RMail™
By RPOST

Email Security

Certified Proof of Content Delivered
Features Spotlight

Explore Our Secure Email Services

Email Privacy & Compliance

Human Error Prevention & DLP

Targeted Attack Pre-emption

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.

Certified Proof of Content Delivered

Outbound AI Security Stack

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

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.

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.

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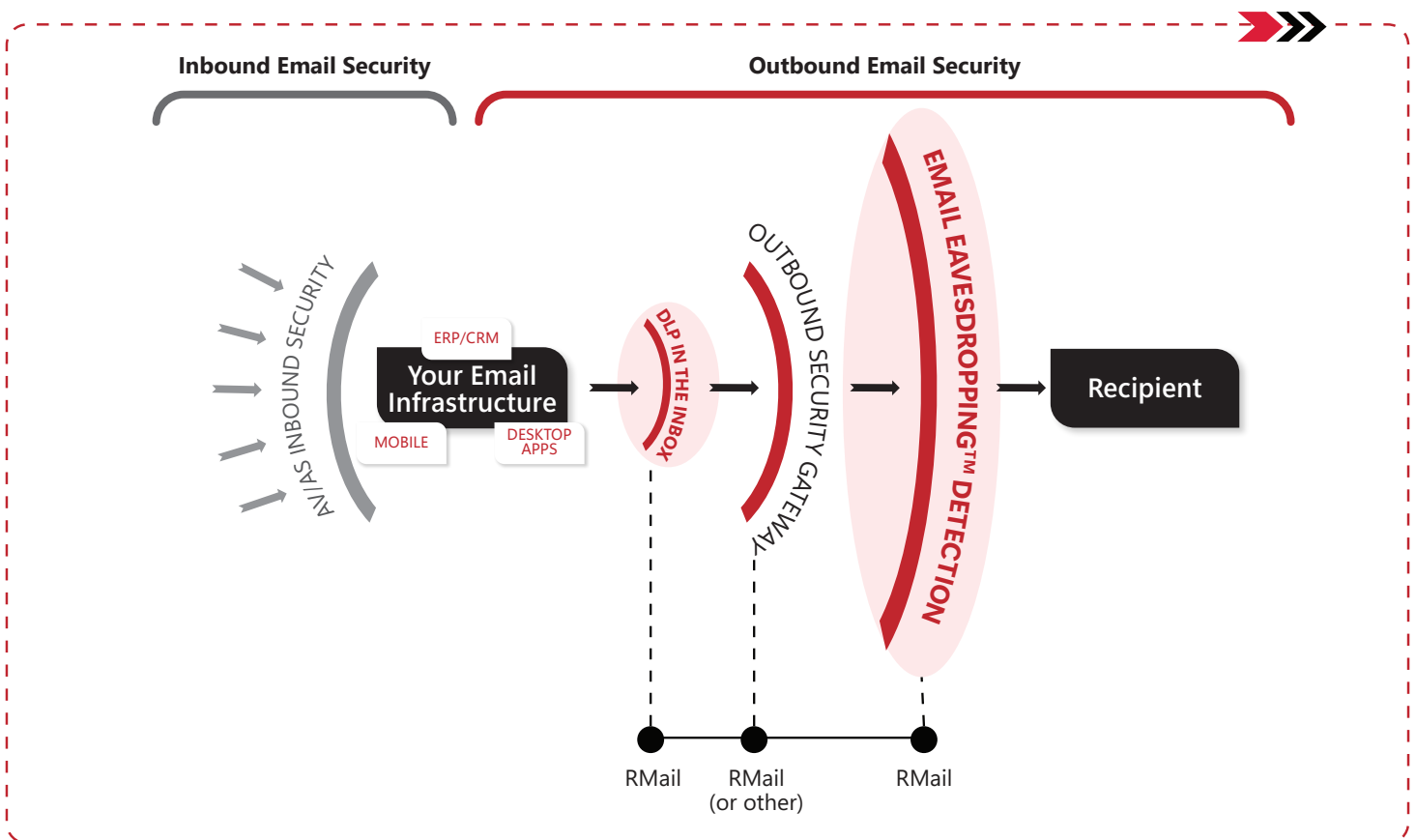
Friendlier Service
Excellent technology is key, outstanding service is gold. Getting both in a single package is pure bliss. Our teams are more knowledgeable and friendlier to work with. That is why our customers rate us with 99% satisfaction scores and 5-star accolades.

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.


Inbound Email Security   **Outbound Email Security**

AV/AS INBOUND SECURITY

ERP/CRM
Your Email Infrastructure
MOBILE   DESKTOP APPS

DLP IN THE INBOX

OUTBOUND SECURITY GATEWAY

EMAIL EAVESDROPPING™ DETECTION

Recipient

RMail   RMail (or other)   RMail

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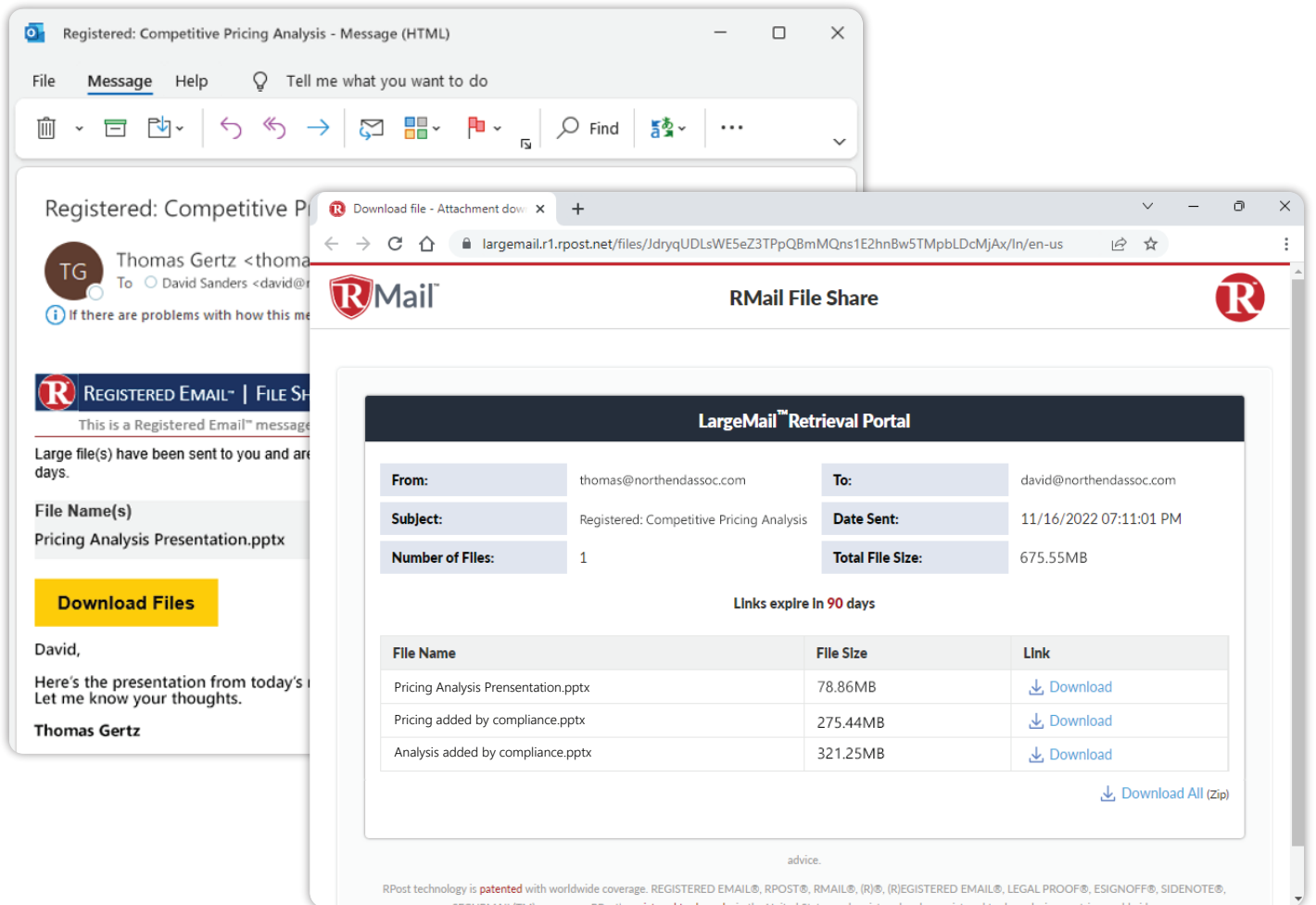
RMail then sends aggregate Email Eavesdropping™ red-alerts to administrators and, if desired, to their managed security service provider as well.

Email Security

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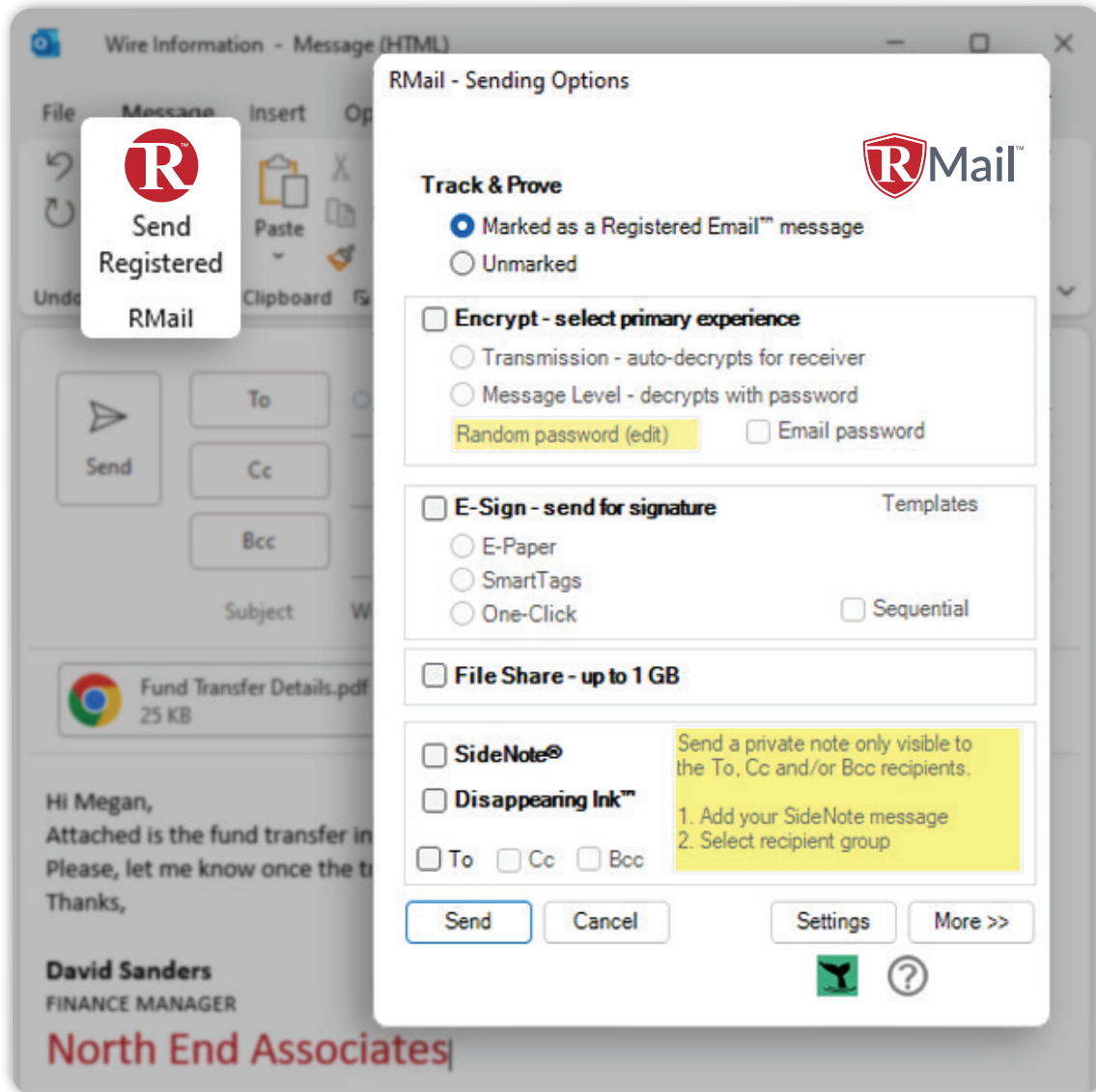
RMail installs seamlessly into Microsoft Outlook, Gmail, Salesforce and more to empower users with its full set of email security, DLP, privacy compliance and productivity tools at the click of a button.

RMail By RPost™

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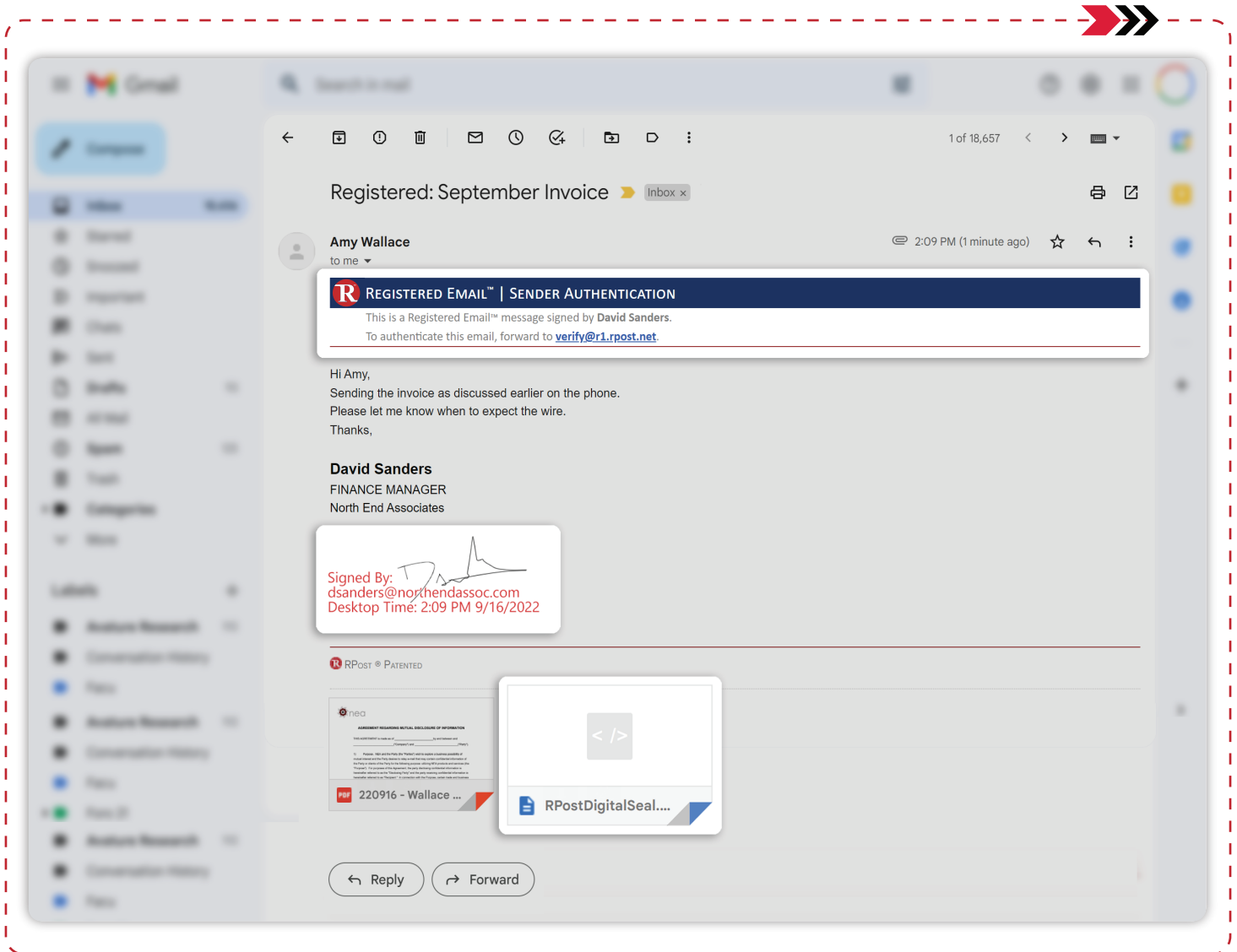
RMail Digital Seal® authentication makes it easy for a recipient to verify origin and authorship of an email (for example, an email carrying an invoice) and re-create a copy of the original message content instantly. This empowers the recipient of the invoice to verify authenticity of payment information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

Legal Proof®: Email Content Delivered

The Power of Proof™:
The Registered Receipt™ email record is a durable, self-contained, and self-authenticating proof record of the entire email transaction, returned to the sender for each Registered Email™ sent. The Registered Receipt™ authenticates and accurately reproduces the original email including attachments, without RMail or any third party storing a copy of the email, attachments or records.

HTML file reconstructs the transaction, is durable and self-contained.

Message status and metadata of the transaction is contained in XML format or can be extracted via API.

Legal delivery time, synched to the Government Atomic Time

Legal delivery status

Legal time of sending

Record of encrypted transmission

Record and identifiers for proof of attachment content

Legal forensic metadata

Benefits:
- The Registered Receipt™ is the only evidence that needs to be stored to reconstruct the original transmission
- Self-authenticates without the need for third-party storage
- Reconstructs the entire transaction in native format, including content and attachments
- Can be forwarded for recipients to authenticate

Legal Proof®: Email Content Delivered

Authentication Record:
Authentication Record: When a Registered Receipt™ email record is submitted to RMail, our systems authenticate the receipt's integrity and, if authentic, reconstruct the original message content along with forensic evidentiary transaction data.

The Receipt Authentication record reconstructs the original transaction without any storage anywhere except the Registered Receipt itself. And, if the original email was sent encrypted, the reconstructed message content also proves fact of encrypted delivery.

The Receipt Authentication record includes SMTP logs, SMTP history, HTTP records and DSN records.

The Authentication record reconstructs original email, including email content and attachments.

Email Lifecycle & Popularity Report

Email Activity Report

Active Tracker™ Intelligence

Original Recipient: jim@insurancegrp.com

Security:	Green
Opens:	3
Locations:	2

Senders can now gain insights into the popularity of their email and the amazing journey their message takes as it is forwarded along.

Risk Details

Time	Activity	Detail	Locale	Location: Country	Location (IP)	Network	Risk
09/15/2022 08:12:46 UTC	Open	M	Frankfurt, Hesse	Germany	52.72.5.168	T-Mobile	Green
09/13/2022 12:54:18 UTC	Open		Boston, MA	USA	94.92.53.178	Verizon	Green
09/12/2022 02:15:17 UTC	Open		Boston, MA	USA	94.52.53.178	Verizon	Green

Original Message Details
Original Send Time: 09/12/2022 1:33:52 UTC
Transaction ID: E64B9039C2CE5914F42EE61BCADAB09C55B94832

Metadata:

[IP Address: 41.67.191.255] [Time Opened: 09/15/2022 08:12:48 AM] [REMOTE_HOST: 192.168.10.153] [HTTP_HOST: open.r1.rpost.net] [SCRIPT_NAME: /open/images/LGy25hw0Z65CNLyOLYzCLCuMKdk95gm4vir26bBCMDIx.gif] HTTP_ACCEPT:*/* HTTP_ACCEPT_ENCODING:gzip, deflate HTTP_HOST:open.r1.rpost.net HTTP_USER_AGENT:Mozilla/4.0 (compatible; ms-office; MSOffice 16) HTTP_X_FORWARDED_FOR:183.82.2.55 HTTP_X_FORWARDED_PROTO:https HTTP_X_FORWARDED_PORT:443 HTTP_X_AMZN_TRACE_ID:Root=1-632d2601-68f7d3e527e10ac35f151b35 HTTP_UA_CPU:AMD64 Accept: */* Accept-Encoding: gzip, deflate Host: open.r1.rpost.net User-Agent: Mozilla/4.0 (compatible; ms-office; MSOffice 16) X-Forwarded-For: 183.82.2.55 X-Forwarded-Proto: https X-Forwarded-Port: 443 X-Amzn-Trace-Id: Root=1-632d2601-68f7d3e527e10ac35f151b35 ua-cpu: AMD64 /LM/W3SVC/5/ROOT 256 2048 C=US, S=VA, L=Herndon, O=Network Solutions L.L.C., CN=Network Solutions DV Server CA 2 CN=tracking.rpost.com 0 CGI/1.1 on 256 2048 C=US, S=VA, L=Herndon, O=Network Solutions L.L.C., CN=Network Solutions DV Server CA 2 CN=tracking.rpost.com 5 /LM/W3SVC/5 192.168.10.186 /open/images/LGy25hw0Z65CNLyOLYzCLCuMKdk95gm4-vir26bBCMDIx.gif 192.168.10.153 192.168.10.153 46808 GET /open/images/LGy25hw0Z65CNLyOLYzCLCuMKdk95gm4vir26bBCM-DIx.gif open.r1.rpost.net 443 1 HTTP/1.1 Microsoft-IIS/8.5 /open/images/LGy25hw0Z65CNLyOLYzCLCuMKdk95gm4vir26bBCMDIx.-gif */* gzip, deflate open.r1.rpost.net Mozilla/4.0 (compatible; ms-office; MSOffice 16) 183.82.2.55 https 443 Root=1-632d2601-68f7d3e527e10ac35f151b35 AMD64

(M) = activity determined to be on a mobile device.
(VPN) = activity was detected at an anonymizing VPN endpoint location.
Location = registered location of the detected network.
Network = registered network associated with the internet protocol.

Email Security

Email Eavesdropping™ Alerts for Wire-Fraud Pre-Emption

Email Activity Report

Email Eavesdropping™ Alert

Original Recipient: David.Smith@northwestinsurance.com

Security:	Red
Opens:	3
Locations:	2

**Pre-empt cybercrime.
After the hook is in, before the steal.**

Email Age: 15 days 1 hour 4 minutes

Risk Details: All Activities

Time (UTC)	Activity	Location	Country	Network Addr.	Network	Risk
09/15/2022 08:12:48	Open (VPN)	Ikeja, Lagos	Nigeria	41.67.191.255	Netcom Africa	Red
09/13/2022 17:06:22	Open	Boston, MA	USA	94.92.53.178	Verizon	Green
09/13/2022 12:54:18	Open	Boston, MA	USA	94.52.53.178	Verizon	Green

Original Message Details
Subject: Weekly analysis
Original Send Time: 09/13/2022 03:20:00 UTC
Transaction ID: A4BD52B62EE9862A5FDDB8F336A99E2D69FEF54A

Metadata:

[IP Address: 41.67.191.255] [Time Opened: 09/15/2022 08:12:48 AM] [REMOTE_HOST: 192.168.10.153] [HTTP_HOST: open.r1.rpost.net] [SCRIPT_NAME: /open/images/LGy25hw0Z65CNLyOLYzCLCuMKdk95gm4vir26bBCMDlx.gif] HTTP_ACCEPT:*/* HTTP_ACCEPT_ENCODING:gzip, deflate HTTP_HOST:open.r1.rpost.net HTTP_USER_AGENT:Mozilla/4.0 (compatible; ms-office; MSOffice 16) HTTP_X_FORWARDED_FOR:183.82.2.55 HTTP_X_FORWARDED_PROTO:https HTTP_X_FORWARDED_PORT:443 HTTP_X_AMZN_TRACE_ID:Root=1-632d2601-68f7d3e527e10ac35f151b35 HTTP_UA_CPU:AMD64 Accept: */* Accept-Encoding: gzip, deflate Host: open.r1.rpost.net User-Agent: Mozilla/4.0 (compatible; ms-office; MSOffice 16) X-Forwarded-For: 183.82.2.55 X-Forwarded-Proto: https X-Forwarded-Port: 443 X-Amzn-Trace-Id: Root=1-632d2601-68f7d3e527e10ac35f151b35 ua-cpu: AMD64 /LM/W3SVC/5/ROOT 256 2048 C=US, S=VA, L=Herndon, O=Network Solutions L.L.C., CN=Network Solutions DV Server CA 2 CN=tracking.rpost.com 0 CGI/1.1 on 256 2048 C=US, S=VA, L=Herndon, O=Network Solutions L.L.C., CN=Network Solutions DV Server CA 2 CN=tracking.rpost.com 5 /LM/W3SVC/5 192.168.10.186 /open/images/LGy25hw0Z65CNLyOLYzCLCuMKdk95gm4-vir26bBCMDlx.gif 192.168.10.153 192.168.10.153 46808 GET /open/images/LGy25hw0Z65CNLyOLYzCLCuMKdk95gm4vir26bBCM-DIx.gif open.r1.rpost.net 443 1 HTTP/1.1 Microsoft-IIS/8.5 /open/images/LGy25hw0Z65CNLyOLYzCLCuMKdk95gm4vir26bBCMDlx.-gif */* gzip, deflate open.r1.rpost.net Mozilla/4.0 (compatible; ms-office; MSOffice 16) 183.82.2.55 https 443 Root=1-632d2601-68f7d3e527e10ac35f151b35 AMD64

RPost patented (rpost.com/patents) including US patent applications 17663425, 63/201,857, 63/366,685, 63/366,661 and other applications.

(M) = activity determined to be on a mobile device.
(VPN) = activity was detected at an anonymizing VPN endpoint location.
Location = registered location of the detected network.
Network = registered network associated with the internet protocol.

If the RMail **active threat hunting** technology identifies unusual activity patterns, RMail generates an Email Eavesdropping™ instant alert, and notifies in real-time IT admins (and optionally senders) with forensic details.

BEC lures start with cybercriminals targeting their victims by eavesdropping on email from sender to recipient, to siphon off email, analyze it, copy it with slight modifications (e.g., payment instructions), and then pivot replies so they route in a loop back to the cybercriminal.

With Email Eavesdropping™ alerts, every email sent out of the organization has every activity associated with it analyzed forensically, for a period of time. These alerts include all the email forensics so that IT security specialists can validate and take immediate action, **before the cybercriminal lures users into mis-wiring money to the criminal's bank.**

![RMail by RPost logo]

Security Breach Locator™ Report

REGISTERED ENCRYPTION™
CERTIFICATE EVIDENCING END-TO-END SECURITY

![RMail logo]

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

Original Sender	Internet Hop ID	Security Details		Time Inducted	Encryption Status
		Message Level	Transmission		
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+
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+
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+

Inbound Details: RMail Cloud to Recipient

End Recipient	Security Details		Time Received	Encryption Status
	Message Level	Transmission		
wanda.mcgrath@holdingsusa.net		TLSv1.2	05/26/2022 07:39:38 PM (UTC)	Best
jonathan.ogden@holdingsusa.net		TLSv1.1	05/26/2022 07:39:38 PM (UTC)	Acceptable
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
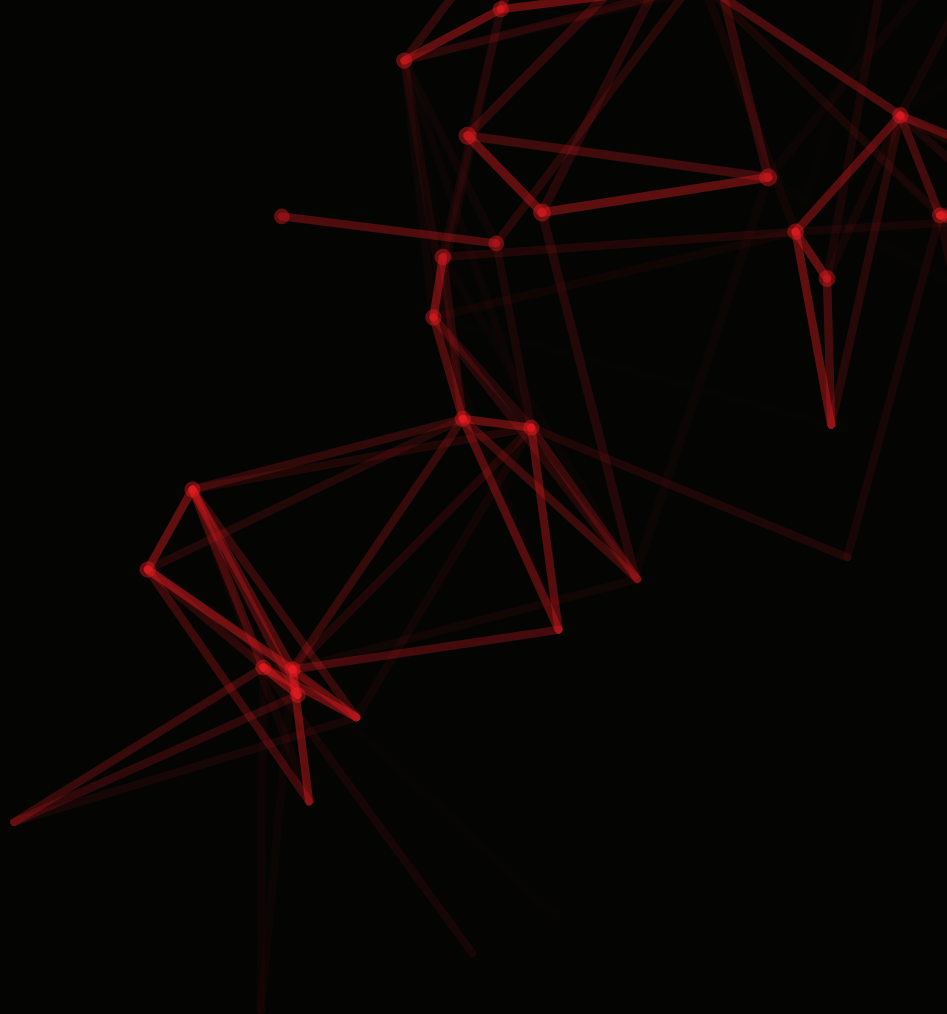- Sender Auto-Training & Security Recommendations
- In-the-Inbox DLP
- Lookalike Domain™ Detection
- Reply Hijack™ Detection

Secure Web Portal Send Option for Recipients

Desktop Apps

Mobile Apps

CRM/ERP

SENDER

NORMAL ROUTE

Encrypted Reply & Secure File Share Reply

FILTER

HIGH VALUE ROUTE

RMail AI Brain

MESSAGE TRANSFORMATION FOR RECIPIENT

RECIPIENT

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

INTERNET FORENSICS

INTERNET DATA

ENTERPRISE SECURITY INTELLIGENCE

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.