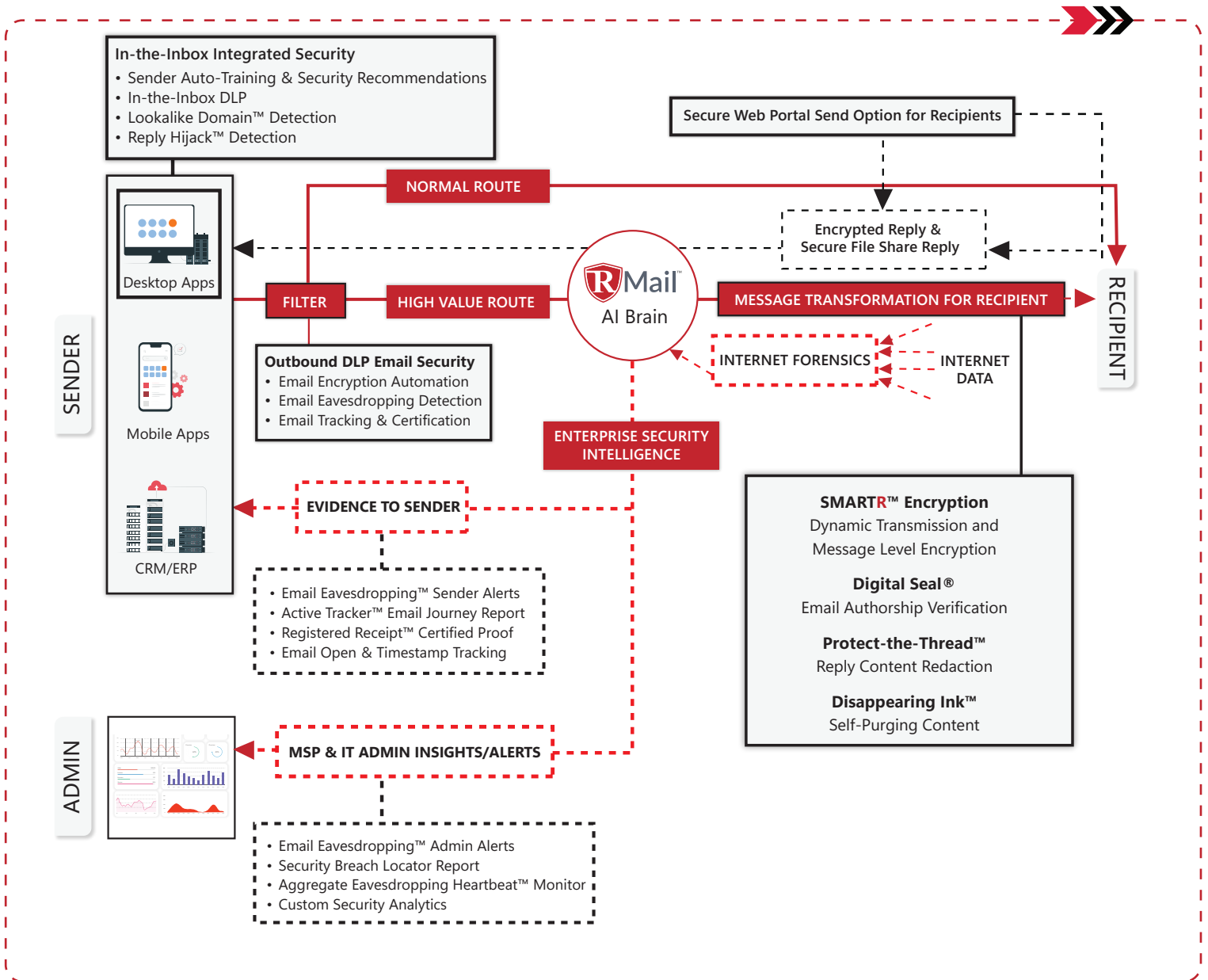| Original Sender	Internet Hop ID	Security Details Message Level	Security Details Transmission	Time Inducted	Encryption Status	End Recipient	Security Details Message Level	Security Details Transmission	Time Received	Encryption Status
mjames@newinsurance.com	smtp13.relay.iad3a.emailsrvr.com (Authenticated sender: mjames-AT-newinsurance.com)	RSA-AES256	TLSv1.2*	05/26/2022 07:39:34 PM (UTC)	Best+	wanda.mcgrath@holdingsusa.net		TLSv1.2	05/26/2022 07:39:38 PM (UTC)	Best
mjames@newinsurance.com	smtp13.relay.iad3a.emailsrvr.com (Authenticated sender: mjames-AT-newinsurance.com)	RSA-AES256	TLSv1.2*	05/26/2022 07:39:34 PM (UTC)	Best+	jonathan.ogden@holdingsusa.net		TLSv1.1	05/26/2022 07:39:38 PM (UTC)	Acceptable
mjames@newinsurance.com	smtp13.relay.iad3a.emailsrvr.com (Authenticated sender: mjames-AT-newinsurance.com)	RSA-AES256	TLSv1.2*	05/26/2022 07:39:34 PM (UTC)	Best+	richard.clark@associatesolutions.net	PDF-AES256	TLSv1.0	05/26/2022 07:39:38 PM (UTC)	Best+

End-to-End Security Summary

Original Sender	Original Recipient	Overall Encryption Status	Status Description
mjames@newinsurance.com	wanda.mcgrath@holdingsusa.net	★★★★☆	Best encryption from sender device, best to recipient gateway
mjames@newinsurance.com	jonathan.ogden@holdinsusa.net	★★★☆☆	Best encryption from sender device, acceptable to recipient.
mjames@newinsurance.com	richard.clark@associatesolutions.net	★★★★★	Best encryption from sender device, best+ to recipient.

For more information about RMail® services, visit www.rmail.com.

An RPost® Technology

If an email is identified as being eavesdropped on, the Registered Encryption™ report identifies the most likely security gaps; **and/or provides audit-ready proof that the security gap must have been after the recipient forwarded the message onward --- and not a fault of the sender.**
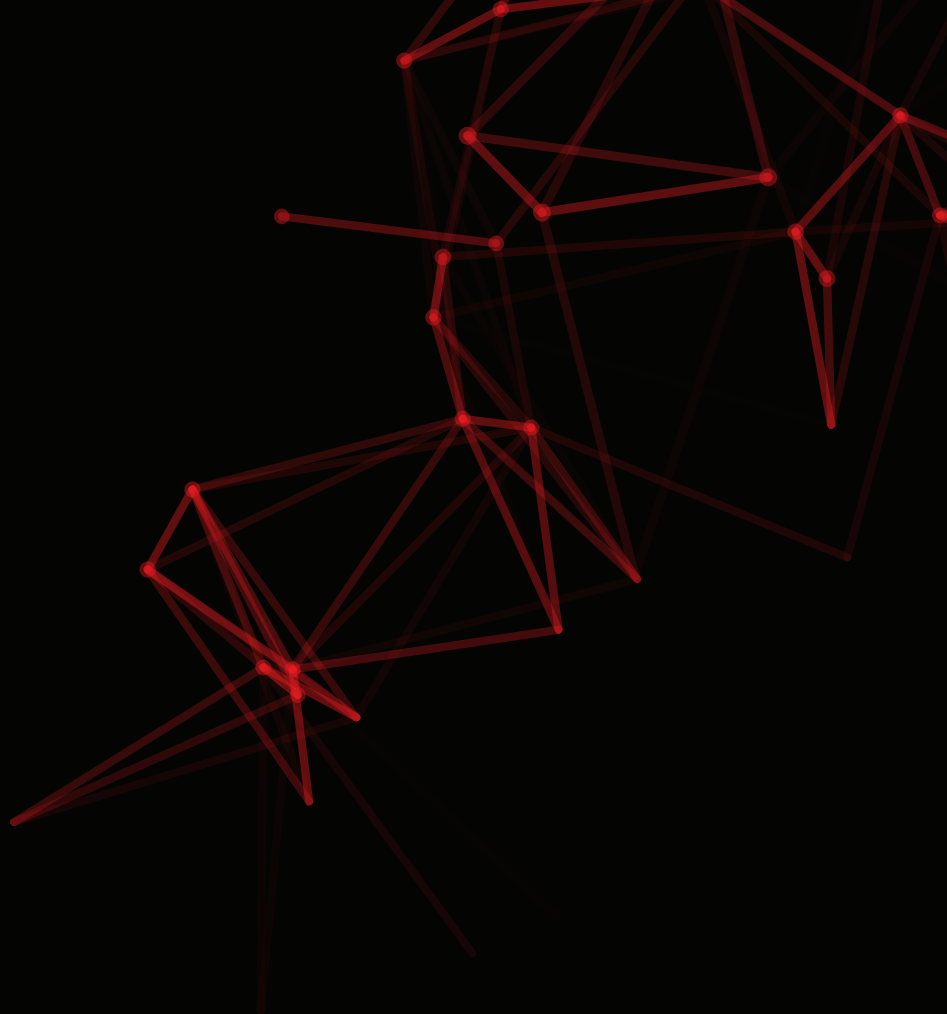
The security forensics provided by RMail are fact, and allow IT admins to easily justify and demonstrate their hypothesis about where cybercriminals may have accessed an email in the path from sender to recipient, even if the breach occurred at the recipient's end.

RMail Outbound Security Cloud

In-the-Inbox Integrated Security
- Sender Auto-Training & Security Recommendations
- In-the-Inbox DLP
- Lookalike Domain™ Detection
- Reply Hijack™ Detection

Secure Web Portal Send Option for Recipients

NORMAL ROUTE

Encrypted Reply & Secure File Share Reply

Desktop Apps

FILTER — HIGH VALUE ROUTE

RMail AI Brain

MESSAGE TRANSFORMATION FOR RECIPIENT

RECIPIENT

INTERNET FORENSICS — INTERNET DATA

Outbound DLP Email Security
- Email Encryption Automation
- Email Eavesdropping Detection
- Email Tracking & Certification

Mobile Apps

ENTERPRISE SECURITY INTELLIGENCE

SENDER

CRM/ERP

EVIDENCE TO SENDER

- Email Eavesdropping™ Sender Alerts
- Active Tracker™ Email Journey Report
- Registered Receipt™ Certified Proof
- Email Open & Timestamp Tracking

SMARTR™ Encryption
Dynamic Transmission and Message Level Encryption

Digital Seal®
Email Authorship Verification

Protect-the-Thread™
Reply Content Redaction

Disappearing Ink™
Self-Purging Content

ADMIN

MSP & IT ADMIN INSIGHTS/ALERTS

- Email Eavesdropping™ Admin Alerts
- Security Breach Locator Report
- Aggregate Eavesdropping Heartbeat™ Monitor
- Custom Security Analytics

Perfect Harmony, Enhance the Outbound

Keep your existing inbound email security – and even your outbound DLP if you so choose. Add RMail outbound security gateway, in-the-inbox integrated cloud email security, and in-the-ether e-security content controls: all, some or one. RMail harmoniously extends your existing email security systems, adding elegantly-easy encryption user experiences, unique BEC targeted attack detection, and more, with AI DLP automation.