



RPOST™

Intelligent Content Security

Where Cybersecurity Meets AI

www.RPost.com



Worldwide Leader, Innovator



Host: DoD / USAF

**Real-World AI Industry Session
with Use-Case / Dev Engagement**

**Location: Pentagon
Collateral Secret Conf Rm 5D855
March 19**

Bottom Line Up Front (BLUF)

With today's evermore complex threat environment, this briefing on, "**Countering Insider Threats, Leaks, and Third-Party Risks with AI Agents**," is timely and maps to current DoD and related department and agency current and next generation published strategies.

Bottom Line Up Front: This RPost technology to be showcased:

1. Complements today's defensive security tech with a strong offense; true AI active threat hunting of sleeper cells embedded in third party systems with agentic AI to un-leak leaks. **The best defense is a strong offense.**
2. Accomplishes not only the Zero Trust Target 2027 capabilities and activities related to Pillars 4, 6, and 7, but also the related **Advanced State 2032 capabilities TODAY.**
3. Meets not only today's Zero Trust goals, but also the Presidential Executive Order related to **DOGE, paragraph 4a**, government tech modernization for maximum efficiency, productivity, inter-operability with data integrity assurance.
4. Implements with **commercial-off-the-shelf software service available on AT&T's GSA schedule**, ready for immediate acquisition, with easy deployment plugged into Microsoft Outlook; proven, the underlying tech has been in use in Federal Government for 20 years.

Bottom Line Up Front (BLUF)

With today's **evermore complex threat environment**, this briefing on **"Countering Insider Threats, Leaks, and Third-Party Risks with AI Agents"** is timely and maps to current DoD and related department and agency current and next generation published strategies.

Bottom Line Up Front (BLUF)

(1) Complements today's defensive security tech with a strong offense; true AI active threat hunting of sleeper cells embedded in third party systems with agentic AI to un-leak leaks. The best defense is a strong offense.

Bottom Line Up Front (BLUF)

(2) Accomplishes not only the Zero Trust Target 2027 capabilities and activities related to Pillars 4, 6, and 7, but also the related **Advanced State 2032 capabilities TODAY.**

Bottom Line Up Front (BLUF)

(3) Meets not only today's Zero Trust goals, but also the Presidential Executive Order related to **DOGE, paragraph 4a, government tech modernization for maximum efficiency, productivity, inter-operability with data integrity assurance.**

Bottom Line Up Front (BLUF)

(4) Implements with **commercial-off-the-shelf software service available on AT&T's GSA schedule**, ready for immediate acquisition, with easy deployment plugged into Microsoft Outlook; proven, the underlying tech has been in use in Federal Government for 20 years.



Countering...

Third-Party Risk & Leaks

Insider Threats & Leaks

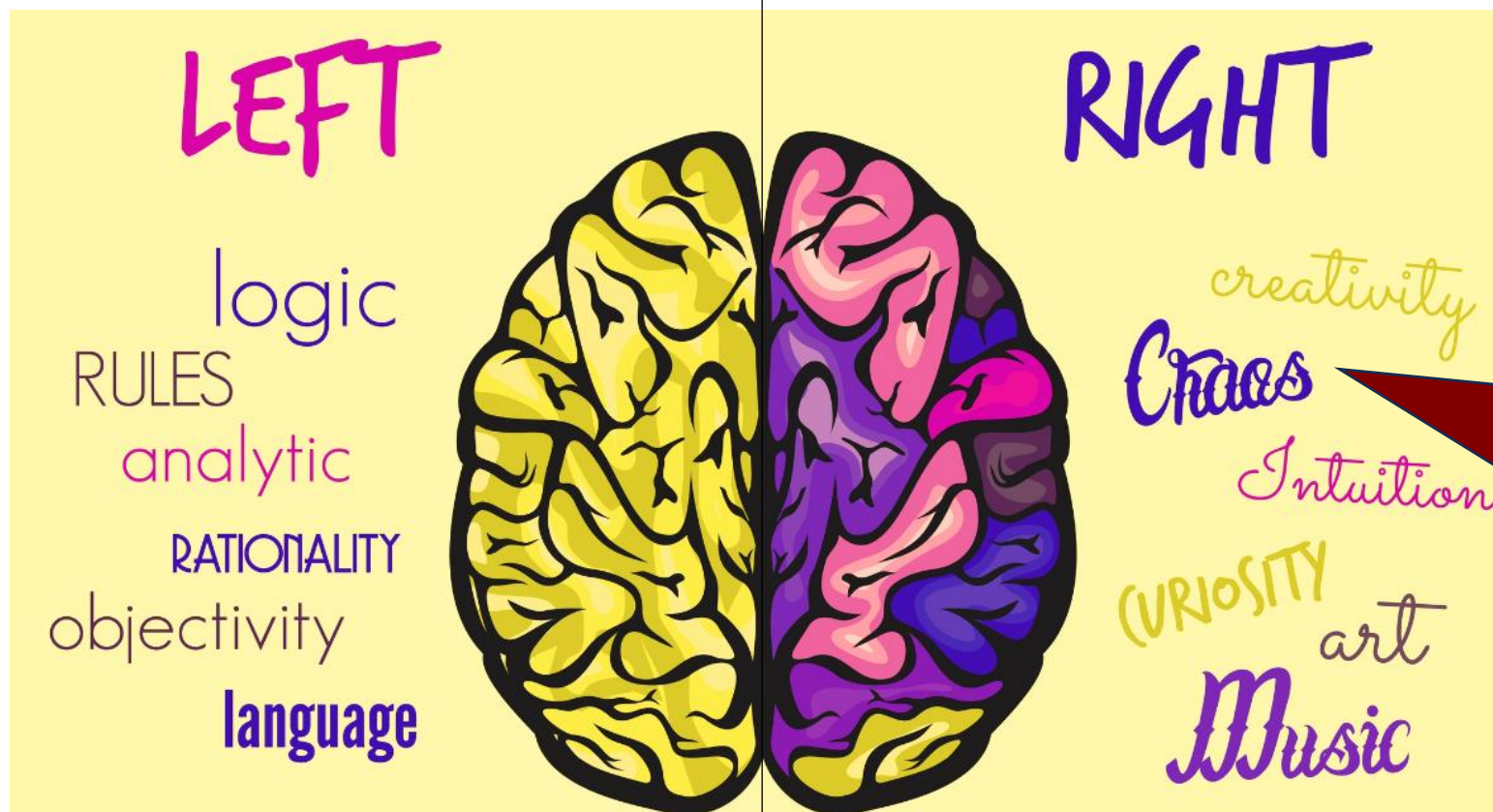
We're Entering a Wave of Cybercriminal Impostor Chaos the World has Never Seen...

...Considering Gen AI can digitally
"clone", create contextual content.

AI from a Left Brain & Right Brain Perspective

Analytical AI

Generative AI



There is **FEAR** in enterprise organizations, 150+ cybercriminal cabals using GenAI to power-up lures

AI from a Left Brain & Right Brain Perspective

Analytical AI

Generative AI

LEFT

logic

RULES

analytic

RATIONALITY

objectivity

language



RIGHT

creativity

Chaos

Intuition

CURIOSITY

art

Music

Counterbalancing analytical AI understood as **REQUIRED** to counterbalance.

There is **FEAR** in enterprise organizations, 150+ cybercriminal cabals using GenAI to power-up lures

It's a Spy
vs. Spy
World.
Power-up
Defense.

AI for the Good Guys








2022

Source: The Forum, Gaming & Leisure, Las Vegas, 21 Feb 2025



**With all the tools we have,
how is it that so many of our
peers have been breached?**

What are we missing?

142 International Cybercriminal Cabals Using Tactical Plan

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire	Drive-by				Process Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Information (3)						OS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Information (6)										Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Information (4)										Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information										Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed-Source Websites										Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open-Source Databases (5)										Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open-Source Websites/Domains										Data from Information Repositories (5)	Hide Infrastructure	Transfer Data to Cloud Account	Firmware Corruption
Search Victim Websites										Data from Local System	Ingress Tool Transfer		Inhibit System Recovery
										Data from Network Shared Drive	Multi-Stage Channels		Network Denial of Service (2)
										Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking (4)
										Data Staged (2)	Non-Standard Port		Service Stop
										Email Collection (3)	Protocol Tunneling		System Shutdown/Reboot

Reconnaissance
10 techniques

Active Scanning (3)

Gather Victim Host Information (4)

See the Unseen, Root of Attack

Source: MITRE ATT&CK®

R RPOST™



Reconnaissance

=

Leaks

@

Your Less Secure Third Parties

...What this means to you...
Context about who is
communicating with whom
about what when in wrong hands



...Context in the wrong hands...

**Boomerangs hyper-contextual
hyper-targeted impersonations**



...Resulting in losses...
**Cybercriminal induced
operational disruption leading
to financial loss or worse.**

[Ransomware, data exfiltration, wire transfer fraud]

They Can Create AI Clones but Need Context to Power-up the Lure

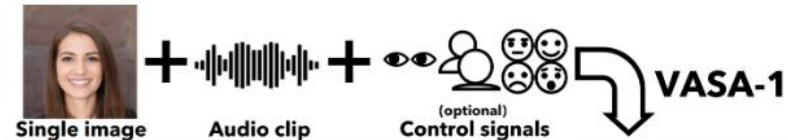
MY VOICE IS NO LONGER MY PASSWORD —

Microsoft's new AI can simulate anyone's voice with 3 seconds of audio

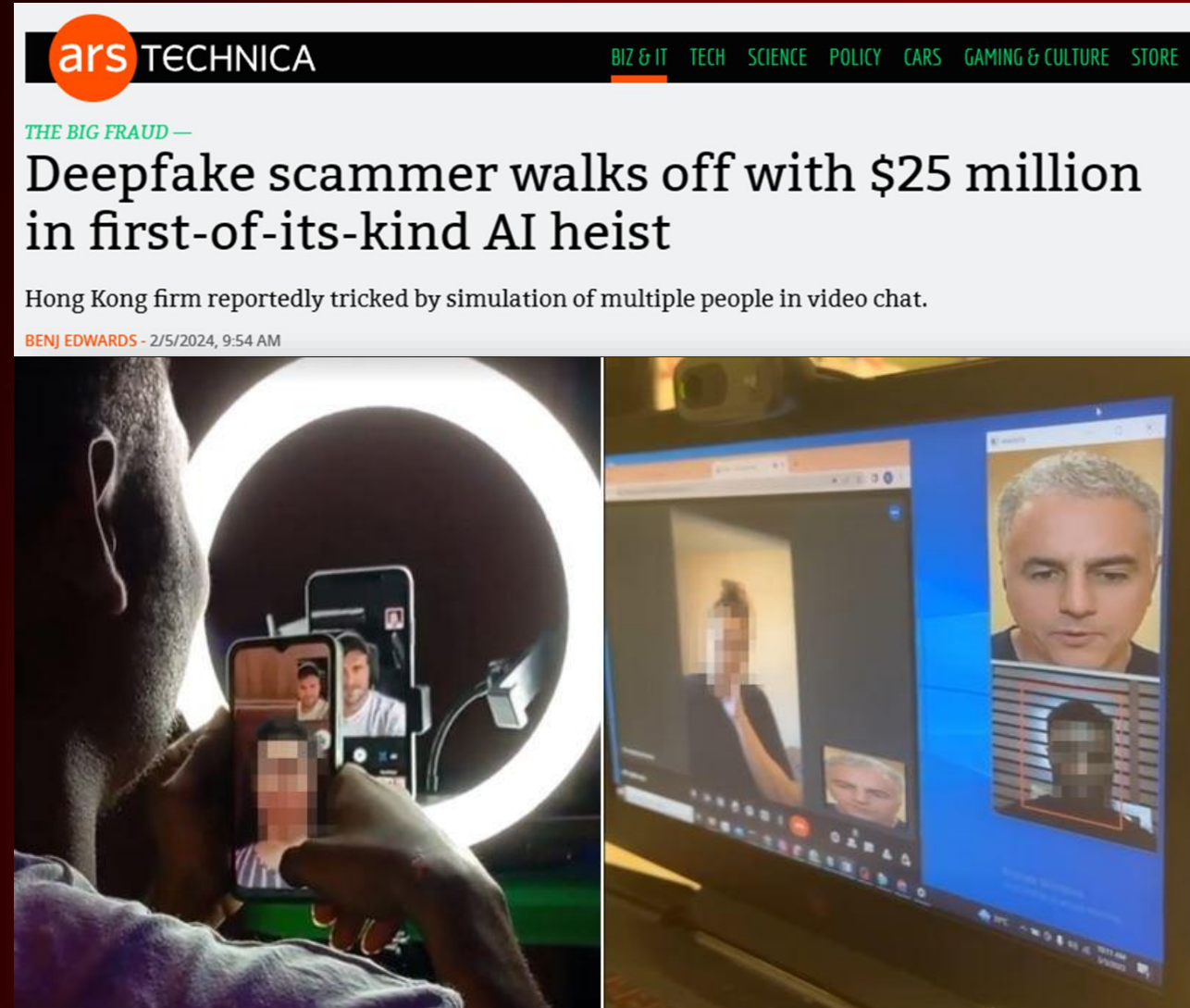
Text-to-speech model can preserve speaker's emotional tone and acoustic environment.

BENJ EDWARDS - 1/9/2023, 4:15 PM

TL;DR: single portrait photo + speech audio = hyper-realistic talking face video with *precise lip-audio sync*, *lifelike facial behavior*, and *naturalistic head movements*, generated in *real time*.



Today... AI Powered-Up



The Age of the AI Clone...

Global cybercrime damage predicted to hit \$10.5 trillion annually by 2025.

Source: Cybersecurity Ventures





Context is King

Third-Party Risk & Leaks

Use Case #1: See the Unseen.
Your Info Leaks at 3rd Parties.



Think... Data Analytics Inside... What about Analytics Outside?

Bottom Line Up Front (BLUF)

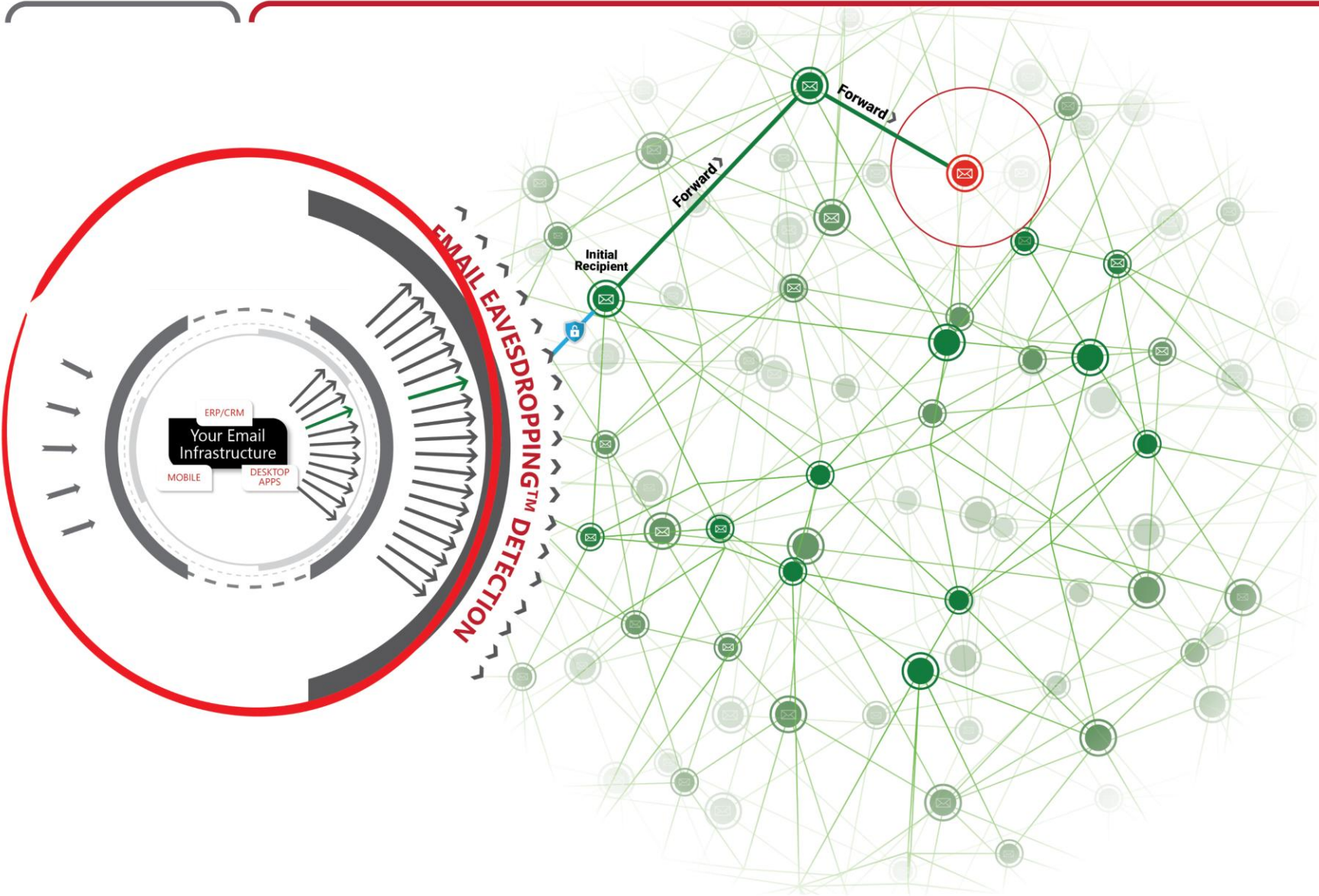
(1) Complements today's defensive security tech with a strong offense; true AI active threat hunting of sleeper cells embedded in third party systems with agentic AI to un-leak leaks. The best defense is a strong offense.

Assume Endpoints Protected

Inbound Email Security

Outbound Email Security

Eavesdropping AI™ Detection Technology

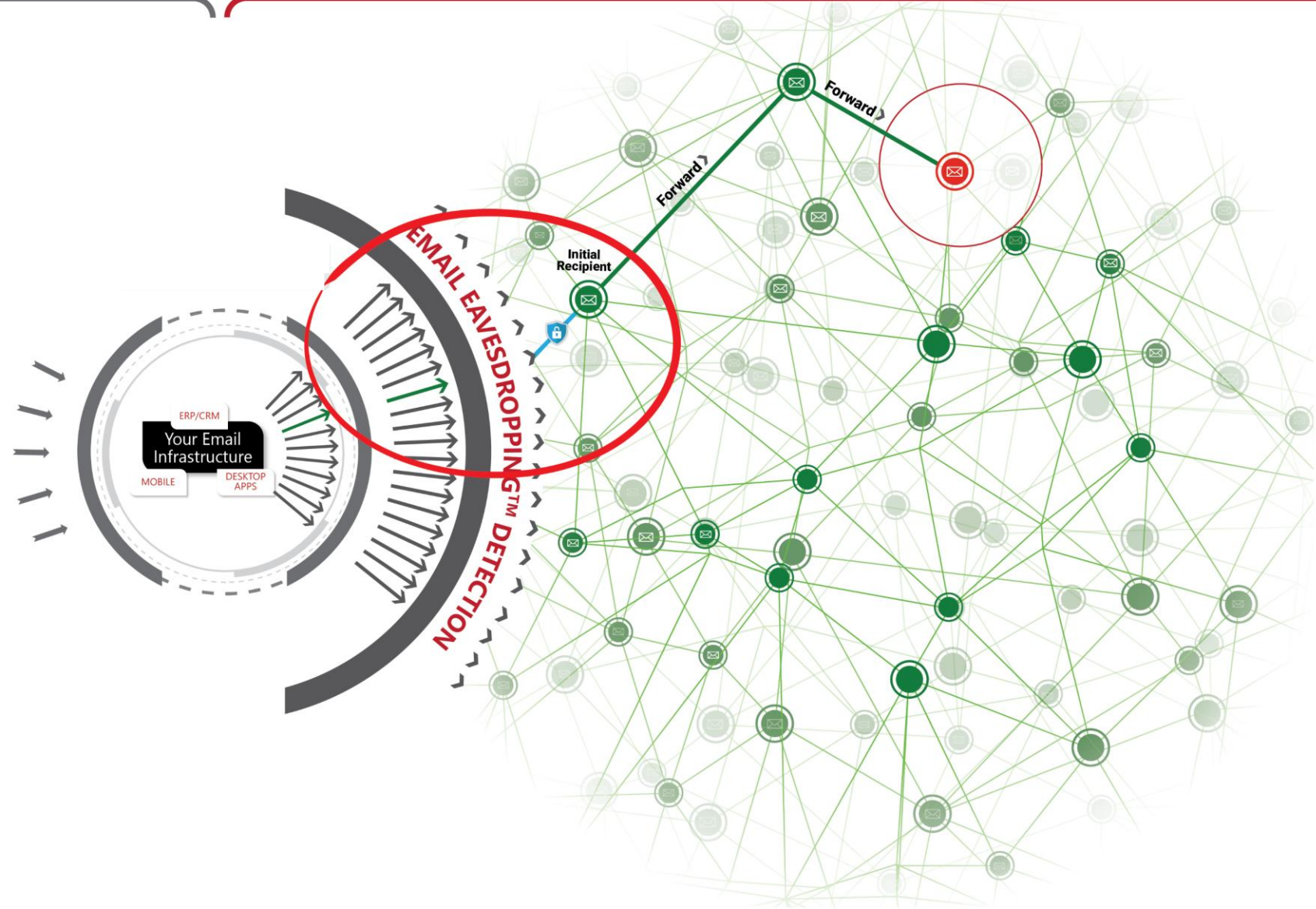


Extended Perimeter Protected, Encrypted

Inbound Email Security

Outbound Email Security

Eavesdropping AI™ Detection Technology

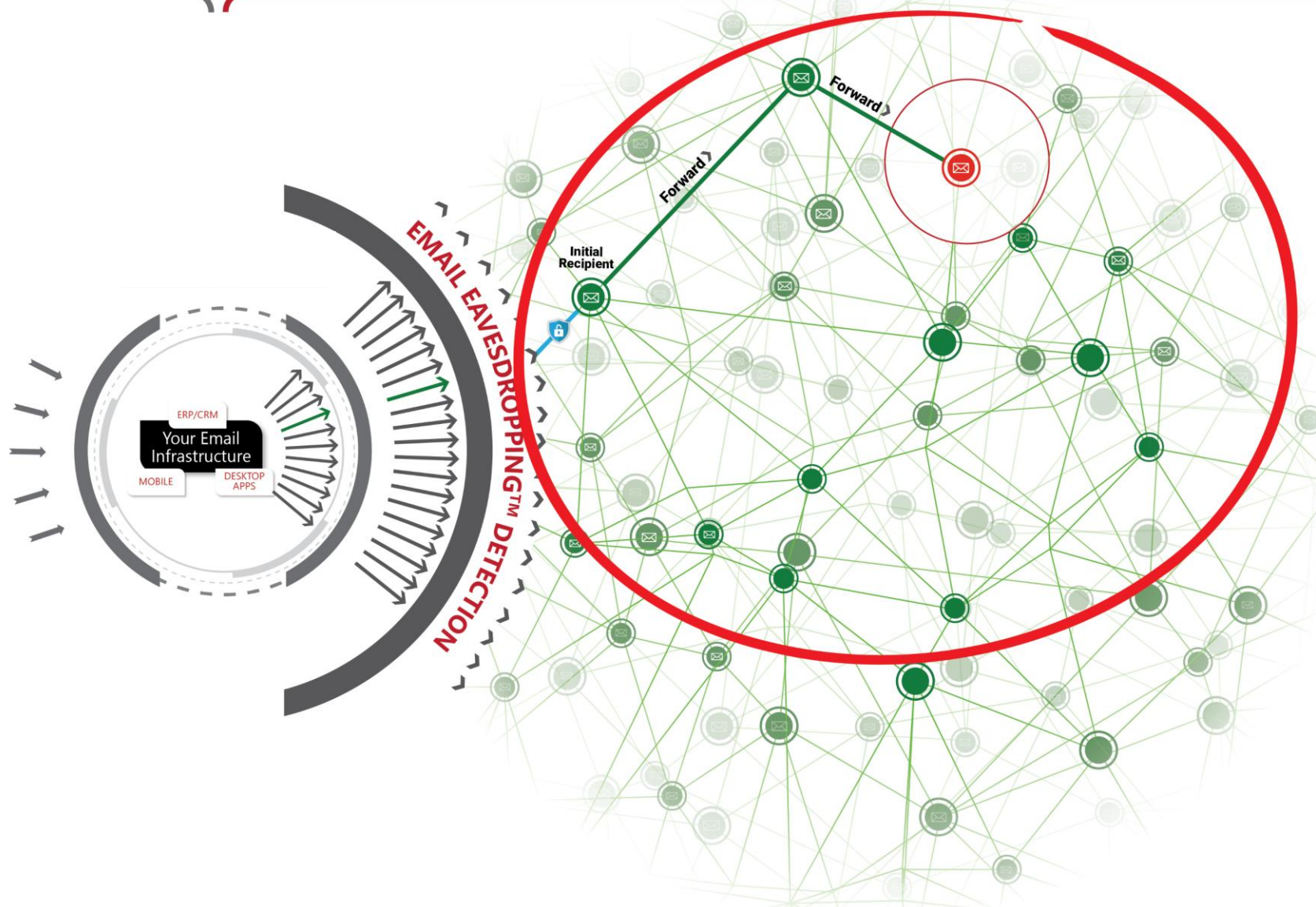


Leaks of YOUR Content at Recipient & Beyond

Inbound Email Security

Outbound Email Security

Eavesdropping AI™ Detection Technology

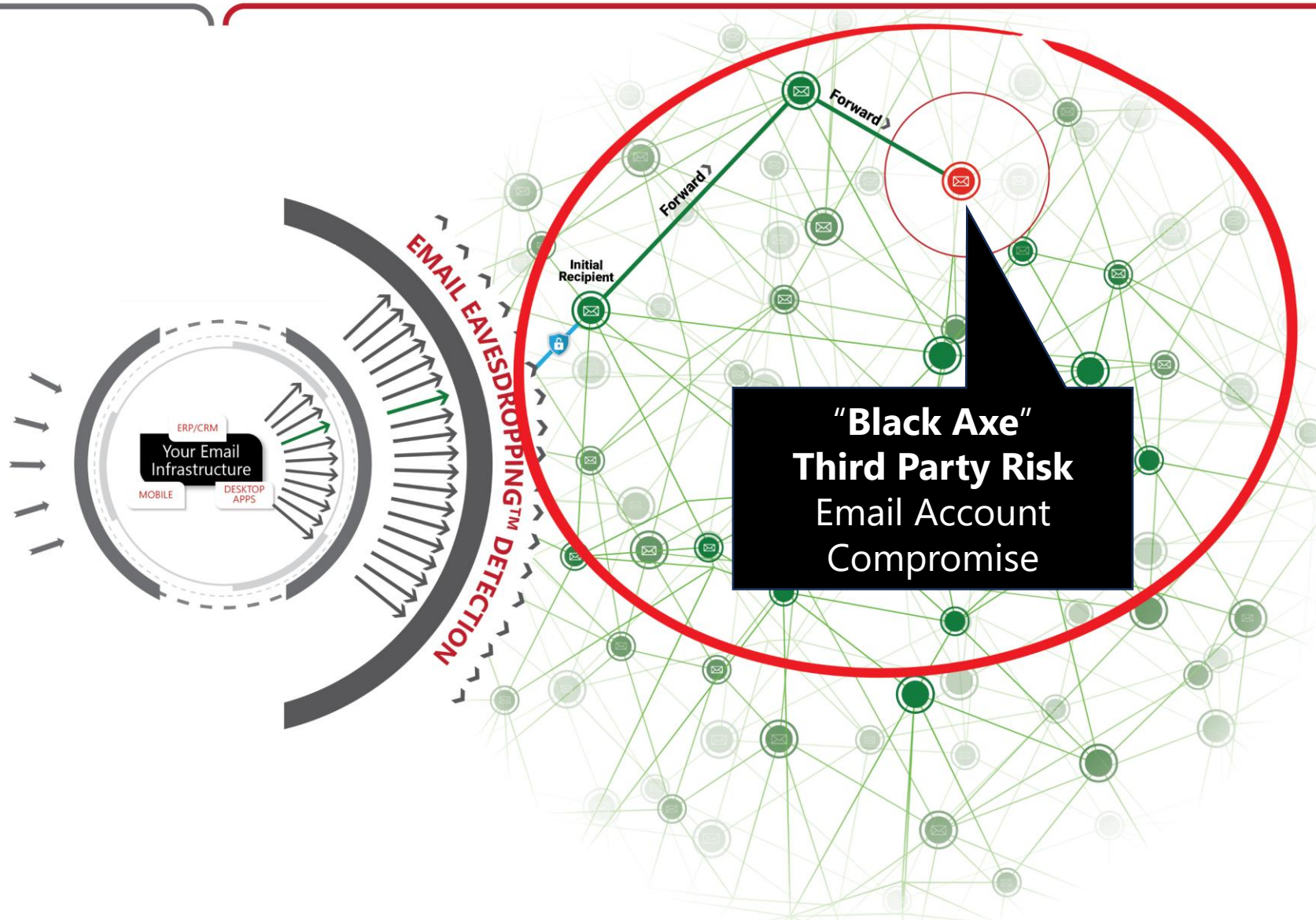


Leaks of YOUR Content at Recipient & Beyond

Inbound Email Security

Outbound Email Security

Eavesdropping AI™ Detection Technology

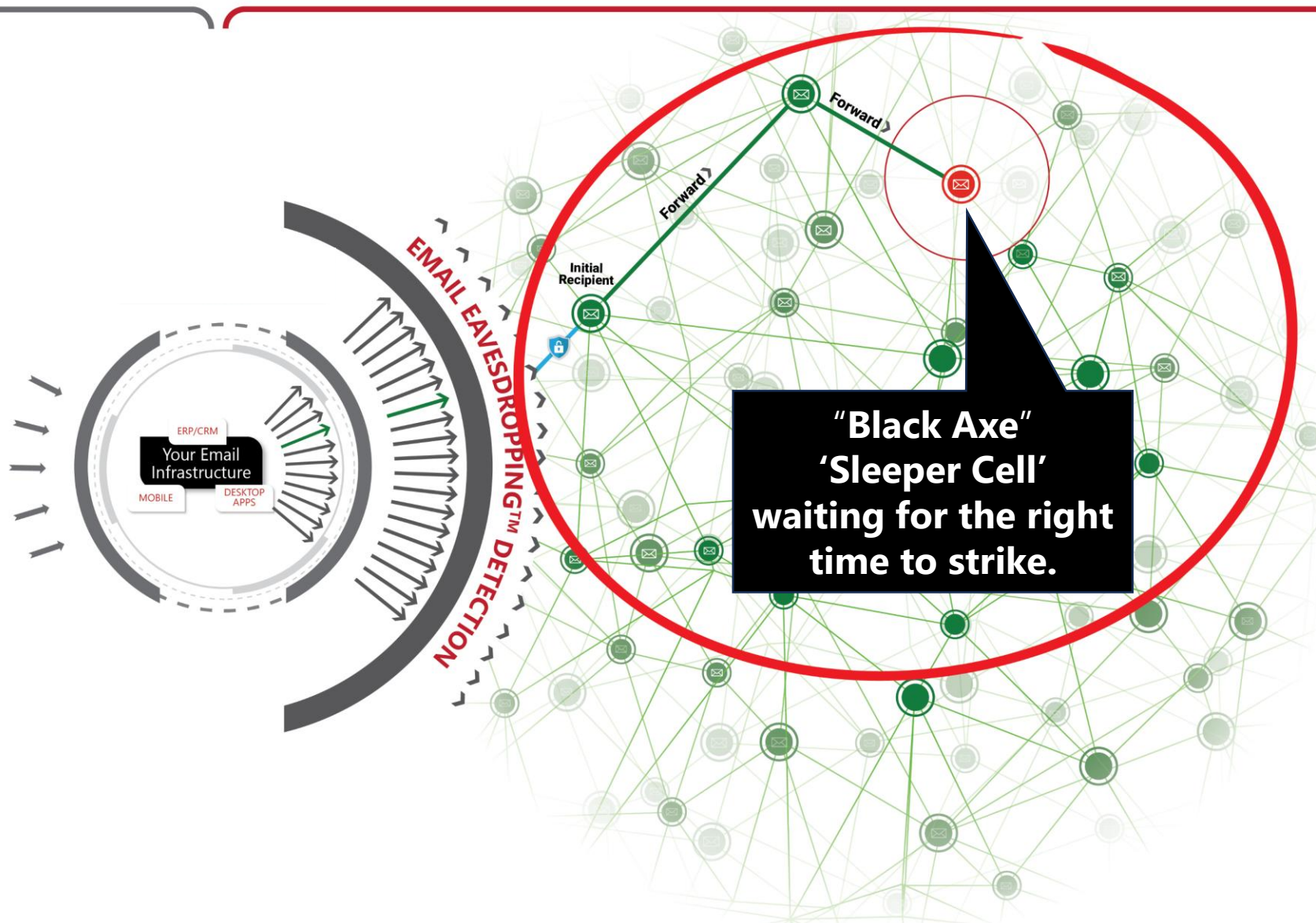


Leaks of YOUR Content at Recipient & Beyond

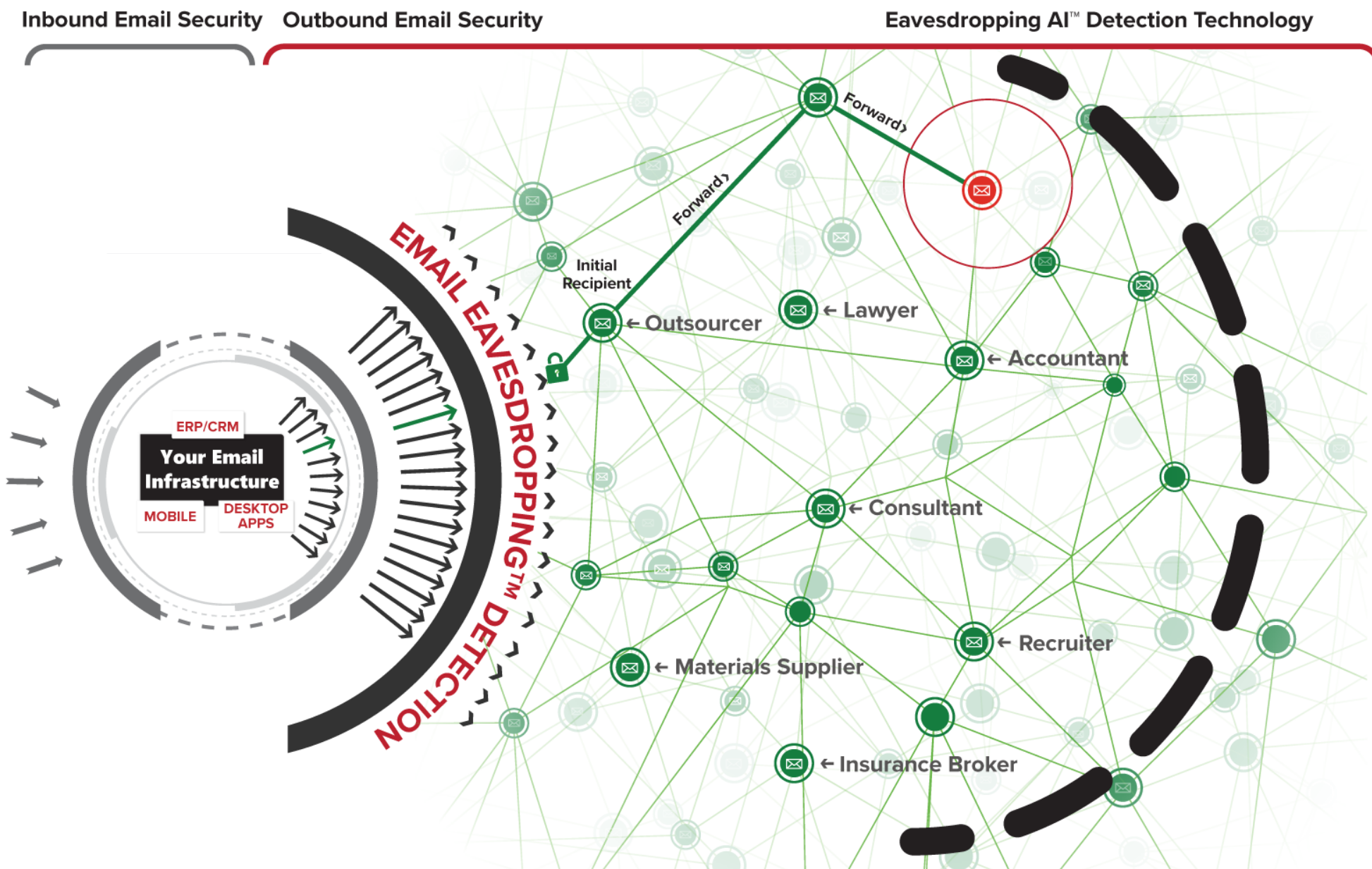
Inbound Email Security

Outbound Email Security

Eavesdropping AI™ Detection Technology

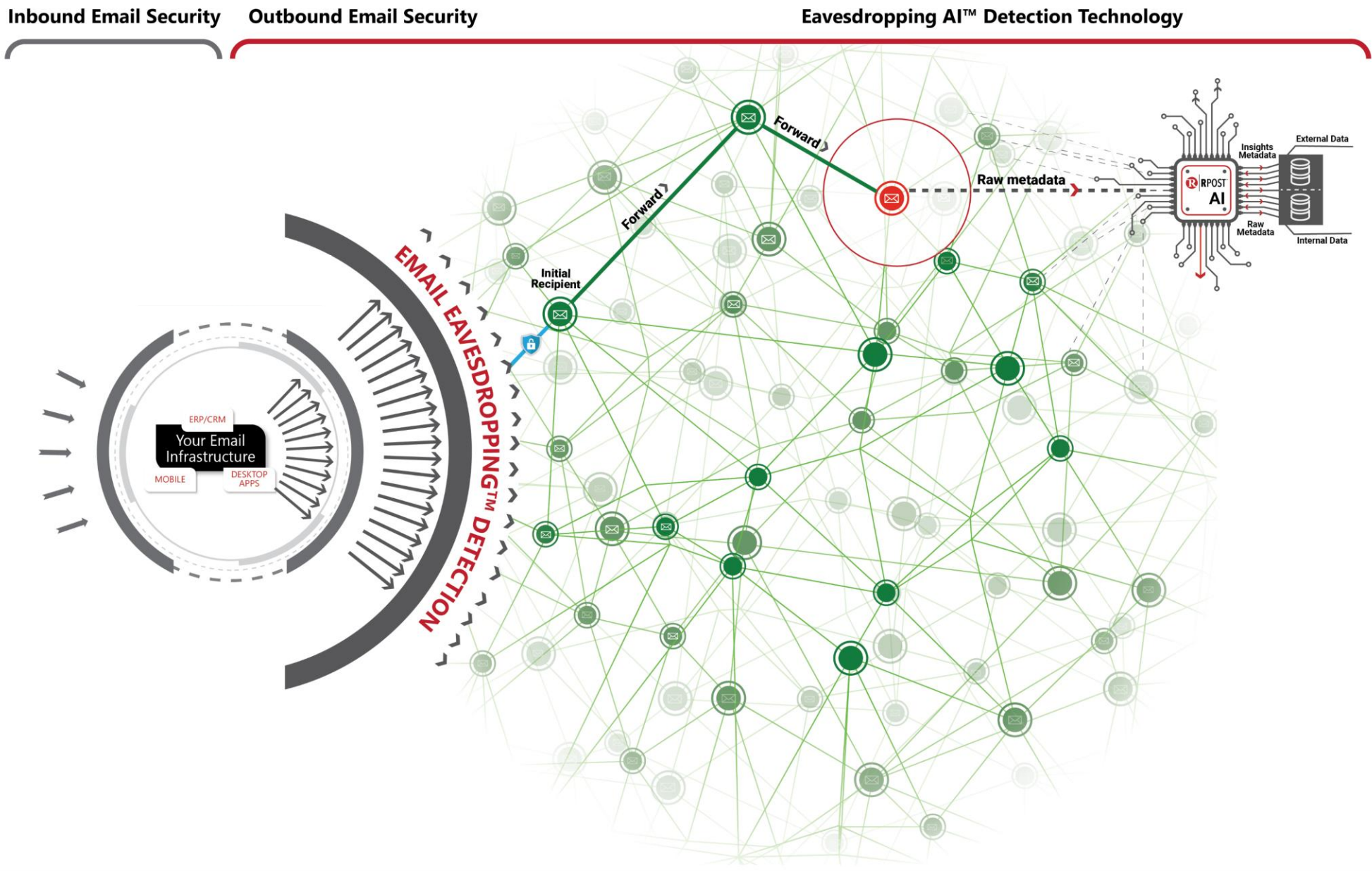


Third- & Fourth-Party Risks

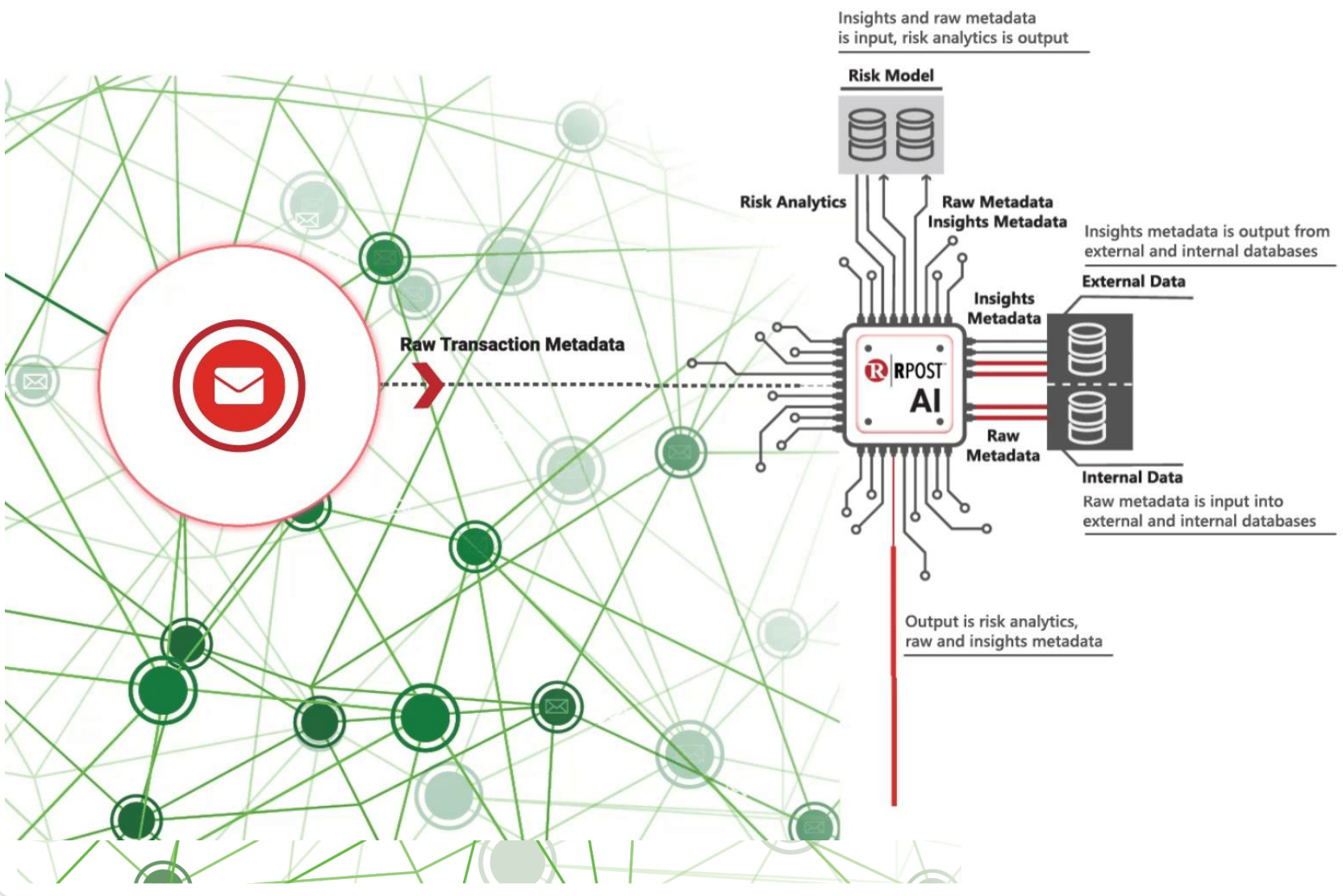


US and non-US patented and patent applications including US18134480, US63632075, US18124419.

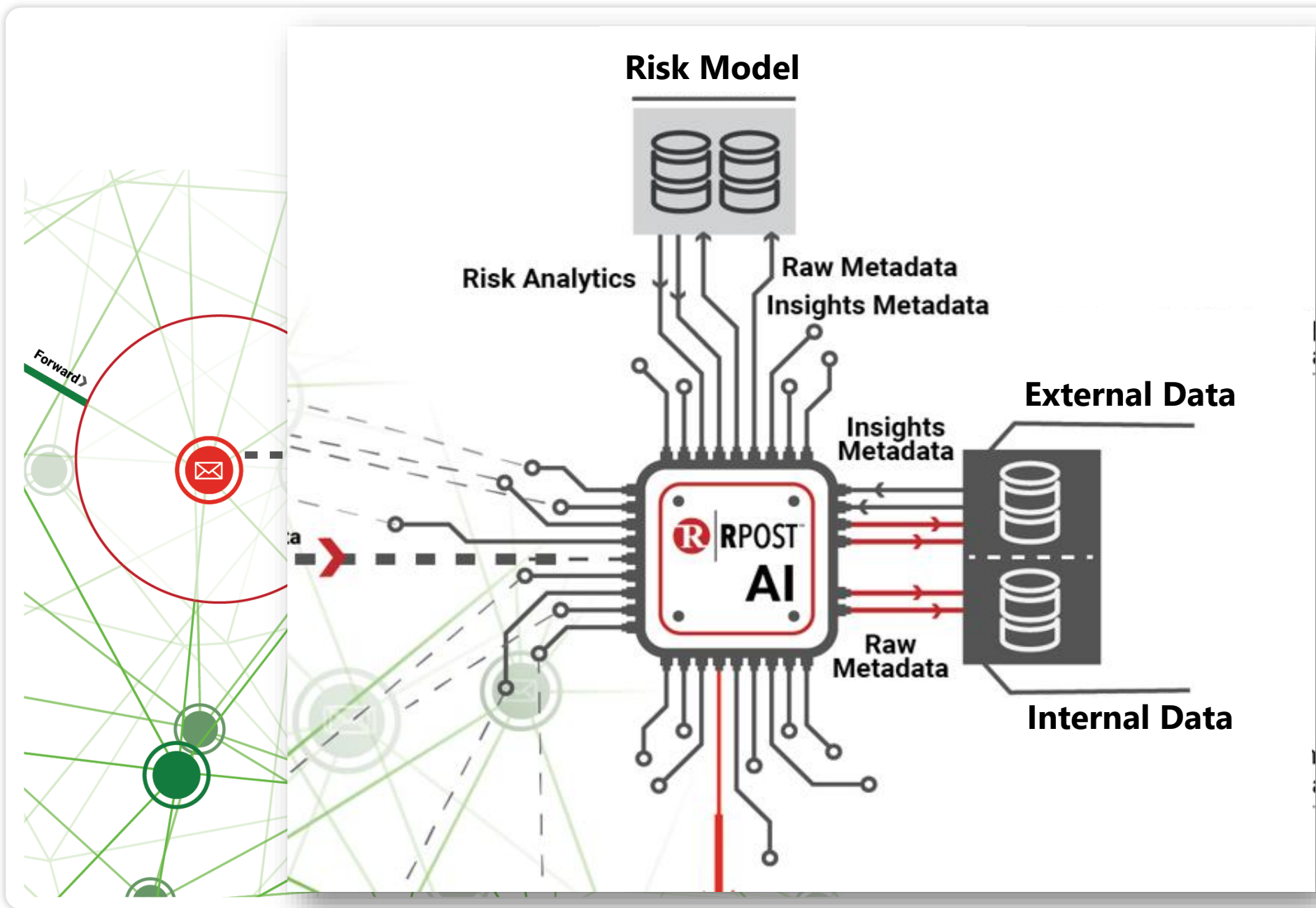
RPost AI is the ONLY Way to See the Unseen



Analytical AI Data Analysis



Analytical AI Data Analysis

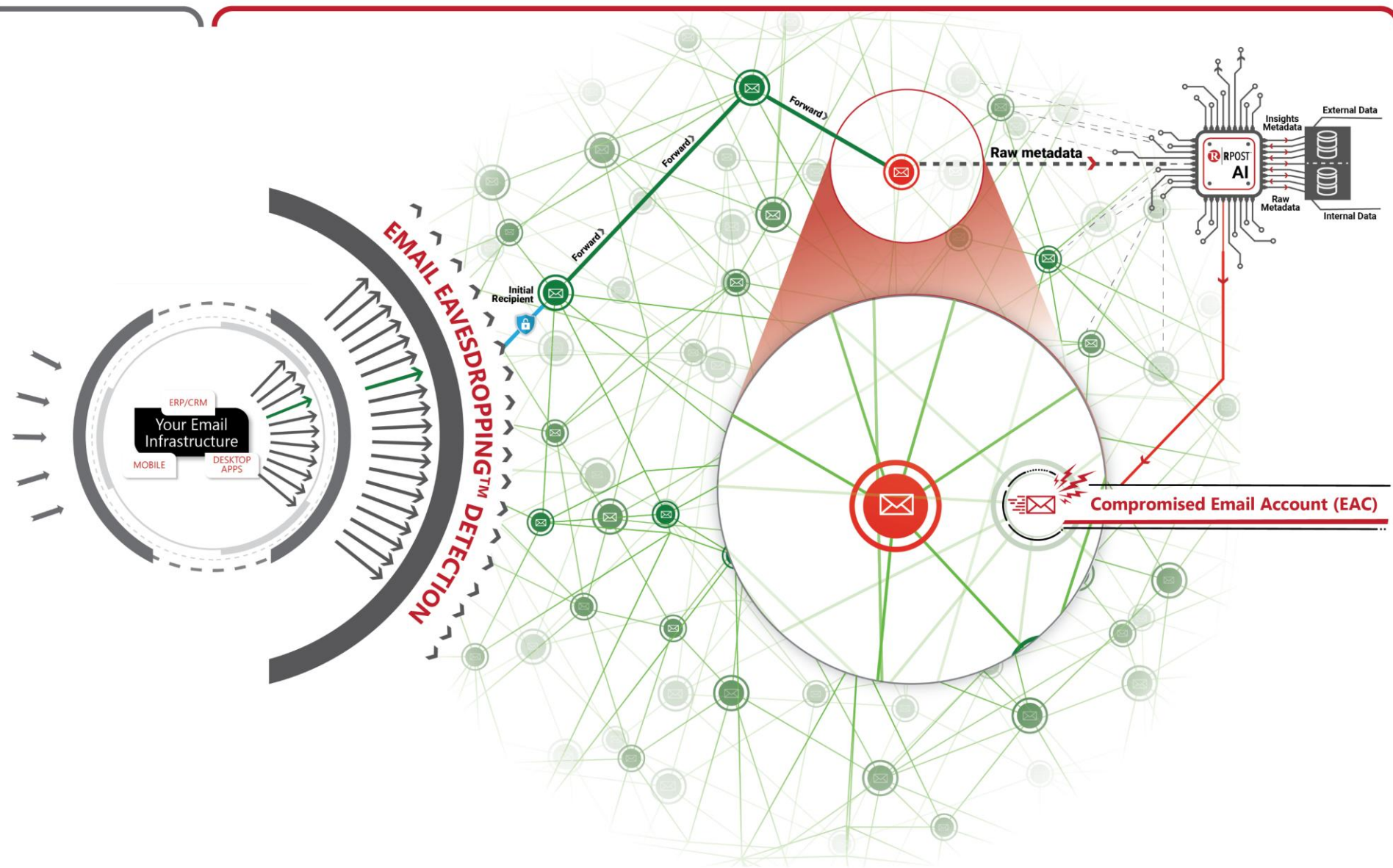


Detect the Thread Leaking Info

Inbound Email Security

Outbound Email Security

Eavesdropping AI™ Detection Technology



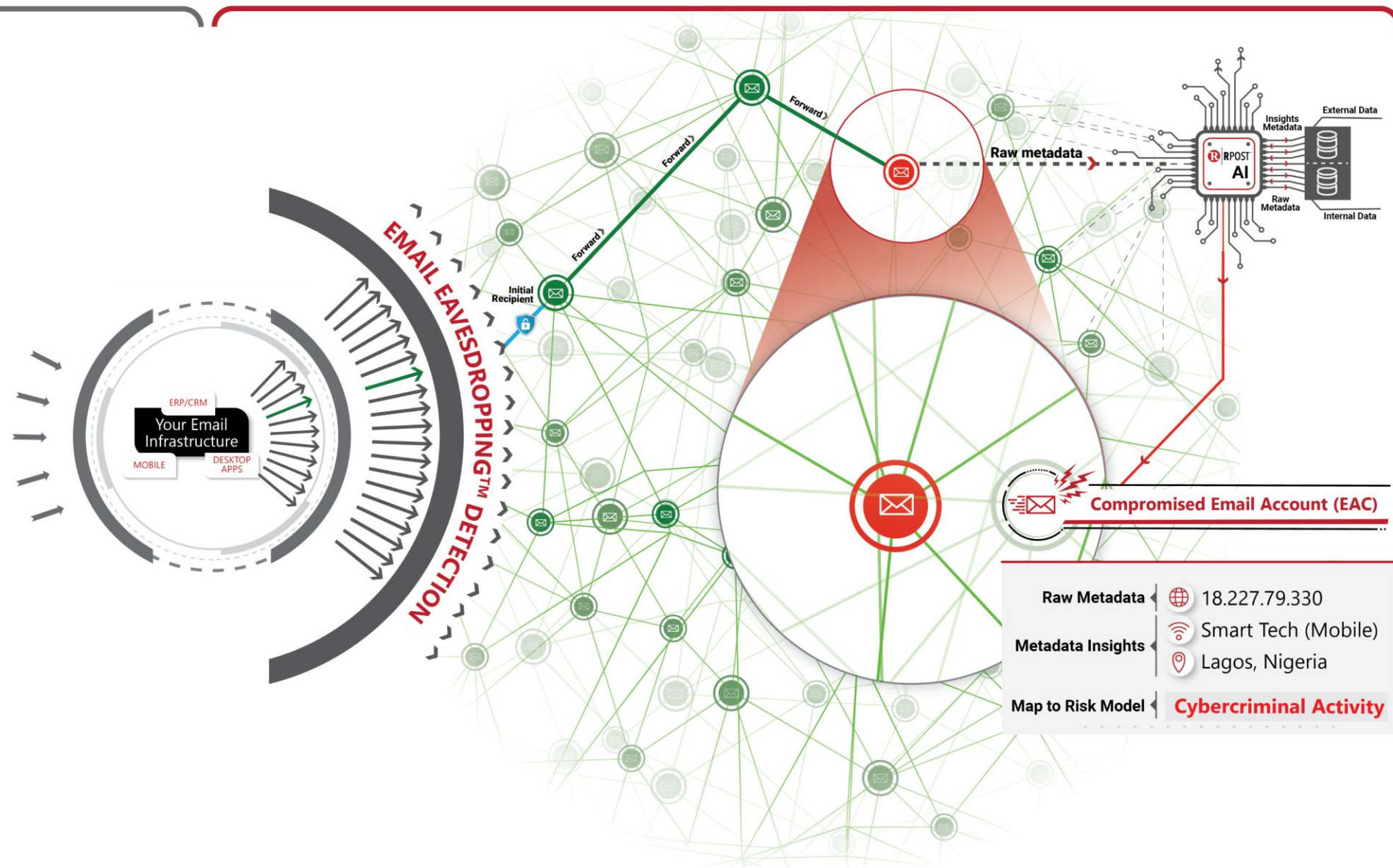
US and non-US patented and patent applications including US18134480, US63632075, US18124419.

Metadata Evidences Leak for Those in Disbelief

Inbound Email Security

Outbound Email Security

Eavesdropping AI™ Detection Technology



See the Unseen Outside Your Network

Black Axe
Est. Benin City
Nigeria



Email Activity Report Email Eavesdropping™ Alert

Sender: [REDACTED]

Recipient: [REDACTED]

Security: Red

Activities: 1

Locations: 1

Last Activity (01/22/2025 07:43:09 UTC)

Email Age: 1 hour 1 minute Pre-empt cybercrime.

Risk Details: All Activities

Time (UTC)
01/22/2025 07:43:09

Original Message
Subject: [REDACTED]
Original Sender: [REDACTED]
Original Send Time: [REDACTED]
Transaction ID: [REDACTED]

Metadata is for [REDACTED]

[IP Address: 98.97.79.43] [Time Opened: 1/22/2025 7:43:09 AM] [REMOTE_HOST: 192.168.10.116] [HTTP_HOST: open.r1.rpost.net] [SCRIPT_NAME: /open/images_v2/EndErwBjq3AQFqlhOnSHjTPv6NJs2uWvQchvBugNMTlw.png] HTTP_ACCEPT:image/webp,image/png,image/svg+xml,image/*;q=0.8;video/*;q=0.5 HTTP_ACCEPT_ENCODING:gzip, deflate, br HTTP_ACCEPT_LANGUAGE:en-GB,en;q=0.9

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

Time (UTC)	Activity	Location	Country	Network Addr.	Network	Risk
01/22/2025 07:43:09	Open (M)	Lagos, LA	Nigeria	98-97-79-43	Spacex-Starl	Red

Impersonation: See the Unseen


Sender: [REDACTED]

Recipient: [REDACTED]@outlook.com

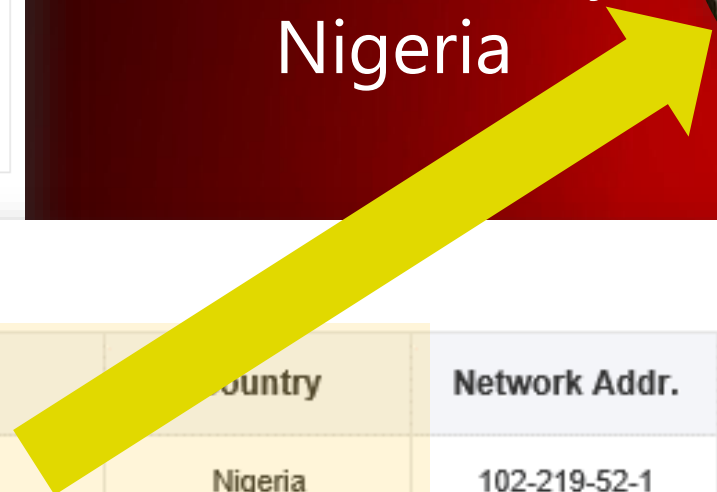
Security: Red

Activities: 2

Locations: 2



Black Axe
Est. Benin City
Nigeria



Email Age: 1 minute

Risk Details: All Activities

Time (UTC)
08/30/2023 16:59:01
08/30/2023 16:58:45

Risk Details: All Activities

Time (UTC)	Activity	Location	Country	Network Addr.	Network	Risk
08/30/2023 16:59:01	Open (M)	Benin City, ED	Nigeria	102-219-52-1	Tizeti-As	Red
08/30/2023 16:58:45	Open (M)	Cape Town, WC	South Africa	196-22-243-3	Cybersmart	Red

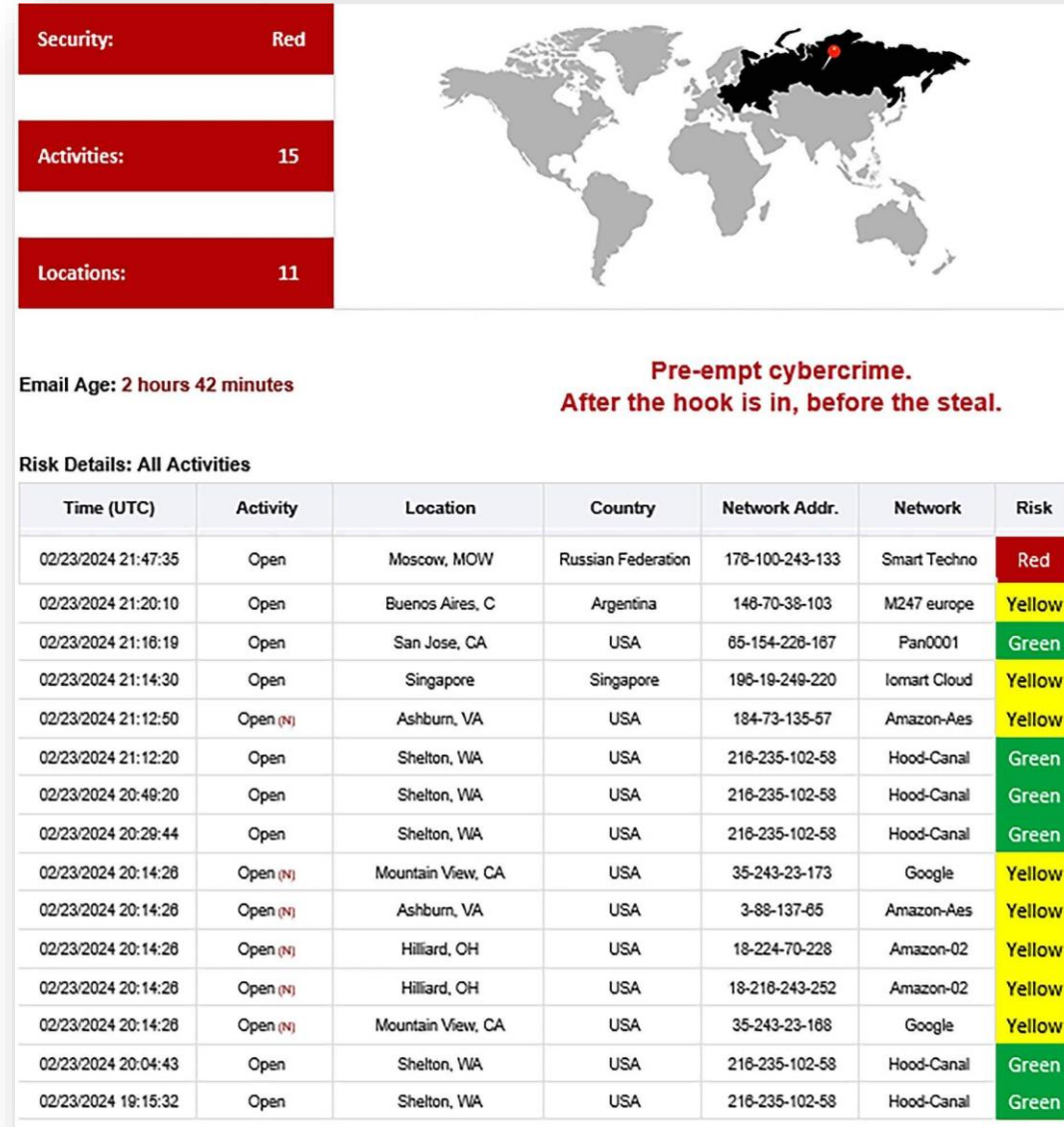
Original Message De

Subject: [REDACTED]

Original Sender: [REDACTED]

Original Send Time: 08/30/2023 16:58:22 UTC

See the Unseen: See Criminals in Action



"Seeing emails opened in Russia was an immediate red flag..."

-- AEGIS Land Title Group

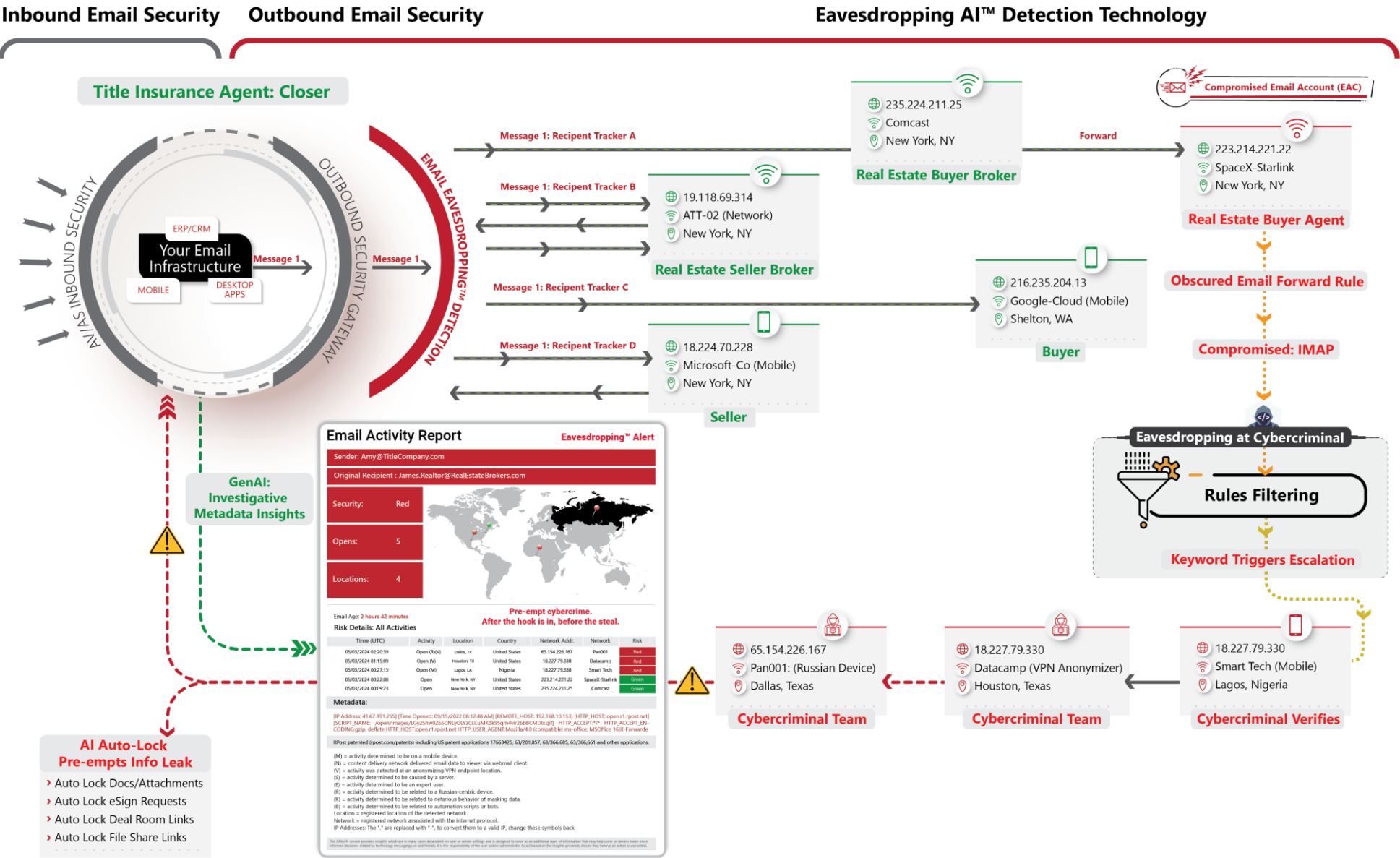
Location	Country	Network Addr.	Network	Risk
Moscow, MOW	Russian Federation	176-100-243-133	Smart Techno	Red
Buenos Aires, C	Argentina	146-70-38-103	M247 europe	Yellow

Within 3 hours of the first send, activity in Russia detected.

Fin7 Russian cybercriminals operating in Texas.

Original Send Time: 08/30/2023 16:58:22 UTC

See the Unseen, Red Alert



A Leak Locked is Not a Breach, if Not Seen

Email Activity Report

Eavesdropping™ Alert

Sender: Amy@TitleCompany.com

Original Recipient : James.Realtor@RealEstateBrokers.com

Security: Red

Opens: 5

Locations: 4



Email Age: 2 hours 42 minutes

Risk Details: All Activities

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

Time (UTC)	Activity	Location	Country	Network Addr.	Network	Risk
05/03/2024 02:20:39	Open (R)(V)	Dallas, TX	United States	65.154.226.167	Pan001	Red
05/03/2024 01:15:09	Open (V)	Houston, TX	United States	18.227.79.330	Datacamp	Red
05/03/2024 00:27:15	Open (M)	Lagos, LA	Nigeria	18.227.79.330	Smart Tech	Red
05/03/2024 00:22:08	Open	New York, NY	United States	223.214.221.22	SpaceX-Starlink	Green
05/03/2024 00:09:23	Open	New York, NY	United States	235.224.211.25	Comcast	Green

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)X-Forwarded-For: 192.168.10.153

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

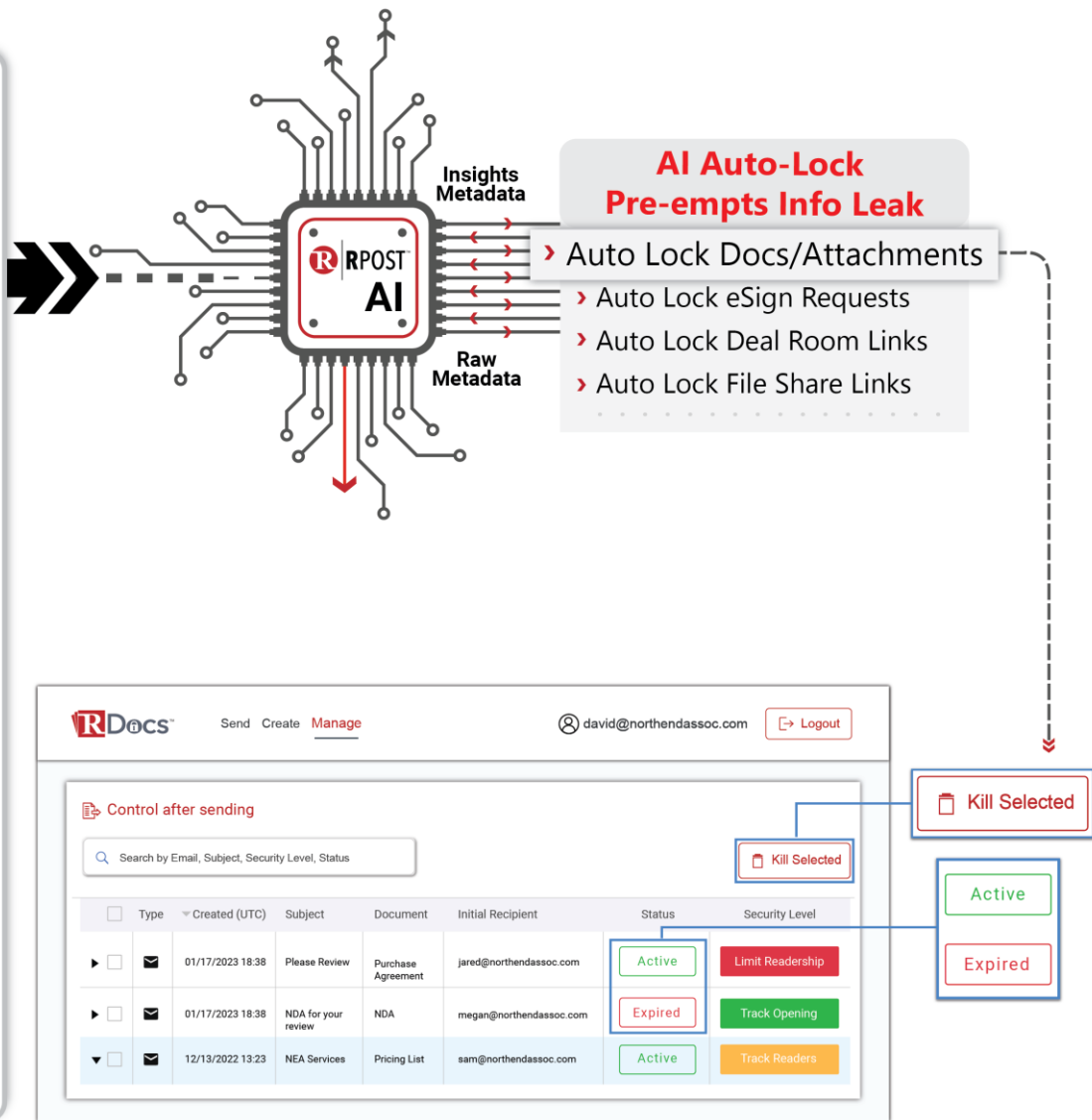
(M) = activity determined to be on a mobile device.
(N) = content delivery network delivered email data to viewer via webmail client.
(V) = activity was detected at an anonymizing VPN endpoint location.
(S) = activity determined to be caused by a server.
(E) = activity determined to be an expert user.
(R) = activity determined to be related to a Russian-centric device.
(K) = activity determined to be related to nefarious behavior of masking data.
(B) = activity determined to be related to automation scripts or bots.

Location = registered location of the detected network.

Network = registered network associated with the internet protocol.

IP Addresses: The "." are replaced with "-", to convert them to a valid IP, change these symbols back.

This RMail® service provides insights which are in many cases dependent on user or admin settings and is designed to serve as an additional layer of information that may help users or admins make more informed decisions related to technology messaging use and threats. It is the responsibility of the user and/or administrator to act based on the insights provided, should they believe an action is warranted.



RDocs™ Send Create Manage david@northendassoc.com Logout

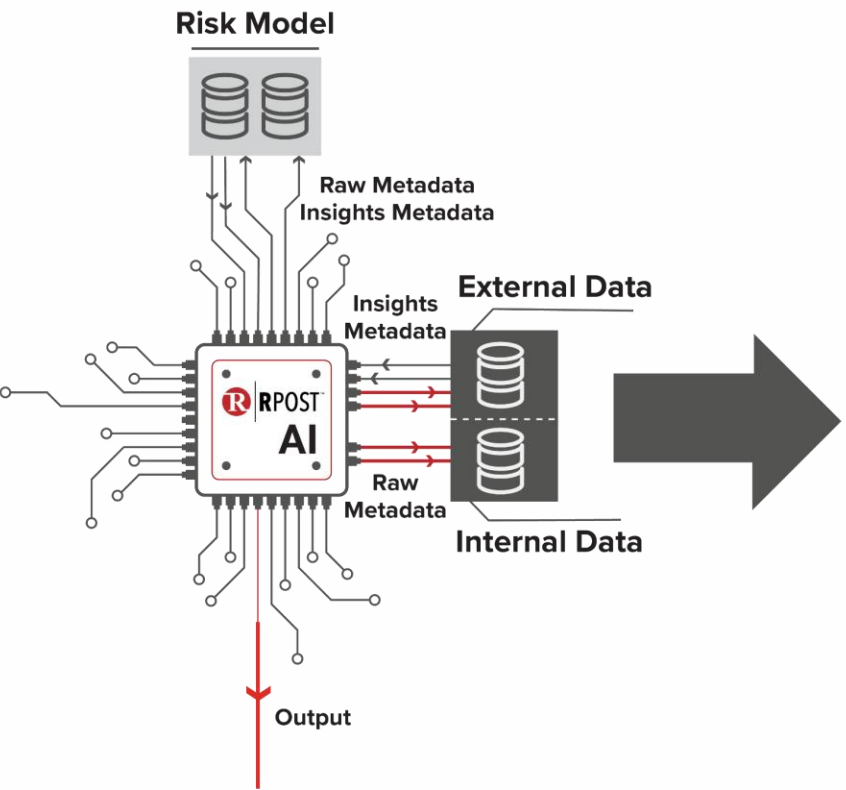
Control after sending

Search by Email, Subject, Security Level, Status

Type	Created (UTC)	Subject	Document	Initial Recipient	Status	Security Level
▶	01/17/2023 18:38	Please Review	Purchase Agreement	jared@northendassoc.com	Active	Limit Readership
▶	01/17/2023 18:38	NDA for your review	NDA	megan@northendassoc.com	Expired	Track Opening
▼	12/13/2022 13:23	NEA Services	Pricing List	sam@northendassoc.com	Active	Track Readers



RPost AI Model



RPost AI Assistant

The RPost AI Assistant interface displays two main reports:

Email Activity Report

Eavesdropping™ Alert

Sender: Amy@TitleCompany.com
Original Recipient: James.Realtor@RealEstateBrokers.com

Security: Red
Opens: 5
Locations: 4

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

Risk Details: All Activities

Time (UTC)	Activity	Location	Country	Network Addr	Network	Risk
05/03/2024 02:20:39	Open (RVV)	Italy, TX	United States	65.154.226.167	Pan001	Red
05/03/2024 01:15:09	Open (V)	Houston, TX	United States	169.150.203.251	Datacamp	Red
05/03/2024 00:27:15	Open (M)	Lagos, LA	Nigeria	129.205.124.224	Globacom-AS	Red
05/03/2024 00:22:08	Open	New York, NY	United States	223.214.221.22	SpaceX Starlink	Green
05/03/2024 00:09:23	Open	New York, NY	United States	235.224.211.25	Comcast	Green

Metadata:

[IP Address: 41.67.191.255] [Time Opened: 09/15/2023 08:12:48 AM] [REMOTE_HOST: 192.168.10.153] [HTTP_HOST: open.rpost.net] [SCRIPT_NAME: /open/images/025hw0265CNyOIVYcLCuMk0k95gm4vir26b8CMDkxg0] [HTTP_ACCEPT: */*] [HTTP_ACCEPT_ENCODING: gzip, deflate] [HTTP_HOST: open.rpost.net] [HTTP_USER_AGENT: Mozilla/4.0 (compatible; ms office; MSOffice 16.0) Forwarded]

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

(M) = activity det (N) = content det (V) = activity was (S) = activity det (E) = activity det (R) = activity det (K) = activity det (B) = activity det Location = regist Network = regist IP Addresses: The

Counter-Insider Threat & Leaks Hub

Threat Intelligence Overview RPost AI Forensics Risk Model Fine Tuning

Total Emails Sent with RPost AI Intelligence: 230 (+20% vs Previous period)

Percentage Emails Sent Encrypted: 9.86% (+37.9% vs Previous period)

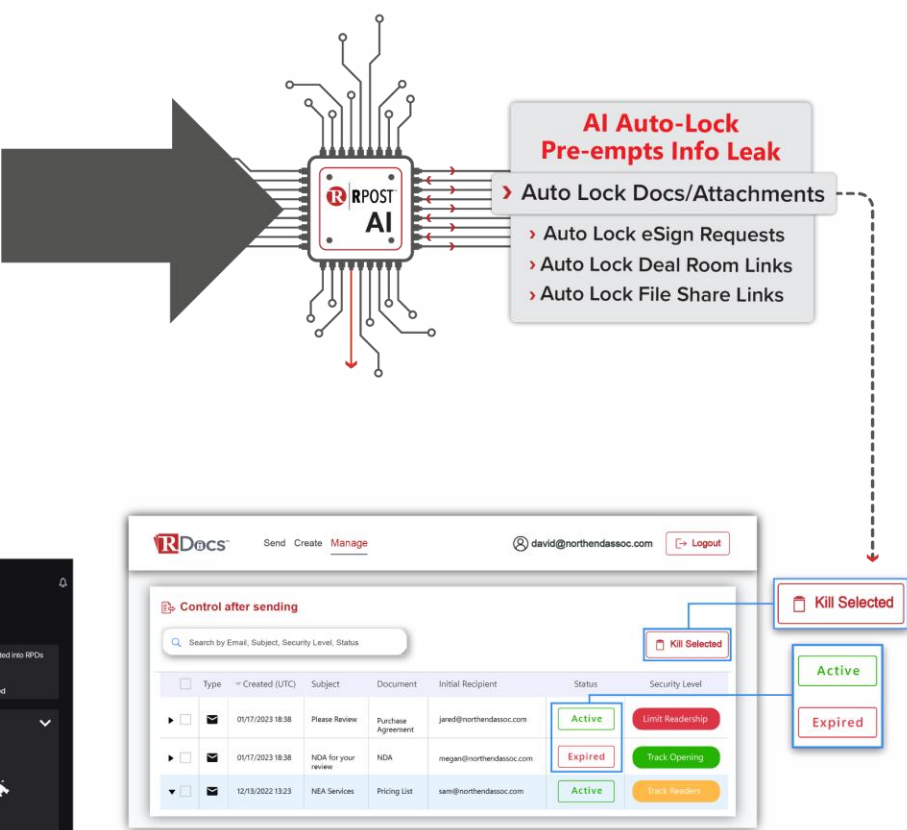
Percentage Documents Converted into RPDs: 6.9% (+33% vs Previous period)

Threat Intelligence Heatmap

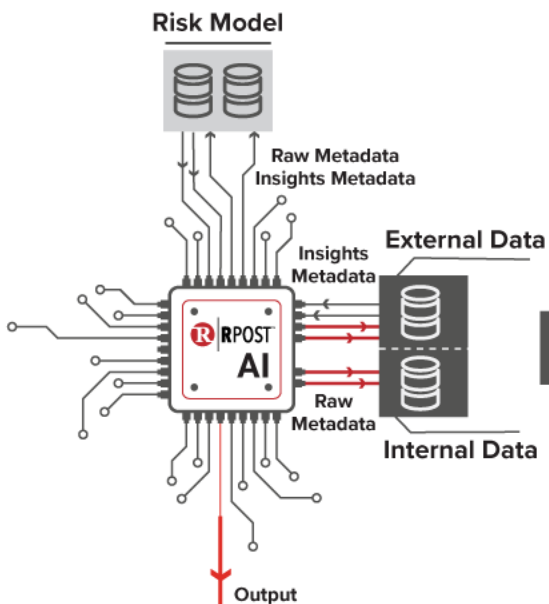
Recipient Watchlist

- David@myvendor.com
- Susan@othervendor.net
- margit@vendor3.uk

RPost AI Agent

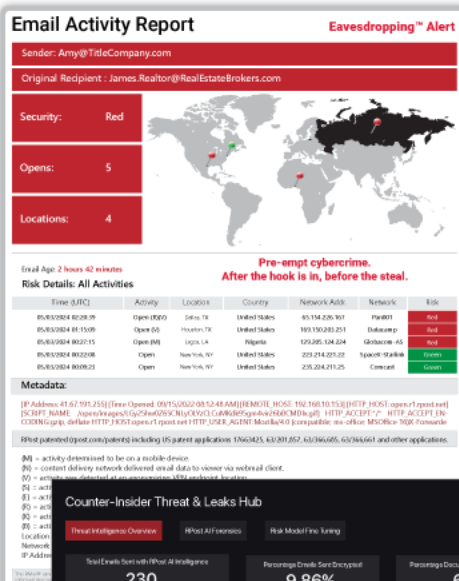


RPost AI Model

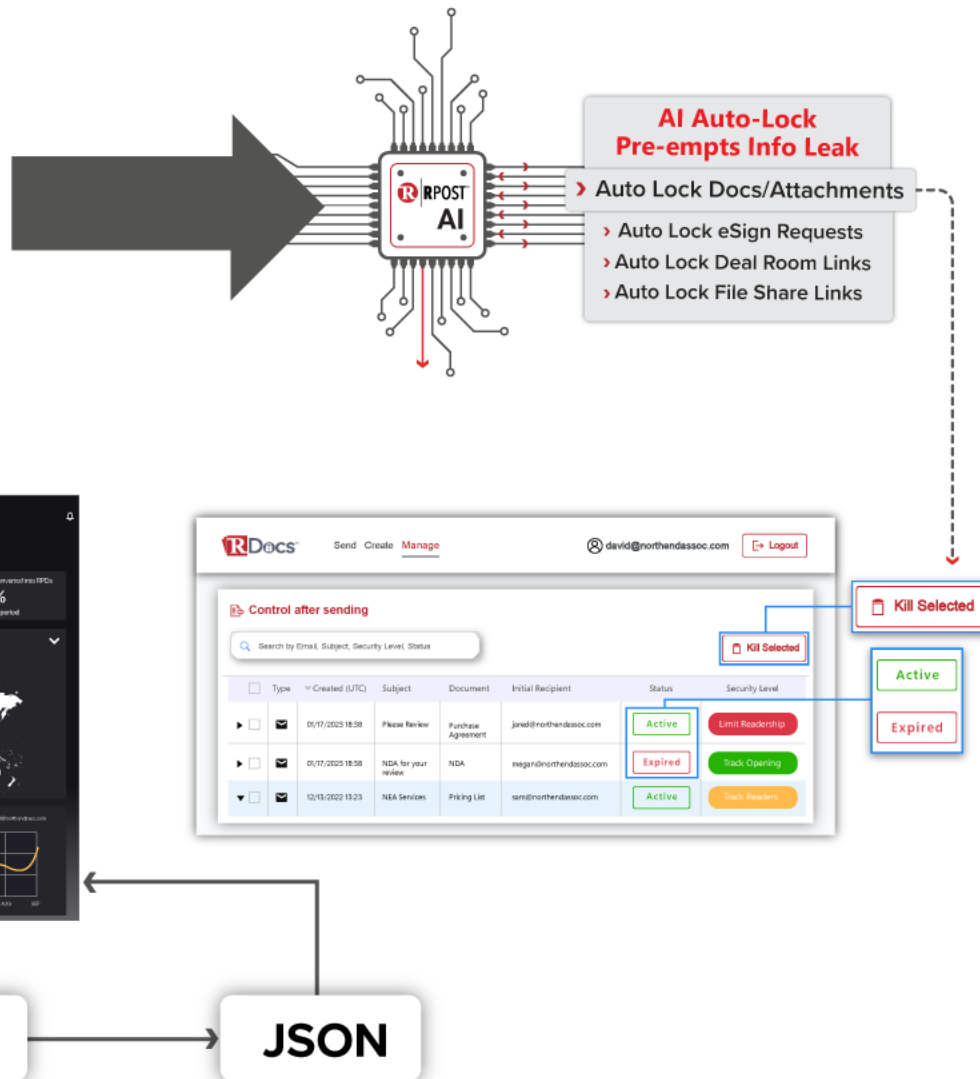


Raw

RPost AI Assistant



RPost AI Agent



Databy VPN
GEO
Leak

RAI

Risk

Email Activity Report

Eavesdropping™ Alert

Sender: Amy@TitleCompany.com

Original Recipient : James.Realtor@RealEstateBrokers.com

Security: Red

Opens: 5

Locations: 4



Email Age: 2 hours 42 minutes

Risk Details: All Activities

Time (UTC)	Activity	Location	Country	Network-Addr	Network	Risk
05/03/2024 02:20:59	Open (RD)	Indian, IN	United States	63.154.226.167	FastNet	Red
05/03/2024 01:15:09	Open (R)	Houston, TX	United States	168.156.205.251	Datacamp	Red
05/03/2024 00:27:15	Open (M)	Lagos, LA	Nigeria	129.205.124.204	Globacom-AS	Red
05/03/2024 00:22:08	Open	New York, NY	United States	212.214.221.22	Speed-Startlink	Green
05/03/2024 00:09:23	Open	New York, NY	United States	212.224.211.25	Comcast	Green

Metadata:

[IP Address: 41.67.191.251] [Time Opened: 09/15/2022 08:12:48 AM] [REMOTE_HOST: 192.168.10.151] [HTTP_HOST: openr1.postnet] [SCRIPT_NAME: /openr1/postnet] [GATEWAY_INTERFACE: CGI/1.1] [CONTENT_LENGTH: 0] [CONTENT_TYPE: text/html] [HTTP_ACCEPT: */*] [HTTP_ACCEPT_ENCODING: gzip, deflate] [HTTP_HOST: openr1.postnet] [HTTP_USER_AGENT: Mozilla/4.0 (compatible; ms office MSOffice 16)X-Forwarded-For: 192.168.10.151]

RPost patented [postnet.com/patent] including US patent applications 17903425, 63/201,057, 63/200,005, 63/200,001 and other applications.

[M] = activity determined to be on a mobile device.
[N] = content delivery network delivered email data to viewer via webmail client.
[O] = activity was detected at an anonymizing VPN endpoint location.
[S] = activity determined to be caused by a server.
[U] = activity determined to be an expert user.
[R] = activity determined to be related to a Russian-centric device.
[Q] = activity determined to be related to nefarious behavior of masking data.
[G] = activity determined to be related to automation scripts or bots.
Location = registered location of the detected network.
Network = registered network associated with the internet protocol.
IP Addresses: The "-" are replaced with "." to convert them to a valid IP; change these symbols back.

The RPost system provides insight which is only as good as the data it is based on. It is not a perfect system. It is a tool to help you understand your data better. It is not a substitute for your own analysis. It is a tool to help you understand your data better. It is not a substitute for your own analysis.

AI Auto Lock

AI Security Analysis

Identified High-Risk Anomaly:

- Sender: [REDACTED]
- Recipient: [REDACTED]
- Risk Type: High (Red category)
- Location: Dallas, Texas, USA
- Activity Pattern: Multiple messages sent within seconds/minutes.
- Timestamps: Several emails were sent at identical timestamps or within a few seconds of each other.

Why It's Concerning:

- The sender exhibits **burst activity**, rapidly sending multiple emails to the same recipient.
- This could indicate a **compromised account** being used to send fraudulent emails.
- The recipient's email (swifthomeloans.com) suggests financial transactions may be involved, in addition to the fact that the emails originate from the same organization (Datacamp Limited) but are flagged as high risk.
- The IPs and locations remain consistent, which could mean a persistent attacker or an insider threat.

Step 1: Selecting a High-Risk Anomaly

I'll choose the most frequent sender (ccamacho@ctot.com, 82 cases) and analyze a sample of the data.

Step 2: Why This Anomaly is Concerning

- Sender: ccamacho@ctot.com has triggered high-risk alerts 82 times.
- Recipients: Multiple emails sent to financial service domains (swifthomeloans.com, theloanst.com).
- Location: All activity originates from Dallas, Texas, which could suggest either a compromised account or a sophisticated insider threat.

Run AI security analysis

For one anomaly flagged as high risk, detail why it is concerning. Then, expand your analysis to examine whether the same risk pattern is evident across a broader dataset, potentially indicating a widespread alert.


Start






Run AI security analysis



What is your security concern?

Start

Un-leak Leaks: Stop Hyper-Targeting

Track Interactivity 

Address	First Read (UTC)	Reads	Total Minutes	Vote	Active/Banned
sasha@belure.com	05/12/2023 13:27	5	21		Active
nicole@dole.com	04/12/2023 18:49	2	6		Active
laddieh@camden.com	04/12/2023 18:55	1	9		Active
james@mansfield.com					Banned
dave@northendassoc.com	04/12/2023 18:53	3	13		Active
jorge@ious.net	04/12/2023 18:51	1	3		Active

Total :  5  1

A leak not seen means a cybercriminal without context to successfully impersonate

Overview

Security

Compliance

Threat Intelligence Overview

RPost AI Forensics

Risk Model Fine Tuning

Security at a Glance

Total Emails Sent with RPost AI Intelligence

230

+25% vs Previous period

Percentage Emails Sent Encrypted

9.86%

+37,9% vs Previous period

Percentage Documents Converted into RPDs

6.9%

+33% vs Previous period

20

Threats Detected
-30% vs Previous Period

17

Prevented Leaks

3

Locked Transactions

4

Reported Lookalike Domains

Recipient Watchlist

David@myvender.com

Susan@othervendor.net

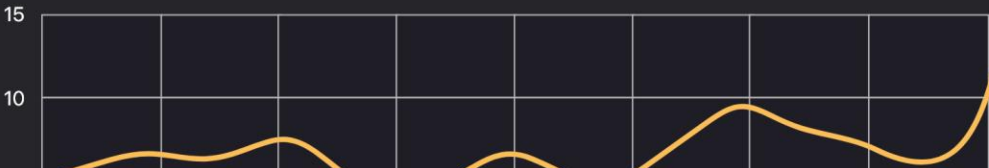
margot@vendor3.uk

Threat Intelligence Heatmap



High Risk Activites Over Time

david@northandsacc.com



Overview

Security ▼

Compliance ▼

Run AI security analysis

What is your security concern?

Start

Overview

Security ▼

Compliance ▼

Run AI security analysis

For one anomaly flagged as high risk, detail why it is concerning. Then, expand your analysis to examine whether the same risk pattern is evident across a broader dataset, potentially indicating a widespread alert.

Start

Activities Report

Recent ▼

Activities Tracker™ Intelligence

Un-Leak Leak™ Content Alive ▶

Original Message Details


Subject:
Invoice


Original Sender:
John J. Mars (John.j@northendassoc.com)


Original Recipient:
Sarah (sandra@bluepartners.com)

Original Send Time:
09/05/2023 06:06:58 PM (UTC)

Details

 Risk Level Red

 Activities 3

 Locations 3



Time(UTC)	Activity	Location	Country	Network Addr	Network	User Agent
▼ 04/11/2023 04:16:46	Open (V)	Logos	Brazil	104-28-77-151	Cloudfornet	Linux; Mozilla/4.0 (compatible; ms-office; MSOffice 16) ●●●
▼ 04/11/2023 04:16:46	Open (M)	Los Angeles	USA	14-195-146-190	AT&T	Microsoft Office/16.0 (Microsoft Outlook 16.0.14326; P) ●●●
▼ 04/11/2023 04:16:46	Open (K)	Bengaluru	India	140-48-47-505	Airtel	Mozilla/4.0 Mobile Apache Ubuntu Yowser meterpreter ●●●
<p>(V) - Activity was detected at an anonymizing VPN endpoint location</p> <p>Linux; Mozilla/4.0 (compatible; ms-office; MSOffice 16) Microsoft Office/16.0 (Microsoft Outlook 16.0.14326; Pro), Mozilla/4.0 (compatible; ms-office; MSOffice rmj) Mozilla/4.0 Mobile Apache Ubuntu Yowser meterpreter Script (compatible; ms-office; MSOffice 16) Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; Microsoft</p>						

Export to XLS

Unique Cities: 3

Unique Networks: 3

AI Security Analysis

[View details](#)

Why This Anomaly is Concerning

Sender: ccamacho@ctot.com has triggered high-risk alerts 82 times.

Recipients: Multiple emails sent to financial service domains (swifthomeloans.com, theloanstore.com), potentially indicating a phishing or fraud attempt.

Metadata is for the current activity

[IP Address: 14.195.146.190] [Time Opened: 1/23/2025 9:19:06 AM] [REMOTE_HOST: 14.195.146.190] [HTTP_HOST: open.qa.rpost.net] [SCRIPT_NAME: /open/images_v2/vzdRyNIG6Er89DI8eovJqGu6RV0PDqm2stcw1yecMjEw.gif] HTTP_CONNECTION:Keep-Alive HTTP_ACCEPT:*/* HTTP_ACCEPT_ENCODING:gzip, deflate HTTP_HOST:open.qa.rpost.net HTTP_USER_AGENT:Mozilla/4.0 (compatible; ms-office; MSOffice 16) HTTP_UA_CPU:AMD64 Connection: Keep-Alive Accept: */* Accept-Encoding: gzip, deflate Host: open.qa.rpost.net User-Agent: Mozilla/4.0 (compatible; ms-office; MSOffice 16) UA-CPU: AMD64 /LM/W3SVC/24/ROOT 0 CGI/1.1 off 24 /LM/W3SVC/24 10.0.40.196 /open/images_v2/vzdRyNIG6Er89DI8eovJqGu6RV0PDqm2stcw1yecMjEw.gif 14.195.146.190 14.195.146.190 50429 GET /open/images_v2/vzdRyNIG6Er89DI8eovJqGu6RV0PDqm2stcw1yecMjEw.gif open.qa.rpost.net 80 0 HTTP/1.1 Microsoft-IIS/10.0 /open/images_v2/

AI Security Analysis



Identified High-Risk Anomaly:

- **Sender:** [REDACTED]
- **Recipient:** [REDACTED]
- **Risk Type:** High (Red category)
- **Location:** Dallas, Texas, USA
- **Activity Pattern:** Multiple messages sent within seconds/minutes.
- **Timestamps:** Several emails were sent at identical timestamps or within a few seconds of each other, suggesting possible automation or account compromise.

Why It's Concerning:

- The sender exhibits **burst activity**, rapidly sending multiple emails to the same recipient.
- This could indicate a **compromised account** being used to send fraudulent emails.
- The recipient's email (swifthomeloans.com) suggests financial transactions may be involved, increasing the risk of phishing or fraud.
- The emails originate from the same **organization (Datacamp Limited)** but are flagged as high risk.
- The IPs and locations remain consistent, which could mean a persistent attacker or an insider threat.

Step 1: Selecting a High-Risk Anomaly

I'll choose the most frequent sender ([REDACTED], 82 cases) and analyze a sample of their activity.

Step 2: Why This Anomaly is Concerning

- **Sender:** [REDACTED] has triggered high-risk alerts 82 times.
- **Recipients:** Multiple emails sent to financial service domains (swifthomeloans.com, theloanstore.com), potentially indicating a phishing or fraud attempt.
- **Location:** All activity originates from Dallas, Texas, which could suggest either a compromised account or a coordinated fraudulent operation.

AI Security Analysis

Share to phone 📱



Share via email 📧

Identified High-Risk Anomaly:

- **Sender:** [REDACTED]
- **Recipient:** [REDACTED]
- **Risk Type:** High (Red category)
- **Location:** Dallas, Texas, USA
- **Activity Pattern:** Multiple messages sent within seconds/minutes.
- **Timestamps:** Several emails were sent at identical timestamps or within a few seconds of each other, suggesting possible automation or account compromise.

Why It's Concerning:

- The sender exhibits **burst activity**, rapidly sending multiple emails to the same recipient.
- This could indicate a **compromised account** being used to send fraudulent emails.
- The recipient's email (swifthomeloans.com) suggests financial transactions may be involved, increasing the risk of phishing or fraud.
- The emails originate from the same **organization (Datacamp Limited)** but are flagged as high risk.
- The IPs and locations remain consistent, which could mean a persistent attacker or an insider threat.

Step 1: Selecting a High-Risk Anomaly

I'll choose the most frequent sender ([REDACTED], 82 cases) and analyze a sample of their activity.

Step 2: Why This Anomaly is Concerning

- **Sender:** [REDACTED] has triggered high-risk alerts 82 times.
- **Recipients:** Multiple emails sent to financial service domains (swifthomeloans.com, theloanstore.com), potentially indicating a phishing or fraud attempt.
- **Location:** All activity originates from Dallas, Texas, which could suggest either a compromised account or a coordinated fraudulent operation.

See what's happening with the security and protection of your profile and take any actions needed.

Overview

Security



Compliance



AI Auto Lock™

Ai Auto Lock™ option for RMail & RSign

Enabled



Eavesdropping Alert

An eavesdropping attack is a malicious attempt to intercept and access data.

Enabled



Encryption

Ai Auto lock option for Rmail & Rsign

Not Enabled



DLP

Ai Auto lock option for Rmail & Rsign

Enabled



Lookalike Domain™ Detector

Ai Auto lock option for Rmail & Rsign

Not Enabled



Reply Hijack™ Alerts

Ai Auto lock option for Rmail & Rsign

Not Enabled



RMail Recommends™

Ai Auto lock option for Rmail & Rsign

Enabled



Double Blind CC™ & Private SideNote®

Ai Auto lock option for Rmail & Rsign

Enabled



Secure Large File Share™

Ai Auto lock option for Rmail & Rsign

Enabled



Secure Reply

An eavesdropping attack is a malicious attempt to intercept and access data.

Enabled



Securely Erase

Ai Auto lock option for Rmail & Rsign

Not Enabled



Prefill and Backfill

Ai Auto lock option for Rmail & Rsign

Enabled



Clickwrap Agreements

Ai Auto lock option for Rmail & Rsign

Enabled



Identity Leakers

Ai Auto lock option for Rmail & Rsign

Not Enabled



Advanced Content Controls

Ai Auto lock option for Rmail & Rsign

Enabled



Self-Destruct on a Timer

Ai Auto lock option for Rmail & Rsign

Enabled



Printing Restrictions



Restrict Views by Location

Minimize Leaked Context

Threat actors know who is communicating to whom about what when.

External leak boomerangs back to your organization as a hyper-targeted-hyper-contextual impersonation lure.



Think... F35 vs. J35

**What is the Value of
Un-Leaking Leaks Agentically?**

Bottom Line Up Front (BLUF)

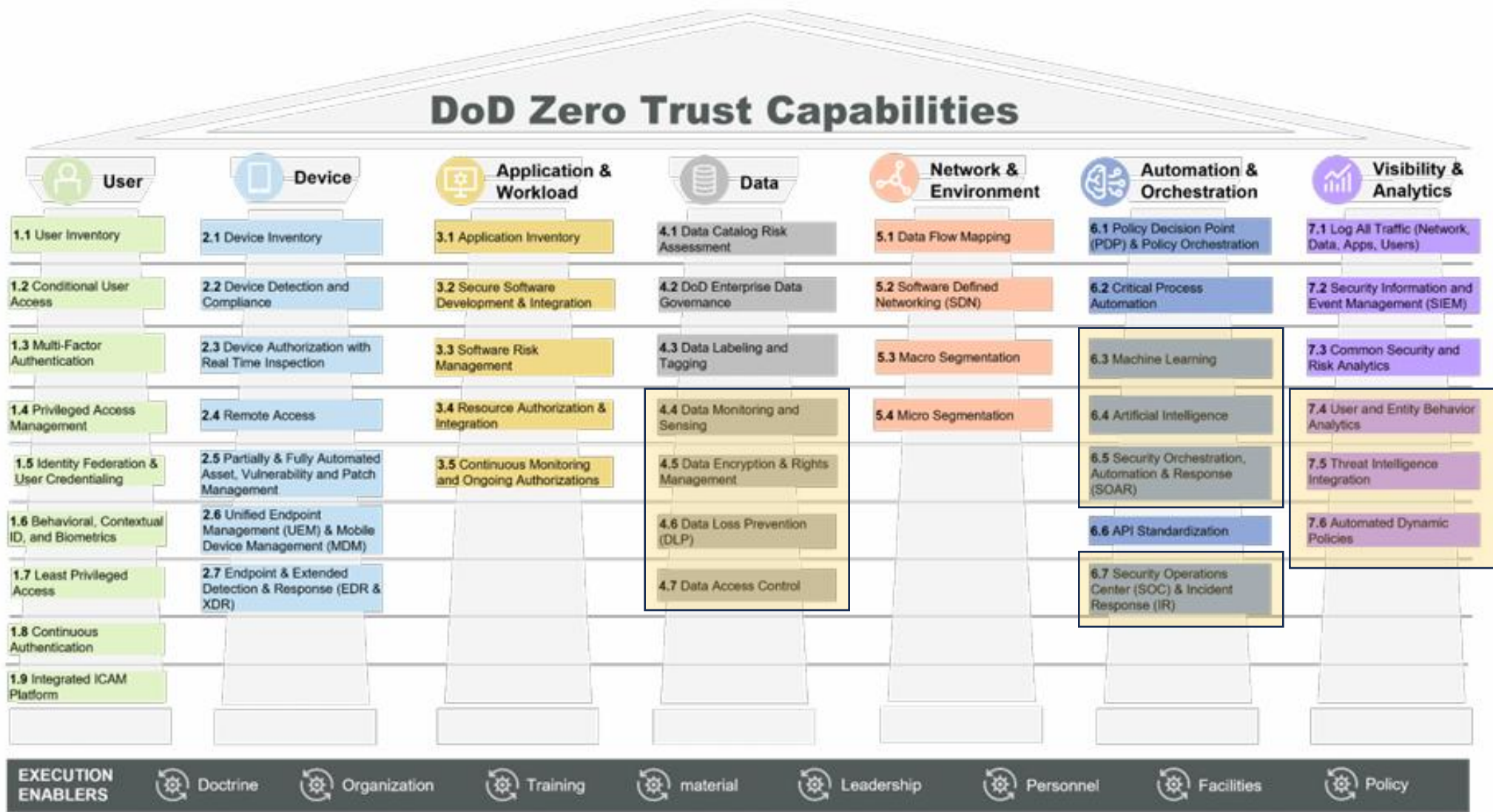
(1) Complements today's defensive security tech with a strong offense; true AI active threat hunting of sleeper cells embedded in third party systems with agentic AI to un-leak leaks. The best defense is a strong offense.

Bottom Line Up Front (BLUF)

(2) Accomplishes not only the Zero Trust Target 2027 capabilities and activities related to Pillars 4, 6, and 7, but also the related **Advanced State 2032 capabilities TODAY.**

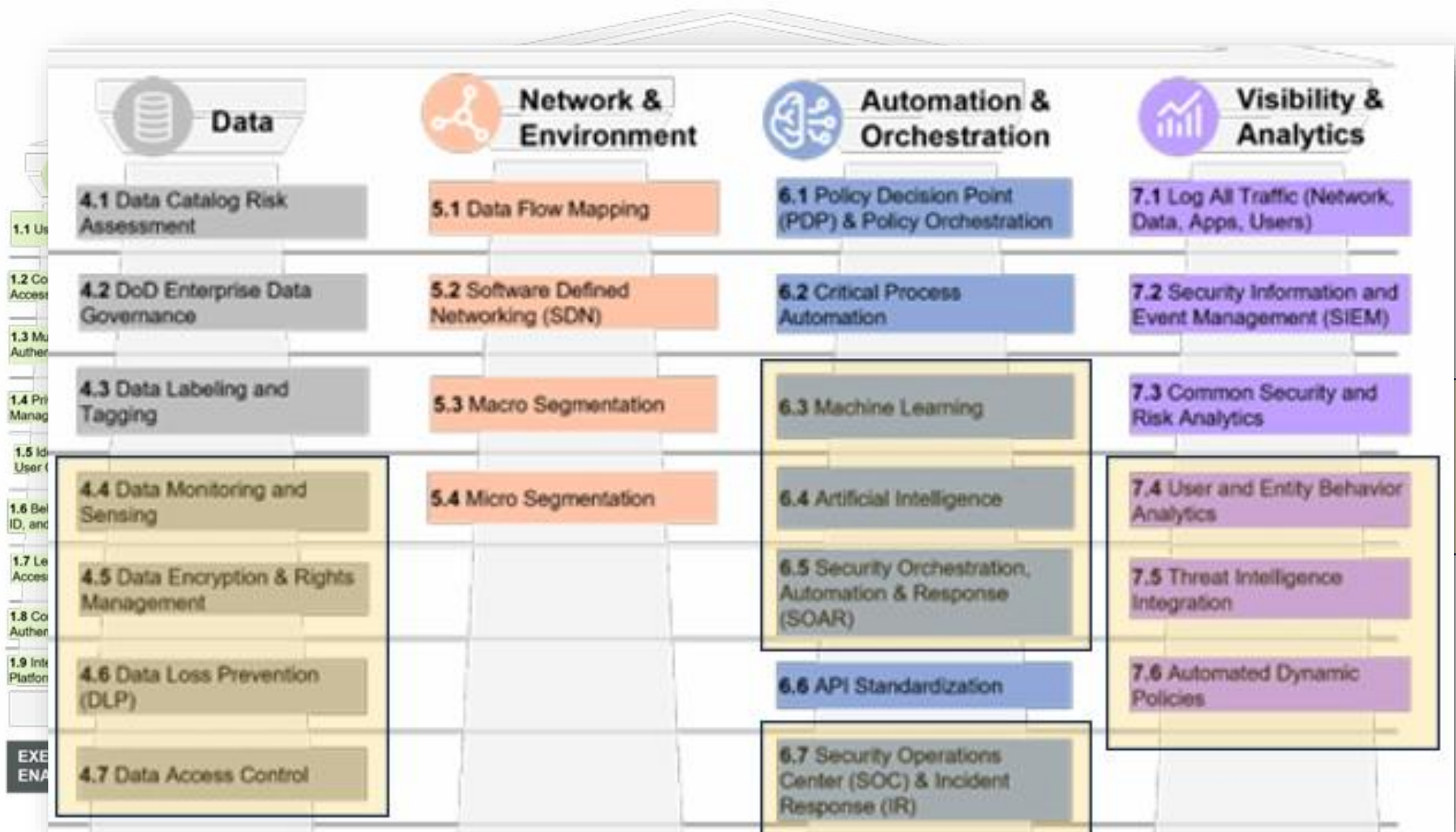
Achieve ZT 2032 for Pillars 4, 6, 7 today.

Figure 5. DoD Zero Trust Capabilities



Achieve ZT
2032 for
Pillars 4, 6,
7 today.

Figure 5. DoD Zero Trust Capabilities



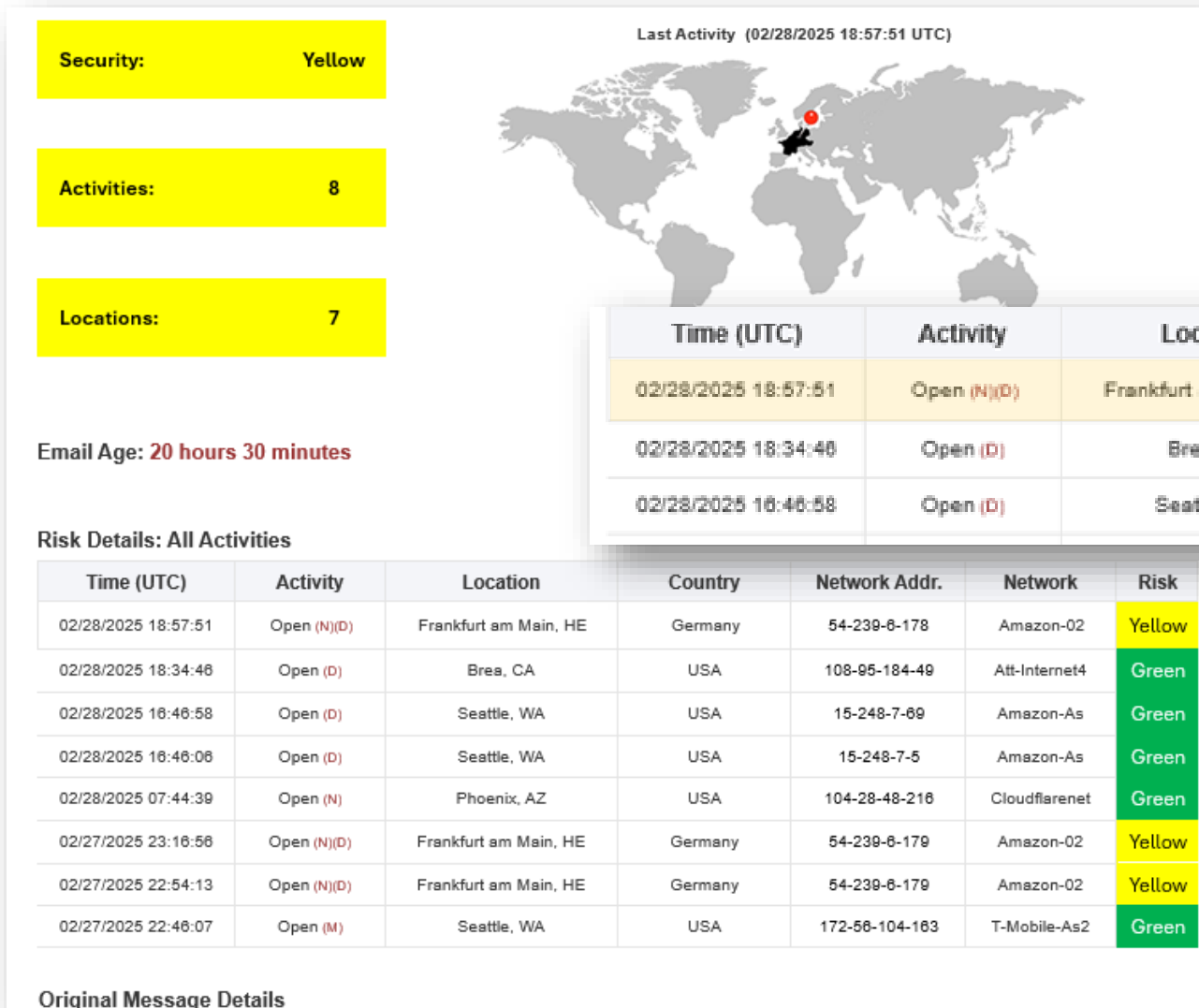


Insider & Third-Party Risk

Use Case #2: Trust But Verify.
Real-Time Security Assessment.

See the Unseen: Information Containment

"See your content route at 3rd / 4th parties that attested to US-centric containment



Trust your third parties to be maintaining your content within US-centric data centers and staff. **But verify**; see what you cannot see today.



Countering...

Third-Party Risk & Leaks

Insider Threats & Leaks

Un-Leak Leaks™

Counter Insider
Threats & Leaks

Psychological Deterrence

Insider threat – Strategic info disclosed

Pre-emptive Kill

Rogue or departing employee

Pro-active Security

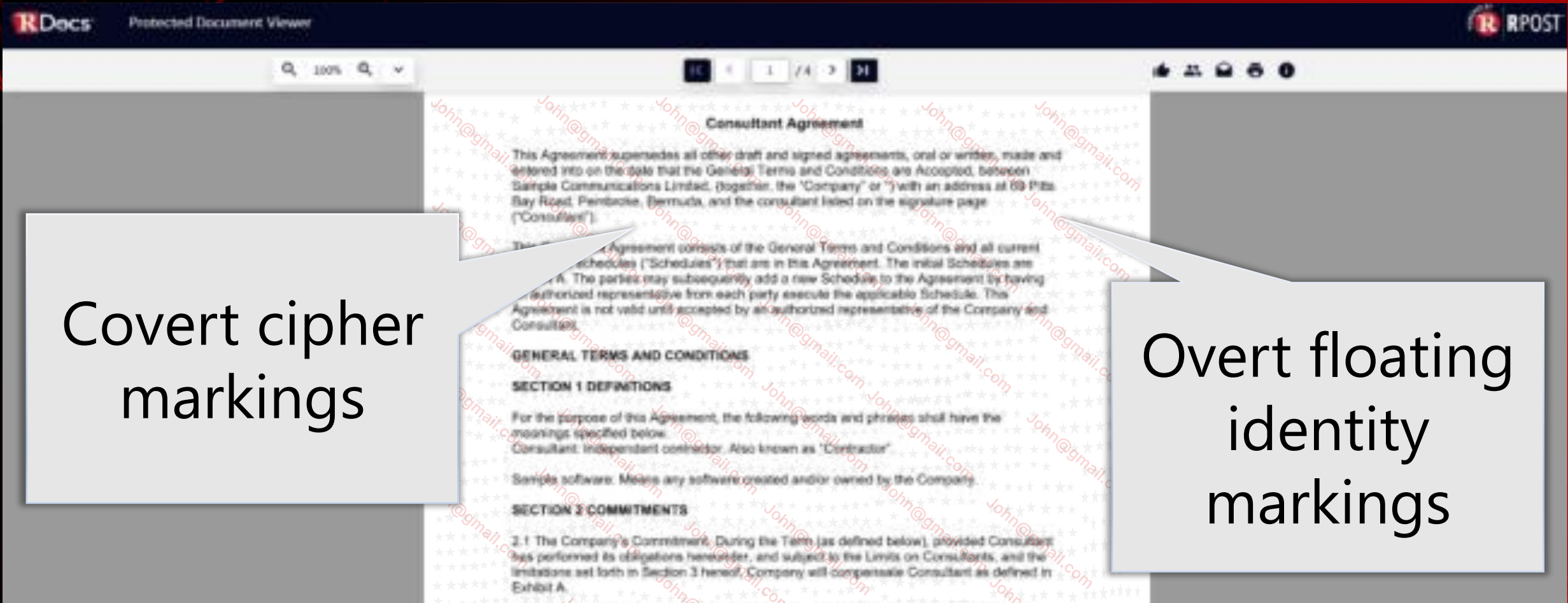
Project ends, enforce file cleanse – future risk

Counter Adversaries
& Third-Party Risks

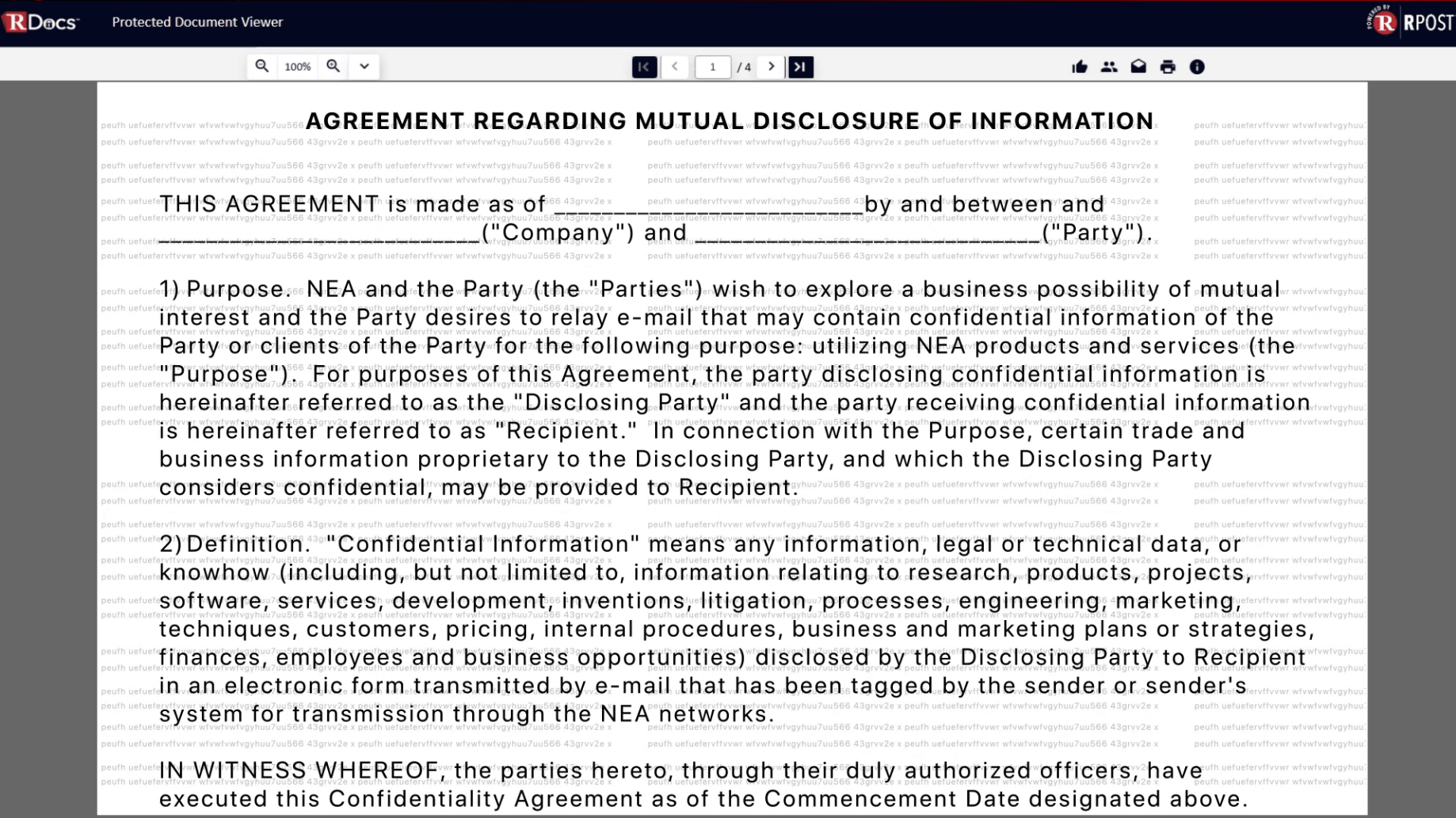
Automate Un-leak

Thwart impersonation attempts - ransomware

Deter Screen Photo Leakers



Deter Screen Photo Leakers



AGREEMENT REGARDING MUTUAL DISCLOSURE OF INFORMATION

THIS AGREEMENT is made as of [blank] by and between and [blank] ("Company") and [blank] ("Party").

1) Purpose. NEA and the Party (the "Parties") wish to explore a business possibility of mutual interest and the Party desires to relay e-mail that may contain confidential information of the Party or clients of the Party for the following purpose: utilizing NEA products and services (the "Purpose"). For purposes of this Agreement, the party disclosing confidential information is hereinafter referred to as the "Disclosing Party" and the party receiving confidential information is hereinafter referred to as "Recipient." In connection with the Purpose, certain trade and business information proprietary to the Disclosing Party, and which the Disclosing Party considers confidential, may be provided to Recipient.

2) Definition. "Confidential Information" means any information, legal or technical data, or knowhow (including, but not limited to, information relating to research, products, projects, software, services, development, inventions, litigation, processes, engineering, marketing, techniques, customers, pricing, internal procedures, business and marketing plans or strategies, finances, employees and business opportunities) disclosed by the Disclosing Party to Recipient in an electronic form transmitted by e-mail that has been tagged by the sender or sender's system for transmission through the NEA networks.

IN WITNESS WHEREOF, the parties hereto, through their duly authorized officers, have executed this Confidentiality Agreement as of the Commencement Date designated above.

©RPost 2025: Private

R RPOST™

The screenshot shows a web-based document viewer interface. At the top left, there's a logo for "RDocs" and the text "Protected Document Viewer". Below this is a navigation bar with search, zoom (100%), and other controls. The main area displays a document titled "CONFIDENTIALITY AGREEMENT". The document contains several sections:

- A header section with a repeating pattern of "peuth uefueferfvvwr wfwvwfwvgghuu7uu566 43grvv2e x" repeated across the page.
- A bolded title: "AGREEMENT REGARDING MUTUAL DISCLOSURE OF INFORMATION."
- A paragraph stating: "THIS AGREEMENT is made as of [blank] by and between and ("Company") and ("Party")."
- A numbered list starting with "1) Purpose. NEA and the Party (the \"Parties\") wish to explore a business possibility of mutual interest and the Party desires to relay e-mail that may contain confidential information of the Party or clients of the Party for the following purpose: utilizing NEA products and services (the \"Purpose\"). For purposes of this Agreement the party disclosing confidential information is hereinafter referred to as the \"Disclosing Party\" and the party receiving confidential information is hereinafter referred to as \"Recipient.\" In connection with the Purpose, certain trade and business information proprietary to the Disclosing Party, and which the Disclosing Party considers confidential, may be provided to Recipient."
- A second numbered item: "2) Definition. \"Confidential Information\" means any information, legal or technical data, or knowhow (including, but not limited to, information relating to research, products, projects, software services development, inventions, litigation processes, engineering marketing techniques, customers, pricing, internal procedures, business and marketing plans or strategies, finances employees and business opportunities) disclosed by the Disclosing Party to Recipient in an electronic form transmitted by e-mail that has been tagged by the sender or sender's system for transmission through the NEA networks."
- A final sentence: "IN WITNESS WHEREOF the parties hereto through their duly authorized officers, have executed this Confidentiality Agreement as of the Commencement Date designated above."

The bottom right corner features a large red watermark reading "COPY BY R POS".

Document ID

Subject/Description

Reader Email

Access Control

Status



14 RPDs selected (x)

Default

Expire Selected

Activate Selected



Kill Selected

+ Folders



Default

myFolders

Steph Dolde...

Shared



Type

Created (UTC)

Subject/Description

Document Name

Initial Readers

Days Since
Last Viewed

Status

Access Control



02/14/2025 18:53

Blog Article

250214 - The Good Old Days of Gentlemanly Ransomware

zkhan@rpost.com

5

Active

Track Readers



02/14/2025 07:10

G&L Contract

250101 - G&L Forum and Alliance Contract

zkhan@rpost.com

16

Active

Track Readers



02/05/2025 00:37

B-29 P&S

210322 - B29 Purchase Agreement - CLEAN

2

Active

Track Readers



12/09/2024 06:21

0150_BR_BL_RPost Seller Impersonation_Paris

investor@rpost.com

0

Expired

Limit Readers


Bottom Line Up Front (BLUF)


(2) Accomplishes not only the Zero Trust Target 2027 capabilities and activities related to Pillars 4, 6, and 7, but also the related **Advanced State 2032 capabilities TODAY.**

Bottom Line Up Front (BLUF)


(3) Meets not only today's Zero Trust goals, but also the Presidential Executive Order related to **DOGE, paragraph 4a, government tech modernization for maximum efficiency, productivity, inter-operability with data integrity assurance.**


Modernize Contract Signoffs, Workflows Sequence


 RPOST ONE™





R1: One Install Does It All™





 Stephanie Dolder


 Dashboard


 Most Popular Apps >


 Curated Training >


 All Training Videos >

 Schedule Live Demo

 Support Center

 Tech Essentials Tips

 RNews




RSign: E-Sign Made Simple

Full Featured E-Sign

Click to get started e-signing with drag-and-drop signature controls, templates, compliant security, and much more.

[SEND NOW](#)




RMail: Encrypt Email & More

Quick Send Secure

Click to send encrypted, with Registered Email™ delivery proof, files up to 1Gb, send for e-sign, and more.

[SEND NOW](#)



RDocs: Document Security

Control or Kill After Sent

Protect, control, track, or kill access to documents in-the-ether, even after sending. [Learn more.](#)

[SEND NOW](#)

Install Most Popular App

Click to install RMail & RSign inside Outlook or [browse all of our apps.](#)

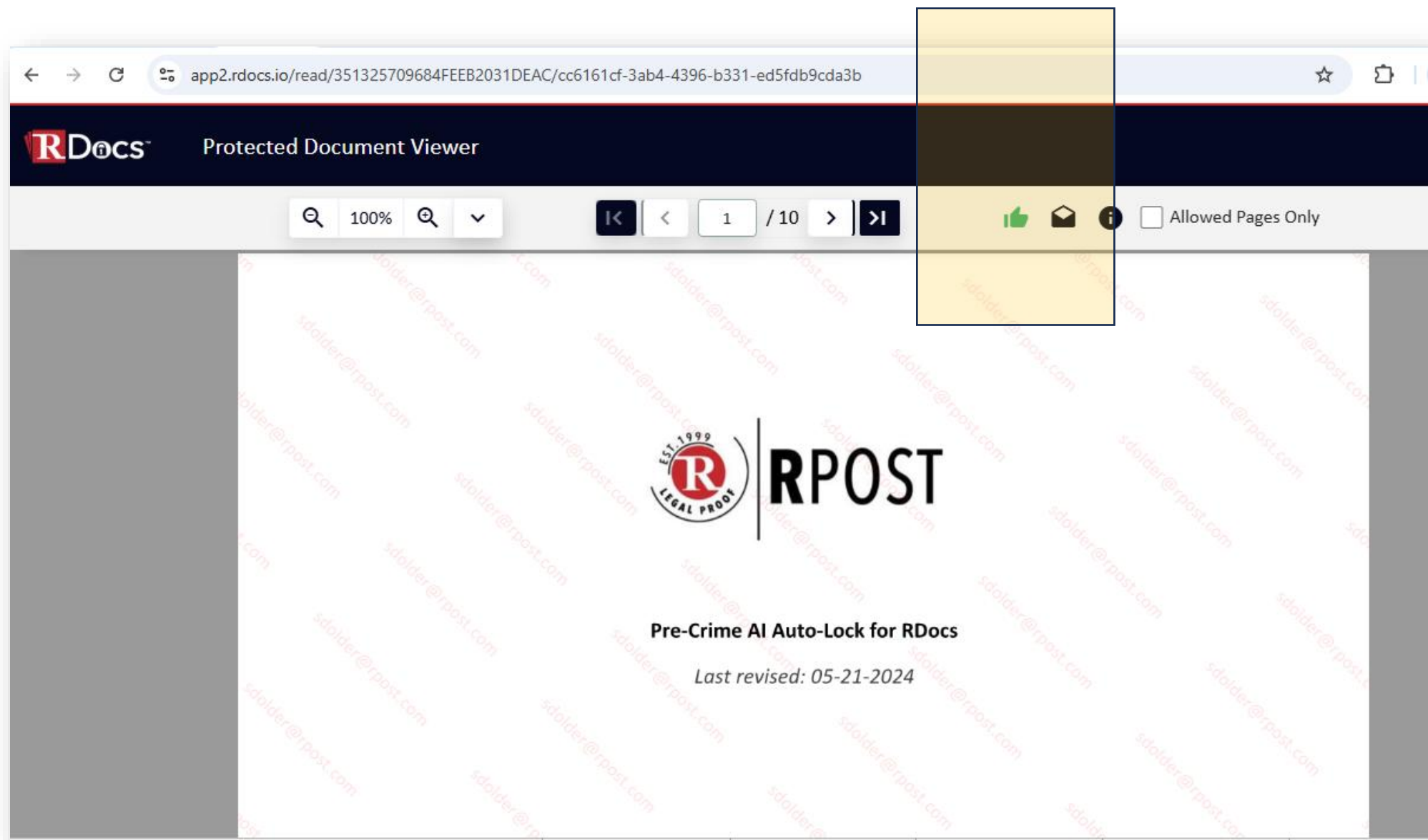
Plan Details

Plan Name	Plan Type
-----------	-----------

Plan Upgrade

Upgrade or add a license to your existing account.

Modernize Internal Signoffs, Social Docs















Modernize Internal Signoffs, Social Docs

Track Interactivity

<input type="checkbox"/>	Address	First Name	Last Name	Mobile	First Read (UTC) ↓	Reads	Total Time (hh:mm:ss)	Vote	Status
▶ <input type="checkbox"/>	nanie1219@hotmail.com	Nanie	Velez		06/25/2024 19:35	1	00:03:00		Active
▶ <input type="checkbox"/>	sdolder@rpost.com	Stephanie	Dolder		06/25/2024 19:23	2	00:22:00		Active
▶ <input type="checkbox"/>	mbrenes@rpost.com	Monse	Brenes		06/25/2024 19:17	2	00:04:00		Active
▶ <input type="checkbox"/>	sdolderrpost@gmail.com	Samantha	Dossier			0	00:00:00	-	Active
▶ <input type="checkbox"/>	testacc2@rpostlabs.com	Megan	Greene			0	00:00:00	-	Banned

Modernize Internal Signoffs, Social Docs



					 
06/25/2024 19:35	1	00:03:00			
06/25/2024 19:23	2	00:22:00			
06/25/2024 19:17	2	00:04:00			
	0	00:00:00	-		
	0	00:00:00	-		
			Total :  2  1		

Modernize Admin Legal or Time Dependent Notices

Receipt: RE: [Non-DoD Source] RPost/Gartner CIO LF Lunch // Invite Pentagon On-site Cy

Receipt <receipt@r1.rpost.net>
To: zkhan@rpost.com

DeliveryReceipt.xml 11 KB HtmlReceipt.htm 237 KB



This receipt contains verifiable proof of your RPost transaction.

The holder of this receipt has proof of delivery, message and attachment content, and official time of sending and receipt. Depend on services selected, the holder also may have proof of encrypted transmission and/or electronic signature.

To authenticate this receipt, forward this email with its attachment to 'verify@r1.rpost.net' or [click here](#)

Delivery Status					
Address	Status	Details	Delivered (UTC*)	Delivered (local)	Opened (local)
[REDACTED]@gmail.com	Delivered and Opened	HTTP-IP:66.249.83.129	03/17/2025 06:15:28 PM (UTC)	03/17/2025 01:15:28 PM (UTC -05:00)	03/17/2025 01:16:53 PM (UTC -05:00)
[REDACTED]@usmc.mil	Delivered and Opened	HTTP-IP:52.243.248.217	03/17/2025 06:15:28 PM (UTC)	03/17/2025 01:15:28 PM (UTC -05:00)	03/17/2025 01:16:02 PM (UTC -05:00)

*UTC represents Coordinated Universal Time: <https://www.ietf.org/timezones/data/zoneinfo/utc.html>

Message Envelope

From: [REDACTED] <[REDACTED]@usmc.mil>
Subject: RE: [Non-DoD Source] RPost/Gartner CIO LF Lunch // Invite Pentagon On-site Cyber-AI Briefing Mar 19
To: [REDACTED] <[REDACTED]@usmc.mil>
Cc: [REDACTED] <[REDACTED]@gmail.com>

Network ID: <00dd01db9768562840f0527adc2d0\$@rpost.com>

Received by RMail System: 03/17/2025 06:15:18 PM (UTC), 03/17/2025 01:15:18 PM (UTC -05:00) (Local)

Client Code:

Message Statistics

Tracking Number: 2DBA1BB93BBA6763CCA1BFF1368A4B706A0B0D88

Message Size: 114321

Features Used:

File Size: File Name:

49.4 KB 250228 - RPost - Pentagon Cyber AI Briefing Invitation.pdf

Delivery Audit Trail

3/17/2025 6:15:27 PM starting gmail.com/default) 3/17/2025 6:15:27 PM connecting from mta81.r3.rpost.net (0.0.0.0) to gmail-smtp-in.l.google.com (142.251.2.26) 3/17/2025 6:15:27 PM connected from 10.0.71.232:56807 3/17/2025 6:15:27 PM >>> 220 mx.google.com ESMTP d9443c01a7336-225c6888eb5si114891975ad.66 - gsmtpp 3/17/2025 6:15:27 PM <<< EHLO mta81.r3.rpost.net 3/17/2025 6:15:27 PM >>> 250-mx.google.com at your service, [3.101.2.139] 3/17/2025 6:15:27 PM >>> 250-SIZE 157286400 3/17/2025 6:15:27 PM >>> 250-8BITMIME 3/17/2025 6:15:27 PM >>> 250-STARTTLS 3/17/2025 6:15:27 PM >>> 250-ENHANCEDSTATUSCODES 3/17/2025 6:15:27 PM >>> 250-PIPELINING 3/17/2025 6:15:27 PM >>> 250-CHUNKING 3/17/2025 6:15:27 PM >>> 250-SMTPUTF8 3/17/2025 6:15:27 PM <<< STARTTLS 3/17/2025 6:15:28 PM >>> 220 2.0.0 Ready to start TLS 3/17/2025 6:15:28 PM tls:TLSv1.2 connected with 128-bit ECDHE-ECDSA-AE S128-GCM-SHA256 (session reused) 3/17/2025 6:15:28 PM tls:Cert: /CN=mx.google.com; issuer=/C=US/O=Google Trust Services/CN=W R2; verified=no 3/17/2025 6:15:28 PM <<< EHLO mta81.r3.rpost.net 3/17/2025 6:15:28 PM >>> 250-mx.google.com at your service, [3.101.2.139] 3/17/2025 6:15:28 PM >>> 250-SIZE 157286400 3/17/2025 6:15:28 PM >>> 250-8BITMIME 3/17/2025 6:15:28 PM >>> 250-ENHANCEDSTATUSCODES 3/17/2025 6:15:28 PM >>> 250-PIPELINING 3/17/2025 6:15:28 PM >>> 250-CHUNKING 3/17/2025 6:15:28 PM >>> 250-SMTPUTF8 3/17/2025 6:15:28 PM <<< MAIL FROM: BODY=8BITMIME 3/17/2025 6:15:28 PM >>> 250 2.0.1 OK d9443c01a7336-225

a7336-225c6888eb5si114891975ad.66 - gsmtpp 3/17/2025 6:15:29 PM closed gmail-smtp-in.l.google.com (142.251.2.26) in=773 out=115907 3/17/2025 6:15:29 PM done gmail.com/default)

3/17/2025 6:15:26 PM starting usmc.mil/default) 3/17/2025 6:15:26 PM connecting from mta81.r3.rpost.net (0.0.0.0) to pri-jeemsg.eemsg.mail.mil (156.112.250.1) 3/17/2025 6:15:26 PM connected from 10.0.71.232:51241 3/17/2025 6:15:27 PM >>> 220 USAT19PA30.eemsg.mail.mil ESMTP 3/17/2025 6:15:27 PM <<< EHLO mta81.r3.rpost.net 3/17/2025 6:15:27 PM >>> 250-USAT19PA30.eemsg.mail.mil 3/17/2025 6:15:27 PM >>> 250-8BITMIME 3/17/2025 6:15:27 PM >>> 250-SIZE 72351744 3/17/2025 6:15:27 PM >>> 250-STARTTLS 3/17/2025 6:15:27 PM <<< STARTTLS 3/17/2025 6:15:27 PM >>> 220 Go ahead with TLS 3/17/2025 6:15:27 PM tls:TLSv1.2 connected with 256-bit ECDHE-RSA-AES256-GCM-SHA384 3/17/2025 6:15:27 PM tls:Cert: /C=US/ST=Maryland/L=Fort Meade/O=DISA/CN=* eemsg.mail.mil; issuer=/C=US/O=Entrust, Inc./OU=See www.entrust.net/legal-terms/OU=gc 2012 Entrust, Inc. - for authorized use only/CN=Entrust Certification Authority - L1K; verified=no 3/17/2025 6:15:27 PM <<< EHLO mta81.r3.rpost.net 3/17/2025 6:15:27 PM >>> 250-USAT19PA30.eemsg.mail.mil 3/17/2025 6:15:27 PM >>> 250-8BITMIME 3/17/2025 6:15:27 PM >>> 250-SIZE 72351744 3/17/2025 6:15:27 PM <<< MAIL FROM: BODY=8BITMIME 3/17/2025 6:15:28 PM >>> 250 sender ok 3/17/2025 6:15:28 PM <<< RCPT TO: 3/17/2025 6:15:28 PM >>> 250 recipient ok 3/17/2025 6:15:28 PM <<< DATA 3/17/2025 6:15:28 PM >>> 354 go ahead 3/17/2025 6:15:28 PM <<< 3/17/2025 6:15:28 PM >>> 250 ok: Message 73348074 accepted 3/17/2025 6:15:28 PM <<< QUIT 3/17/2025 6:15:28 PM >>> 221 USAT19PA30.eemsg.mail.mil 3/17/2025 6:15:28 PM closed pri-jeemsg.eemsg.mail.mil (156.112.250.1) in=408 out=115910 3/17/2025 6:15:28 PM done usmc.mil/default)

From: postmaster@mta81.r3.rpost.net: Hello, this is the mail server on mta81.r3.rpost.net. I am sending you this message to inform you on the delivery status of a message you previously sent. Immediately below you will find a list of the affected recipients; also attached is a Delivery Status Notification (DSN) report in standard format, as well as the headers of the original message. relayed to mailer gmail-smtp-in.l.google.com (142.251.2.26)

[IP Address: 66.249.83.129] [Time Opened: 3/17/2025 6:16:53 PM] [REMOTE_HOST: 192.168.20.95] [HTTP_HOST: open.r1.rpost.net] [SCRIPT_NAME: /open/images_v2/PzkgdXQ6CCTZ1X1CPKw1FbtKQ8toY0Z1hDTnBHwMjEw.png] HTTP_ACCEPT_ENCODING: gzip, deflate, br HTTP_HOST: open.r1.rpost.net HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 5.1; rv:11.0) Gecko Firefox/11.0 (via ggphht.com GoogleImageProxy) HTTP_X_FORWARDED_FOR: 66.249.83.129 HTTP_X_FORWARDED_PROTO: https HTTP_X_FORWARDED_PORT: 443 HTTP_X_AMZN_TRACE_ID: Root=1-67d88715-34985ea48ba2c8062d5909d6 Accept-Encoding: gzip, deflate, br Host: open.r1.rpost.net User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:11.0) Gecko Firefox/11.0 (via ggphht.com GoogleImageProxy) X-Forwarded-For: 66.249.83.129 X-F-Forwarded-Proto: https X-Forwarded-Port: 443 X-Amzn-Trace-Id: Root=1-67d88715-34985ea48ba2c8062d5909d6 /LM/W3SVC/12/ROOT/256 2048 CN=rpost.com Root Cert CN=admin1.devx.rpost.info 0 CGI/1.1 on 256 2048 CN=rpost.com Root Cert CN=admin1.devx.rpost.info 12 /LM/W3SVC/12 192.168.10.112 /open/images_v2/PzkgdXQ6CCTZ1X1CPKw1FbtKQ8toY0Z1hDTnBHwMjEw.png 192.168.20.95 192.168.20.95 39092 GET /open/images_v2/PzkgdXQ6CCTZ1X1CPKw1FbtKQ8toY0Z1hDTnBHwMjEw.png open.r1.rpost.net 443 1 HTTP/1.1 Mozilla/5.0 (Windows NT 5.1; rv:11.0) Gecko Firefox/11.0 (via ggphht.com GoogleImageProxy) 66.249.83.129 https 443 Root=1-67d88715-34985ea48ba2c8062d5909d6

From: postmaster@mta81.r3.rpost.net: Hello, this is the mail server on mta81.r3.rpost.net. I am sending you this message to inform you on the delivery status of a message you previously sent. Immediately below you will find a list of the affected recipients; also attached is a Delivery Status Notification (DSN) report in standard format, as well as the headers of the original message. relayed to mailer pri-jeemsg.eemsg.mail.mil (156.112.250.1)

[IP Address: 52.243.248.217] [Time Opened: 3/17/2025 6:16:02 PM] [REMOTE_HOST: 192.168.10.57] [HTTP_HOST: open.r1.rpost.net] [SCRIPT_NAME: /open/images_v2/oV2A6RZk1froPBglg121XZ8qurmQWOeDpJChzhDMjEw.png] HTTP_ACCEPT_ENCODING: gzip, deflate, br HTTP_HOST: open.r1.rpost.net HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 10.0; Win64; x84) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 HTTP_X_FORWARDED_FOR: 52.243.248.217 HTTP_X_FORWARDED_PROTO: https HTTP_X_FORWARDED_PORT: 443 HTTP_X_AMZN_TRACE_ID: Root=1-67d886e2-32813dad1c726bd333a2ea4d Accept-Encoding: gzip, deflate, br Host: open.r1.rpost.net User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x84) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 X-Forwarded-For: 52.243.248.217 X-Forwarded-Proto: https X-Forwarded-Port: 443 X-Amzn-Trace-Id: Root=1-67d886e2-32813dad1c726bd333a2ea4d /LM/W3SVC/12/ROOT/256 2048 CN=rpost.com Root Cert CN=admin1.devx.rpost.info 0 CGI/1.1 on 256 2048 CN=rpost.com Root Cert CN=admin1.devx.rpost.info 12 /LM/W3SVC/12 192.168.10.112 /open/images_v2/oV2A6RZk1froPBglg121XZ8qurmQWOeDpJChzhDMjEw.png 192.168.10.57 192.168.10.57 41850 GET /open/images_v2/oV2A6RZk1froPBglg121XZ8qurmQWOeDpJChzhDMjEw.png open.r1.rpost.net 443 1 HTTP/1.1 Mozilla/5.0 (Windows NT 10.0; Win64; x84) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 52.243.248.217 https 443 Root=1-67d886e2-32813dad1c726bd333a2ea4d



Modernize Admin Legal or Time Dependent Notices

Receipt: RE: [Non-DoD Source] RPost/Gartner CIO LF Lunch // Invite Pentagon On-site Cyl



Receipt <receipt@r1.rpost.net>

To zkhan@rpost.com



DeliveryReceipt.xml 11 KB



HtmlReceipt.htm 237 KB



REGISTERED RECEIPT
EVIDENCE OF DELIVERY, CONTENT & TIME



This receipt contains verifiable proof of your RPost transaction.
The holder of this receipt has proof of delivery, message and attachment content, and official time of sending and receipt. Depending on services selected, the holder also may have proof of encrypted transmission and/or electronic signature.

To authenticate this receipt, forward this email with its attachment to 'verify@r1.rpost.net' or [click here](#)

Delivery Status					
Address	Status	Details	Delivered (UTC*)	Delivered (local)	Opened (local)
[REDACTED]@mail.com	Delivered and Opened	HTTP-IP:66.249.83.129	03/17/2025 06:15:28 PM (UTC)	03/17/2025 01:15:28 PM (UTC -05:00)	03/17/2025 01:16:53 PM (UTC -05:00)
[REDACTED]@usmc.mil	Delivered and Opened	HTTP-IP:52.243.248.217	03/17/2025 06:15:28 PM (UTC)	03/17/2025 01:15:28 PM (UTC -05:00)	03/17/2025 01:16:02 PM (UTC -05:00)

*UTC represents Coordinated Universal Time: <https://www.rmail.com/resources/coordinated-universal-time/>

Message Envelope	
From:	[REDACTED] Khan [REDACTED]@st.com>
Subject:	RE: [Non-DoD Source] RPost/Gartner CIO LF Lunch // Invite Pentagon On-site Cyber-AI Briefing Mar 19
To:	[REDACTED]@usmc.mil>
Cc:	[REDACTED]@gmail.com>





```

7/336-225c6888eb5511489175ad66 - gsmtp 3/17/2025 6:15:29 PM closed gmail-smtp-in.l.google.com (142.251.2.26) in=773 out=11590
7/3/17/2025 6:15:28 PM done gmail.com/{default}

3/17/2025 6:15:28 PM starting usmc.mil{default} 3/17/2025 6:15:28 PM connecting from mta81.r3.post.net (0.0.0.0) to pri-jeemsg.eemsg.
mail.mil (156.112.250.1) 3/17/2025 6:15:28 PM connected from 10.0.71.232:51241 3/17/2025 6:15:27 PM >>> 220 USAT19PA30.eemsg.m
ail.mil ESMTP 3/17/2025 6:15:27 PM <<< EHLO mta81.r3.post.net 3/17/2025 6:15:27 PM >>> 250-USAT19PA30.eemsg.mail.mil 3/17/202
5 6:15:27 PM >>> 250-8BITMIME 3/17/2025 6:15:27 PM >>> 250-SIZE 72351744 3/17/2025 6:15:27 PM >>> 250 STARTTLS 3/17/2025 6
:15:27 PM >>> STARTTLS 3/17/2025 6:15:27 PM >>> 220 Go ahead with TLS 3/17/2025 6:15:27 PM tls:TLSv1.2 connected with 256-bit E
CDHE-RSA-AES256-GCM-SHA384 3/17/2025 6:15:27 PM tls:Cert: /C=US/ST=Maryland/L=Fort Meade/O=DISA/CN=*.eemsg.mail.mil; iss
uer=/C=US/O=Entrust, Inc./OU=See www.entrust.net/legal-terms/OU=C) 2012 Entrust, Inc. - for authorized use only/CN=Entrust Certific
ation Authority - L1K; verified=no 3/17/2025 6:15:27 PM <<< EHLO mta81.r3.post.net 3/17/2025 6:15:27 PM >>> 250-USAT19PA30.eemsg.
mail.mil 3/17/2025 6:15:27 PM >>> 250-8BITMIME 3/17/2025 6:15:27 PM >>> 250 SIZE 72351744 3/17/2025 6:15:27 PM <<< MAIL FROM
: BODY=8BITMIME 3/17/2025 6:15:28 PM >>> 250 sender ok 3/17/2025 6:15:28 PM <<< RCPT TO: 3/17/2025 6:15:28 PM >>> 250 recip
ient ok 3/17/2025 6:15:28 PM <<< DATA 3/17/2025 6:15:28 PM >>> 354 go ahead 3/17/2025 6:15:28 PM <<< 3/17/2025 6:15:28 PM >>>
250 ok: Message 723546074 accepted 3/17/2025 6:15:28 PM <<< QUIT 3/17/2025 6:15:28 PM >>> 221 USAT19PA30.eemsg.mail.mil 3/17/
2025 6:15:28 PM closed pri-jeemsg.eemsg.mail.mil (156.112.250.1) in=406 out=115910 3/17/2025 6:15:28 PM done usmc.mil{default}

From:postmaster@mta81.r3.post.net:Hello, this is the mail server on mta81.r3.post.net. I am sending you this message to inform you on t
he delivery status of a message you previously sent. Immediately below you will find a list of the affected recipients; also attached is a Deliv
ery Status Notification (DSN) report in standard format, as well as the headers of the original message. relayed to mailer gmail-smtp-in.l.g
oogle.com (142.251.2.26)

[IP Address: 66.249.83.129] [Time Opened: 3/17/2025 6:16:53 PM] [REMOTE_HOST: 192.168.20.95] [HTTP_HOST: open.r1.rpost.net] [SC
RIPT_NAME: /open/images_v2/PIzkgdXQC6CCTZX1CPKfw1FbtKQ8toY0Z1hDTnBHwMjEw.png] HTTP_ACCEPT_ENCODING:gzip, deflate
, br HTTP_HOST:open.r1.rpost.net HTTP_USER_AGENT:Mozilla/5.0 (Windows NT 5.1; rv:11.0) Gecko Firefox/11.0 (via ggphpt.com GoogleI
mageProxy) HTTP_X_FORWARDED_FOR:66.249.83.129 HTTP_X_FORWARDED_PROTO:https HTTP_X_FORWARDED_PORT:443 HT
TP_X_AMZN_TRACE_ID:Root=1-67d86715-34985ea46ba2c9062d5909d6 Accept-Encoding: gzip, deflate, br Host: open.r1.rpost.net User
-Agent: Mozilla/5.0 (Windows NT 5.1; rv:11.0) Gecko Firefox/11.0 (via ggphpt.com GoogleImageProxy) X-Forwarded-For: 66.249.83.129 X-F
orwarded-Proto: https X-Forwarded-Proto: 443 X-Amzn-Trace-Id: Root=1-67d86715-34985ea46ba2c9062d5909d6 /LM/W3SVC/12/ROOT 2
56 2048 CN=rpst.com Root Cert CN=admin1.devx.rpost.info 0 CGI/1.1 on 256 2048 CN=rpst.com Root Cert CN=admin1.devx.rpost.info
12 /LM/W3SVC/12 192.168.10.112 /open/images_v2/PIzkgdXQC6CCTZX1CPKfw1FbtKQ8toY0Z1hDTnBHwMjEw.png 192.168.20.95 192.16
8.20.95 39092 GET /open/images_v2/PIzkgdXQC6CCTZX1CPKfw1FbtKQ8toY0Z1hDTnBHwMjEw.png open.r1.rpost.net 443 1 HTTP/1.1 Mic
rosoft-Internet-Explorer/10.0 /open/images_v2/PIzkgdXQC6CCTZX1CPKfw1FbtKQ8toY0Z1hDTnBHwMjEw.png gzip, deflate, br open.r1.rpost.net Mozilla
/5.0 (Windows NT 5.1; rv:11.0) Gecko Firefox/11.0 (via ggphpt.com GoogleImageProxy) 66.249.83.129 https 443 Root=1-67d86715-34985ea
46ba2c9062d5909d6

From:postmaster@mta81.r3.post.net:Hello, this is the mail server on mta81.r3.post.net. I am sending you this message to inform you on t
he delivery status of a message you previously sent. Immediately below you will find a list of the affected recipients; also attached is a Deliv
ery Status Notification (DSN) report in standard format, as well as the headers of the original message. relayed to mailer pri-jeemsg.eemsg
.mail.mil (156.112.250.1)

[IP Address: 62.243.248.217] [Time Opened: 3/17/2025 6:16:02 PM] [REMOTE_HOST: 192.168.10.57] [HTTP_HOST: open.r1.rpost.net] [S
CRIPT_NAME: /open/images_v2/oV2A6RZk1froPBglf21Xzi6qurmQW0eDpJChzhDMjEw.png] HTTP_ACCEPT:image/* HTTP_HOST:ope
n.r1.rpost.net HTTP_USER_AGENT:Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0
.0 Safari/537.36 HTTP_X_FORWARDED_FOR:52.243.248.217 HTTP_X_FORWARDED_PROTO:https HTTP_X_FORWARDED_PORT:4
43 HTTP_X_AMZN_TRACE_ID:Root=1-67d866e2-32813dad1c726bd333a2ea4d Accept: image/* Host: open.r1.rpost.net User-Agent: Moz
illa/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 X-Forwarded-For: 52.2
43.248.217 X-Forwarded-Proto: https X-Forwarded-Proto: 443 X-Amzn-Trace-Id: Root=1-67d866e2-32813dad1c726bd333a2ea4d /LM/W3SVC
/12/ROOT 256 2048 CN=rpst.com Root Cert CN=admin1.devx.rpost.info 0 CGI/1.1 on 256 2048 CN=rpst.com Root Cert CN=admin1.d
evx.rpost.info 12 /LM/W3SVC/12 192.168.10.112 /open/images_v2/oV2A6RZk1froPBglf21Xzi6qurmQW0eDpJChzhDMjEw.png 192.168.1
0.57 192.168.10.57 41650 GET /open/images_v2/oV2A6RZk1froPBglf21Xzi6qurmQW0eDpJChzhDMjEw.png open.r1.rpost.net 443 1 HT
TP/1.1 Microsoft-Internet-Explorer/10.0 /open/images_v2/oV2A6RZk1froPBglf21Xzi6qurmQW0eDpJChzhDMjEw.png image/* open.r1.rpost.net Mozilla
/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 52.243.248.217 https 443 R
oot=1-67d866e2-32813dad1c726bd333a2ea4d

```

Modernize Admin Legal or Time Dependent Notices

Receipt: RE: [Non-DoD Source] RPost/Gartner CIO LF Lunch // Invite Pentagon On-site Cyk



Receipt <receipt@r1.rpost.net>

To zkhan@rpost.com



DeliveryReceipt.xml 11 KB



HtmlReceipt.htm 237 KB



REGISTERED RECEIPT
EVIDENCE OF DELIVERY, CONTENT & TIME



This receipt contains verifiable proof of your RPost transaction.

The holder of this receipt has proof of delivery, message and attachment content, and official time of sending and receipt. Depending on services selected, the holder also may have proof of encrypted transmission and/or electronic signature.

To authenticate this receipt, forward this email with its attachment to 'verify@r1.rpost.net' or [click here](#)

Delivery Status

Receipt: Insurance Policy Review (Delivery Failure)

Authentication <support@r1.ppost.net>
To: tom@northendassoc.com

SMTP Log-1.txt 3 KB	SMTP Log-2.txt 2 KB	SMTP Log-3.txt 2 KB
SMTP Log-4.rec.txt 151 bytes	SMTP History-1.txt 3 KB	SMTP History-2.txt 2 KB
SMTP History-3.txt	MUA_Record-1.txt	HTTP_Record-1.txt

RECEIPT AUTHENTICATION
PROOF OF DELIVERY, CONTENT & TIME

The receipt you have submitted to our system is valid.
**** A copy of the original message will be sent to your email address.**

To retrieve the decryption password [click here](#).

Address	Status	Details
drlucasjones@outlook.com	Delivered and Opened	MUA+HTTP-IP
bobdavisinsurance@gmail.com	Delivered and Opened	HTTP-IP: 74.12
alice@northendassoc.com	Relayed to Mail Server	relayed.mx-biz (67.195.228.75)
mark@northendassoc.com	Delivery Failed	5.1.2 (bad destination domain)

*UTC represents Coordinated Universal Time: <https://www.mail-archive.com/>

Message Envelope

From: tom@northendassoc.com
Subject: Insurance Policy Review
To: <drlucasjones@outlook.com>
Cc: <alice@northendassoc.com>
Bcc:
Network ID: <0bfdd01d60bbcd...>
Received by RMail System: 4/6/2020 2:40:18 AM
Client Code:

Message Statistics

Tracking Number: F95542A9A2EEBB4E
Message Size: 638204
Features Used:
File Size (bytes): 460330
File Name: Insurance Policy Review.pdf

Delivery Audit Trail

4/6/2020 2:40:18 AM starting outlook-com-inta-tls in 4/6/2020 2:40:18 AM starting outlook-com-protection.outlook.com (104.47.0.33) in 4/6/2020 2:40:18 AM connecting from mta21.r1.ppost.net (0.0.0.0) to outlook-com.olc.protection.outlook.com (104.47.0.33)
4/6/2020 2:40:18 AM C [IP Address: 76.118.20.145] [Time Opened: 4/6/2020 2:40:37 AM] [REMOTE_HOST: 76.118.20.145] [HTTP_HOST: open.r1.ppost.net] [SCRIPT_NAME: /open/images/zlXGa6EaCoTd1tFGFvMAYAMQ2rxxyt4erzkd0.gif]
4/6/2020 2:40:18 AM Mon, 6 Apr 2020 02:40:37 AM HTTP_CONNECTION: Keep-Alive
4/6/2020 2:40:18 AM HTTP_ACCEPT: */*
4/6/2020 2:40:18 AM HTTP_ACCEPT_ENCODING: gzip, deflate
4/6/2020 2:40:18 AM HTTP_HOST: open.r1.ppost.net
4/6/2020 2:40:18 AM HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
4/6/2020 2:40:18 AM Connection: Keep-Alive
4/6/2020 2:40:18 AM Accept: /*
4/6/2020 2:40:18 AM Accept-Encoding: gzip, deflate
4/6/2020 2:40:18 AM Host: open.r1.ppost.net
4/6/2020 2:40:18 AM User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
4/6/2020 2:40:18 AM Content-Type: application/pdf
4/6/2020 2:40:18 AM Content-Disposition: inline; filename=Insurance Policy Review.pdf
4/6/2020 2:40:18 AM Content-Length: 455000
4/6/2020 2:40:18 AM Content-MD5: 8b1a9953c421c2ee30e292fc222c7b5c
4/6/2020 2:40:18 AM Content-Type: application/pdf
4/6/2020 2:40:18 AM Content-Disposition: inline; filename=Insurance Policy Review.pdf
4/6/2020 2:40:18 AM Content-Length: 455000
4/6/2020 2:40:18 AM Content-MD5: 8b1a9953c421c2ee30e292fc222c7b5c

Receipt: Insurance Policy Review (Delivery Failure)

Authentication <support@r1.ppost.net>
To: tom@northendassoc.com

SMTP Log-1 - Notepad
File Edit Format View Help
4/6/2020 2:40:18 AM starting outlook.com/mta-tls

SMTP Log-2 - Notepad
File Edit Format View Help
4/6/2020 2:40:18 AM C [IP Address: 76.118.20.145] [Time Opened: 4/6/2020 2:40:37 AM] [REMOTE_HOST: 76.118.20.145] [HTTP_HOST: open.r1.ppost.net] [SCRIPT_NAME: /open/images/zlXGa6EaCoTd1tFGFvMAYAMQ2rxxyt4erzkd0.gif]
4/6/2020 2:40:18 AM Mon, 6 Apr 2020 02:40:37 AM HTTP_CONNECTION: Keep-Alive
4/6/2020 2:40:18 AM HTTP_ACCEPT: */*
4/6/2020 2:40:18 AM HTTP_ACCEPT_ENCODING: gzip, deflate
4/6/2020 2:40:18 AM HTTP_HOST: open.r1.ppost.net
4/6/2020 2:40:18 AM HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
4/6/2020 2:40:18 AM Connection: Keep-Alive
4/6/2020 2:40:18 AM Accept: /*
4/6/2020 2:40:18 AM Accept-Encoding: gzip, deflate
4/6/2020 2:40:18 AM Host: open.r1.ppost.net
4/6/2020 2:40:18 AM User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
4/6/2020 2:40:18 AM Content-Type: application/pdf
4/6/2020 2:40:18 AM Content-Disposition: inline; filename=Insurance Policy Review.pdf
4/6/2020 2:40:18 AM Content-Length: 455000
4/6/2020 2:40:18 AM Content-MD5: 8b1a9953c421c2ee30e292fc222c7b5c
4/6/2020 2:40:18 AM Content-Type: application/pdf
4/6/2020 2:40:18 AM Content-Disposition: inline; filename=Insurance Policy Review.pdf
4/6/2020 2:40:18 AM Content-Length: 455000
4/6/2020 2:40:18 AM Content-MD5: 8b1a9953c421c2ee30e292fc222c7b5c

HTTP Record-1 - Notepad
File Edit Format View Help
4/6/2020 2:40:18 AM C [IP Address: 76.118.20.145] [Time Opened: 4/6/2020 2:40:37 AM] [REMOTE_HOST: 76.118.20.145] [HTTP_HOST: open.r1.ppost.net] [SCRIPT_NAME: /open/images/zlXGa6EaCoTd1tFGFvMAYAMQ2rxxyt4erzkd0.gif]
4/6/2020 2:40:18 AM Mon, 6 Apr 2020 02:40:37 AM HTTP_CONNECTION: Keep-Alive
4/6/2020 2:40:18 AM HTTP_ACCEPT: */*
4/6/2020 2:40:18 AM HTTP_ACCEPT_ENCODING: gzip, deflate
4/6/2020 2:40:18 AM HTTP_HOST: open.r1.ppost.net
4/6/2020 2:40:18 AM HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
4/6/2020 2:40:18 AM Connection: Keep-Alive
4/6/2020 2:40:18 AM Accept: /*
4/6/2020 2:40:18 AM Accept-Encoding: gzip, deflate
4/6/2020 2:40:18 AM Host: open.r1.ppost.net
4/6/2020 2:40:18 AM User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
4/6/2020 2:40:18 AM Content-Type: application/pdf
4/6/2020 2:40:18 AM Content-Disposition: inline; filename=Insurance Policy Review.pdf
4/6/2020 2:40:18 AM Content-Length: 455000
4/6/2020 2:40:18 AM Content-MD5: 8b1a9953c421c2ee30e292fc222c7b5c
4/6/2020 2:40:18 AM Content-Type: application/pdf
4/6/2020 2:40:18 AM Content-Disposition: inline; filename=Insurance Policy Review.pdf
4/6/2020 2:40:18 AM Content-Length: 455000
4/6/2020 2:40:18 AM Content-MD5: 8b1a9953c421c2ee30e292fc222c7b5c

tom@northendassoc.com
To: drlucasjones@outlook.com; bobdavisinsurance@gmail.com
Cc: alice@northendassoc.com; mark@northendassoc.com

If there are problems with how this message is displayed, click here to view it in a web browser.

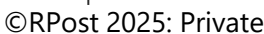
Insurance Policy Review.pdf
455 KB

REGISTERED EMAIL™ | ENCRYPTED

This is an encrypted email from [tom@northendassoc.com](#).

Please use your password to open the encrypted message attached to this email.

How to Open:
Click on the "Open" button in the top right corner of the email client. If you are using a mobile device, you may need to tap the "Open" button multiple times. Once the message is opened, you will see the decrypted content of the email.




Bottom Line Up Front (BLUF)

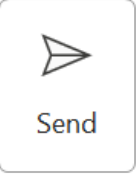
(4) Implements with **commercial-off-the-shelf software service available on AT&T's GSA schedule**, ready for immediate acquisition, with easy deployment plugged into Microsoft Outlook; proven, the underlying tech has been in use in Federal Government for 20 years.

Modernize Internal Signoffs, Social Docs



File Message

 Send Registered RMail Clipboard


 Send

RPostONE for Outlook

Track & Prove

- ☒ Marked as a Registered Email™ message
- ☐ Unmarked
- ☒ Active Tracker™ Protection

☐ **Encrypt - select primary experience**

- ☐ Transmission - auto-decrypts for recipient
- ☐ Message Level - decrypts with password
- 
- ☐ Email password to recipient

☐ **RDocs – Rights Protected Docs** [Send to RDocs](#)

- ☐ Track Views
- ☐ Track Readers
- ☐ Limit Readers [Set Expiration](#)

☐ **File Share - up to 1 GB** [Manage Files](#)

☐ **E-Sign - send for signature** [Send to RSign](#)

- ☐ E-Paper
- ☐ Smart Tags
- ☐ One-Click ☐ Sign in Sequence



☐ **SideNote®**

☐ **Disappearing Ink™**

☐ To ☐ Cc ☐ Bcc

Threat Intelligence

- ☒ AI Auto-Lock
- ☒ Eavesdropping
- ☒ Reply Hijack
- ☒ Lookalike Domain
- ☒ AI Recommends
- ☐ Redact & Mask Data

[Send](#) [Cancel](#)   [Less](#)

See the Unseen: See Criminals in Action

To

Cc

Bcc

Subject

RE: RPost // Form

From: zkhan@rpost.com

Reply-to: zkhan@rposts.com

Recipient	Domain Age	Notes
zkhan@rposts.com	7 days	Unsafe

Best

Zafar

Connect on LinkedIn

Zafar Khan

zkhan@RPost.com



**Made in California,
Served to the World.
Since 2000.**

