RPostONE™

Preempt Risk.
Protect Information.
Prove Resilience.

Executive brief for CIOs, CISOs and security leaders

Cybersecurity, Intelligent Content and Digital Workflows for Humans & AI

The enterprise boundary is no longer the security boundary.

RPostONE with RAPTOR™ AI protects communications, content, third parties, AI use and high-value digital transactions even in the places where modern attacks originate - beyond traditional endpoints.

PRE-Crime™ | Email Security | DLP | DSPM-Extended | Threat Intelligence | Insider Risk | Third-Party Risk | GRC

Extend security even beyond the gateway, beyond the endpoint and beyond the enterprise boundary.

EXECUTIVE THESIS

The Security Perimeter Has Moved

Enterprises have become adept at protecting infrastructure they control. But increasingly, the material risk appears elsewhere: a compromised supplier with cybercriminals conducing reconnaissance to identify targets of opportunity and attacking with hyper-contextual tactics, content shared externally with loss of control of access rights after share, AI hookup to email risking prompt injection triggering AI agent actions, a naïve insider or a third party using a free (shadow) or not-privacy-protecting AI leaking strategic information to become open source knowledge, a link that resolves to a high reputation IP address when passing through the inbound security gateways only to have the DNS routing for the link swapped to a malicious site after arriving into the inbox, an insider moving selected critical information into a personal repository for later (post-employment or unauthorized) access or leaking, or a threat actor quietly studying a transaction before launching the attack.

RPostONE combines critical tools that can be purchased all-in-one or in layers separately, and applies them to the communications, content and transactions where risk actually develops.

PREEMPT Cyber reconnaissance before an attack	**DEFEND** Email, identity and AI-era threats	**PROTECT** Data, documents and insider risk
HUNT Threat intelligence and third-party compromise	**GOVERN** Privacy, sovereignty, resilience and legal proof	**TRANSACT** Secure digital business workflows

This is not a rip-and-replace proposition.

RPostONE can serve as a core email security platform or add specialty layers around Microsoft 365, an existing secure email gateway, current DLP controls and established security operations. The strategy is simple: keep what already works and add the layers that address the gaps.

Analyst-aligned market context

Gartner's 2025 Email Security research evaluates core email protection, outbound security and integrated email security, and notes that buyers may need complementary or supplemental controls. RPost is included in both the Gartner 2025 Magic Quadrant™ for Email Security and Critical Capabilities for Email Security reports, among other analyst accolades.

ARCHITECTURE

Critical Cybersecurity Capabilities

RMail Email Security Platform with RAPTOR™ AI

A layered, modular platform combining inbound gateway controls, outbound DLP, post-delivery defense, secure communications, compliance proof and AI-era threat intelligence.

CORE PLATFORM	WHAT IT DOES	CIO/CISO OUTCOME
Inbound Protection	Blocks and evaluates spoofing, malware, suspicious senders, URLs and other inbound threats before delivery.	Reduce malicious content reaching users. RMail verifies sender reputation, authentication results, headers, links, attachments, spam and phishing patterns, and malware indicators before a message reaches the inbox.
Outbound DLP	Inspects content, attachments, destinations and policy conditions before messages leave the organization.	Reduce sensitive-data loss and misuse. RMail combines an advanced policy engine enhanced by AI classification of message content, attachment and recipients.
Secure Communications	Encrypts and controls sensitive email and file delivery beyond the enterprise.	Protect information outside systems you control. RMail's encryption and secure file share services adapt dynamically and provides complete control of sent sensitive content, wherever it resides.

Additive specialty layers

PRE-Crime™ - Threat intelligence, cyber counterintelligence and threat hunting focused on suspicious reconnaissance around legitimate business communications. Traditional detection and response focus on reacting only after the incident begins. PRE-Crime™, powered by RAPTOR™ AI, closes this gap. RAPTOR™ AI generates forensic interaction metadata from how emails, documents, and transaction content are accessed after delivery. It separates expected from unexpected interactions, distinguishes benign anomalies from malicious reconnaissance, and attributes malicious activity to specific people, email threads, or AI threat actors. This creates a new security signal that existing endpoint tools were never designed to generate.

Double DLP® - Human-error and leak preemption using recipient risk analysis, workflow pausing and post-send protection. With **Double DLP™** and **AI Auto-Lock**, protection extends beyond the initial send event, enabling post-delivery remediation when anomalies arise after content has left the enterprise. This is offensive cybersecurity: not simply detecting attacks after execution, but threat hunting and access denial of key business context attackers need, to succeed.

AI-Era Threat Defense & AI Observability - Prompt injection detection, AI-generated lure analysis, semantic classification and visibility into AI use through communications. RAPTOR AI adds communication context and data-protection routing. By combining AI-generated email detection with sender history, workflow context, and ICES semantic analysis, RAPTOR AI can detect fraud that broader AI governance programs do not inspect.

Zero-Day ICES™ - In-the-inbox defense for evasive phishing, BEC, identity anomalies and threats that activate after an email has been already delivered.

Registered Compliance - auditable evidence of delivery, content, timing, encryption and privacy controls. Registered Email™ is the original proof of delivery standard and court-accepted legal proof, extending beyond email to cover other common communication channels like SMS and WhatsApp.

Extended protection beyond email

- RDocs® - DSPM extension, AI classification, persistent document rights, sovereignty controls and AI-era leak protection.
- Insider Risk - malicious file movement and naive AI leakage.
- Third-Party Risk - behavioral indicators that can surface compromise between formal assessments.
- Impersonation Detection - sender identity, lookalikes, reply-path anomalies and contextual risk.
- Transaction Workflow Security - RSign™, RForms™, RDocs, Registered Email and RMail across forms, approvals, signatures and proof.

SPOTLIGHT

SPOTLIGHT SPECIALTY LAYER: PRE-Crime Cyber Counterintelligence

CYBER COUNTERINTELLIGENCE

See the Unseen. Un-Leak the Leak. Preempt the Attack.

Bottom Line

Entirely unique to RPost and easily additive to currently embedded Microsoft 365, Microsoft Purview, or any email security gateway is RAPTOR™ AI PRE-Crime™ Cyber Counterintelligence at the content layer -- a new capability for exposing suspicious leaks and leakers, identifying reusable adversary fingerprints, and remotely denying access before stolen context can be weaponized.

Most cybersecurity tools monitor what enters a network, executes on an endpoint, or triggers an alert inside a protected environment. RAPTOR watches what happens after authorized email, documents, file shares, and strategic content leave that environment and reach coalition partners, contractors, suppliers, advisers, and other third parties. That is the blind spot. It is also where the next attack may already be forming.

The New Threat: Context Is the Weapon

Adversaries increasingly avoid hardened primary targets and compromise less-protected third- and fourth-party accounts instead. From those trusted footholds, threat actors and rogue AI agents can silently read communications, map relationships, identify operational timing, and learn who is communicating with whom, about what, and when.

Generative AI transforms that stolen context into operational scale. It can produce highly credible impersonations, targeted social engineering, deepfake-enabled interactions, data-exfiltration campaigns, fraud, and mission compromise. This is the modern man-in-the-middle attack. The adversary may not intercept encrypted traffic. It may simply reside inside a trusted account, quietly studying legitimate content and waiting for the moment when context becomes leverage.

What's New - and Fundamentally Different

RAPTOR attaches to authorized outbound content flows and generates new forensic interaction data beyond the sender's endpoints. It requires no recipient software, participation, security action, or compliant behavior.

Each interaction can produce protocol-level signals about network source, infrastructure, device, application, geography, timing, access sequence, and behavior. RAPTOR's specialized AI agents analyze these signals to separate expected interaction from unexpected activity, then distinguish benign causes - such as security scanning or permitted circulation - —from possible malicious observation.

When suspicious activity emerges, additional agents expand the analysis across related messages, threads, matters, recipients, third parties, and millions of connected data points.

The result is something conventional defenses rarely provide -- new intelligence generated from the adversary's interaction with protected content outside the controlled perimeter. RAPTOR does not merely consume known threat indicators. It helps create previously unavailable intelligence. RAPTOR

does not hack back. It turns the adversary's interaction with authorized content into intelligence, attribution, and intervention.

Elegantly Easy Technical Hook-In

RAPTOR is designed lightweight, to add onto existing infrastructure without requiring new software or systems inside the network. For email and attachments, it can connect through a routing rule at the last-hop outbound gateway, APIs, and/or MCPs.

Three Cyber Counterintelligence Layers

Offensive counter-reconnaissance: RAPTOR quietly exposes adversaries eavesdropping on sensitive content and causes them to reveal elements of their infrastructure, operating environment, and behavioral patterns.

Defensive cyber counterintelligence: RAPTOR converts those observations into reusable fingerprints, then hunts for matches across otherwise benign-looking activity to identify additional exposed users, content, matters, and third parties.

Automated context denial: RAPTOR's Double DLP™ and AI Auto-Lock™ agents can remotely pause, restrict, or terminate access after a leak but before the content is viewed, further distributed, or weaponized.

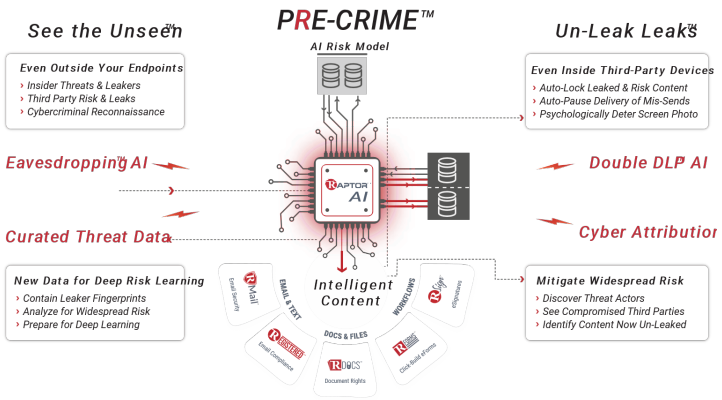
Why It Matters

RAPTOR does more than identify that a leak may exist. It can help determine: whether the exposed content was actually viewed; who or what interacted with it; which third party may be compromised; what infrastructure and behavior characterize the observer; whether the same fingerprint appears elsewhere; and whether access can still be stopped before reportable or operational impact.

This transforms static, questionnaire-based third-party risk into continuous operational intelligence. It also changes the defender's timeline. Instead of waiting for reconnaissance to become targeting, targeting to become impersonation, and impersonation to become mission impact, RAPTOR works to interrupt the sequence at its source: the adversary's acquisition of context.

Kill the Context, and You May Kill the Attack it was Going to Build.

The mission is clear: see what existing tools cannot see, expose the watcher, trace the pattern, un-leak the leak, and deny the adversary the intelligence needed to act. RAPTOR AI moves cybersecurity from POST-Crime response to PRE-Crime advantage.



SCENARIO-LED SECURITY

Incidents the Existing Stack Can Miss

Supply Chain / BEC Risk: The invoice was fraudulent. The attack started three months earlier.

PRE-Crime™ cyber offense

A trusted supplier has been compromised. The attacker does not rush. For weeks, they watch invoice formats, payment timing, approvers and account details through anonymized infrastructure. Then, on the day a large payment is due, Finance receives a familiar-looking invoice with subtly altered banking information. It matches the project, the amount, the timing and the language. The payment is made. The real supplier calls weeks later asking why it remains unpaid.

RPOST SOLUTION

RAPTOR AI PRE-Crime analyzes post-delivery interaction patterns, network and device anomalies, geography, timing and anonymization signals surrounding protected communications. When high-risk access appears, AI Auto-Lock™ can deny access to protected content before it is further weaponized.

CISO TAKEAWAY

Traditional defenses focus on the fraudulent message. RPost is designed to surface the adversary learning how to create it.

SECURITY DISCIPLINES: Preemptive Cybersecurity · Cyber Counterintelligence · External Threat Intelligence · BEC

Dynamic DNS Swap Detection: Link was safe when the gateway checked it.

Persistent post-delivery defense

At 9:04 PM, a cloud-sharing message passes inspection because its URL points to harmless content. At 11:00 PM the attacker changes the DNS destination, waiting for the link to be clicked by the user the following day. The exact same link now resolves to a Microsoft 365 credential-harvesting page. Nothing in the delivered email changed. The destination did.

RPOST SOLUTION

LinkWatch™ continues checking links after delivery for DNS swaps, redirect changes, rebinding and other changes in destination behavior.

CISO TAKEAWAY

A gateway verdict is a snapshot. Attackers operate on a timeline.

SECURITY DISCIPLINES: Email Security · Persistent URL Intelligence · Continuous Threat Monitoring · Zero Day

Leaks into Shadow AI: The employee is trying to be productive. The leak is still real.

AI-era naive insider risk

A product manager connects a free personal AI assistant to summarize daily email. A colleague sends a confidential three-year roadmap. The assistant automatically reads the email and attachment, extracting launch dates, acquisition plans, pricing strategy and competitive positioning into an unapproved external workflow. No hacker was involved. No warning appeared.

RPOST SOLUTION

RDocs applies persistent protection to sensitive files. Approved humans can be allowed to read while unapproved AI agents, automation tools or other access paths are restricted, whether the content is shared through email, Teams, SharePoint or other workflows.

CISO TAKEAWAY

AI leakage is often not an attack. It is a shortcut - and internal AI policy cannot govern every external recipient.

SECURITY DISCIPLINES DSPM · AI Security · Insider Risk · Data Protection · Shadow AI

SCENARIO-LED SECURITY

When “Normal” Behavior Becomes Material Risk

Insider Threat IP Theft: The departing employee steals only the documents that matter.

Malicious insider threat

A sales executive accepts a role with a competitor. They don't download the whole CRM. Monday: the top 200 accounts. Tuesday: the discount matrix. Wednesday: pipeline forecasts. Thursday: next year’s pricing strategy. Each transfer looks plausible. Together, they contain the company’s commercial playbook.

RPOST SOLUTION

RAPTOR AI classification identifies the sensitivity of the content being moved and applies persistent document controls. Double DLP can combine that classification with destination, recipient and policy context to pause or block suspicious outbound movement, or access to content can be revoked wherever it resides, even on the sales executive’s personal mailbox.

CISO TAKEAWAY

The important signal is not only whether a file moved somewhere it should not, but whether access is still permitted.

SECURITY DISCIPLINES: Insider Risk · DLP · DSPM · Data Protection

Third Party Risk: The vendor was green yesterday. Its mailbox was compromised this morning.

Real-time third-party compromise identification

A strategic supplier passed its annual security review. Its questionnaire is complete and its rating is strong. Months later, one executive mailbox is compromised. Within hours, an attacker begins watching an upcoming high-value payment. The vendor-risk dashboard still shows green. The actual risk has changed completely.

RPOST SOLUTION

RAPTOR AI evaluates changing external-recipient behavior, networks, devices, geography, anonymization and interaction patterns around sensitive communications.

CISO TAKEAWAY

Periodic assessment tells you whether a vendor was secure when you checked. RPost adds a behavioral signal for what may be happening now.

SECURITY DISCIPLINES: Third-Party Risk · External Threat Intelligence · GRC · Supply-Chain Security

Resilience: The Board does not ask what the policy said. It asks what happened.

GRC, resilience and evidentiary compliance

After a disputed transaction, the CISO and General Counsel need to answer: What exactly was sent? Was it encrypted? Who received it? When was it delivered? Which controls applied? The organization can produce policies and training records. Leadership wants evidence of the individual transaction.

RPOST SOLUTION

Registered Email™, Registered Encryption™, RMail and RDocs combine security controls with auditable evidence of content, delivery, timing, privacy controls and protected-document activity.

CISO TAKEAWAY

Security architecture shows what should happen. Evidentiary controls help prove what actually happened even if leaks or attacks begin beyond one’s endpoints.

SECURITY DISCIPLINES: GRC · Privacy · Cyber Resilience · Evidentiary Compliance

SCENARIO-LED SECURITY

From DSPM Visibility to Persistent Protection

Data Protection: AI classification to apply security intelligence selectively

A consulting firm may correctly secure project files in SharePoint, yet still need to send those files to lawyers, customers and contractors. One recipient should see the financial pages, another only the operating section, and a third should lose access in 30 days. The repository and access per document page can be perfectly governed while the document is no longer under repository control.

RDocs as a DSPM extension

RAPTOR AI can classify document sensitivity and turn that intelligence (whether using its native AI or BYOM for other AIs or Policy Engines) into controls such as approved readers, page-level access, geographic restrictions, expiration, remote kill, AI Auto-Lock and denied-access reporting. The value is not another label; it is the policy action that follows the label.

Discover → Classify → Understand Exposure → Protect → Monitor → Remediate

TRADITIONAL DSPM **RDOCS & RAPTOR AI EXTENSION**

Data exfiltration before the data is seen

A board document is mistakenly sent externally. Security discovers the error twenty minutes later. With RDocs and AI Auto-Lock, newly detected risk can block the content before it is displayed - potentially un-leaking the leak before exposure.

Sovereign data after sharing

A sensitive design is stored correctly in Germany, then accessed later from a restricted geography. Sovereignty is not only where data rests; it is also where protected information can be consumed.

Thirty-day engagement, permanent copies

A consulting engagement ends, but recipients may retain downloaded documents. RDocs can expire or revoke access to distributed copies rather than relying on recipients to remember to delete them.

SECURITY DISCIPLINES DSPM · AI Classification · Data Protection · Data Sovereignty · Insider Risk

AI-era edge cases: deepfake-enabled impersonation can make a synthetic candidate or executive appear authentic in a web meeting, while prompt injection can make a harmless-looking email contain instructions intended for an AI assistant. RPost extends monitoring and controls to both the communication and the AI workflow.

OUTCOME-DRIVEN METRICS

Measure What Matters

Security investment should ultimately be measured in risk reduced, exposure prevented, response accelerated and resilience demonstrated - not simply alert volume. Measure Security in Terms the Business Can Act On.

CIOs and CISOs are under increasing pressure to show that cybersecurity investment is improving business outcomes—not simply generating more alerts, policies, or tools.

RPost supports **outcome-driven metrics (ODMs)** that connect operational cybersecurity performance with measurable business value across the following key areas:

Why ODMs Matter

The objective is not simply to answer:

"How many threats did the product detect?"

The more valuable questions are:

Did we prevent a material loss?
Did we reduce sensitive-data exposure?
Did we identify third-party risk soon enough?
Did we shorten investigation time?
Can we prove controls operated when required?
Did we improve security without slowing the business?

RPost gives CIOs and CISOs a framework for measuring cybersecurity in terms of **risk reduced, exposure prevented, transactions protected, evidence produced, and operational effort saved**.

RPost offers customers to select modules in the RAPTOR AI dashboard to ease presentation of proof of value. Examples:

Preemptive Risk Reduction

- Number of suspicious reconnaissance events identified before fraud or compromise
- High-risk interactions within third-party environments surfaced before transaction impact
- Time from anomalous activity detection to investigation or intervention
- Number of potential payment-interceptions or BEC events preempted

Email Security Effectiveness

- Zero-day or evasive threats identified after gateway delivery
- Lookalike, impersonation, and BEC attempts detected
- Persistent-link risks identified after initial message inspection
- Reduction in malicious content reaching end users

Data Protection & DLP

- Sensitive messages paused before delivery
- Wrong/risky-recipient events prevented
- Sensitive documents protected after send

- Post-delivery access revoked before confidential content was viewed

Extended DSPM & Insider Risk

- Sensitive documents classified by risk level
- High-risk files moving outside approved business boundaries identified and controlled
- AI-related sensitive-content exposure events identified and prevented
- Documents protected subject to geographic, reader, or sovereignty restrictions
- Reduction in unprotected sensitive-data movement

Third-Party Risk

- External counterparties exhibiting new anomalous behavior identified
- Time from third-party behavioral change to security visibility
- Risk signals identified between formal vendor assessments
- High-value transactions with active third-party risk indicators protected

GRC, Privacy & Resilience

- Percentage of regulated communications with auditable encryption evidence
- Percentage of critical communications with delivery and content proof
- Time required to assemble evidence for audit, legal, or incident review
- Reduction in unresolved or unverifiable transaction events

Operational Efficiency

- Security capabilities consolidated into a common RPostONE platform
- Reduction in manual review through automated risk decisions
- Security workflows initiated automatically through policy, API, or MCP
- User friction avoided through transparent security controls

DEPLOYMENT

Keep What Already Works. Add the Layers That Are Missing.

RPost is designed to be additive to the enterprise architecture - without requiring a new endpoint agent simply to gain the specialty layers you need.

Microsoft 365 / Existing Email Platform

Your current collaboration and messaging environment remains in place.

↓

Existing Gateway / Last-Hop Routing

RPost can replace inbound or outbound gateway or simply add layers by hooking into the last-hop in your email flow.

↓

RPost Specialty Security Layers

PRE-Crime, Zero-Day ICES, Double DLP, Registered Compliance, AI-Era Threats and AI Observability, RDocs and Collaboration and Workflow Protection related modules.

↓

External Recipients / Third Parties / AI / Transactions

Security extends to the interactions and content that move beyond the enterprise endpoint.

Deployment options

- Email or gateway routing
- Microsoft Outlook / Microsoft 365 add-in
- API automation and MCP servers for AI-agent workflows
- Supported third-party applications and connectors

Why CIOs and CISOs care

RPost can add specialized visibility and control without forcing a replacement of Microsoft 365, the incumbent SEG, existing DLP investments or changes in user workflows. The deployment philosophy is operationally conservative even when the security capability is differentiated.

Beyond the gateway. Beyond the inbox. Beyond the endpoint. Beyond enterprise boundary.

PLATFORM SUMMARY

The RPost CISO View

RPost spans and extends established security disciplines without requiring the enterprise to collapse them into a single replacement platform.

PREEMPT:	PRE-Crime™ · Cyber Counterintelligence · External Threat Intelligence
DEFEND:	Email Security · Zero-Day ICES™ · Persistent Link Protection · AI-Era Threats and AI Observability
PROTECT:	DLP · DSPM · AI Classification · Insider Risk · Data Sovereignty · RDocs Intelligent Content
HUNT:	Threat Intelligence · Threat Hunting · Real-Time Third-Party Compromise Identification
GOVERN:	GRC · Privacy · Registered Compliance · Email Encryption · Cyber Resilience
TRANSACT:	RSign™ · RForms™ · Identity-Supported eSignature · Digital Transaction Workflows

RAPTOR™ AI is the intelligence layer across RPostONE

Analytical AI, machine learning, fuzzy logic, social graphing, semantic analysis and agentic orchestration are applied where they materially improve threat detection, classification, human-error preemption, cyber counterintelligence, document protection and workflow automation.

RPostONE™

AI-Infused Cybersecurity, Intelligent Content and Digital Workflows

Preempt risk. Protect information. Prove resilience.

Keep what already works. Add the layers that are missing.

Research references: Gartner, Magic Quadrant™ for Email Security (1 Dec 2025); Gartner, Critical Capabilities for Email Security (1 Dec 2025). RPost is listed among included vendors in both reports.

Appendix: Cyber Counterintelligence Customer Case Study

Cybercriminal Use of DarkAI to Identify Targets and Broker Leads to Specialized Threat Actors

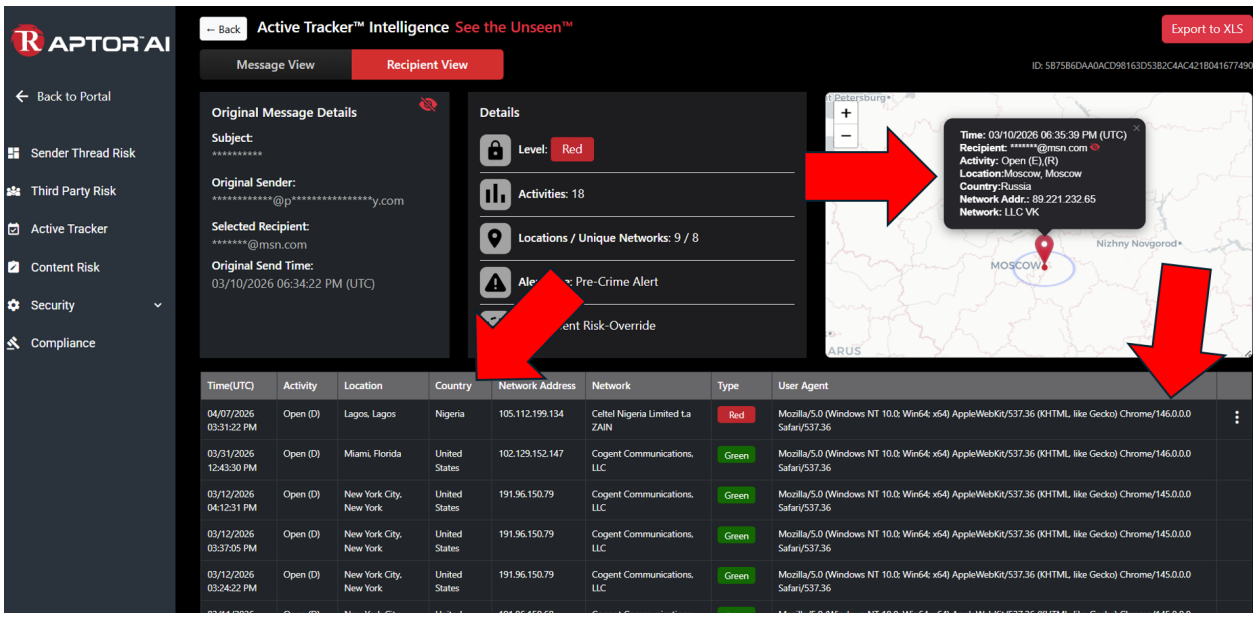
In this record (one selected email), we see that from the original send time of this email from the title insurance agent (transaction closer) to the buyer over an approximate 30-day period, RAPTOR™ AI generated 18 unique AI threat intelligence analyses involving approximately 200 unique AI agent actions, with activity clustering into three distinct operational phases.

1. Initial Reconnaissance Event (High Significance / Russian Origin)

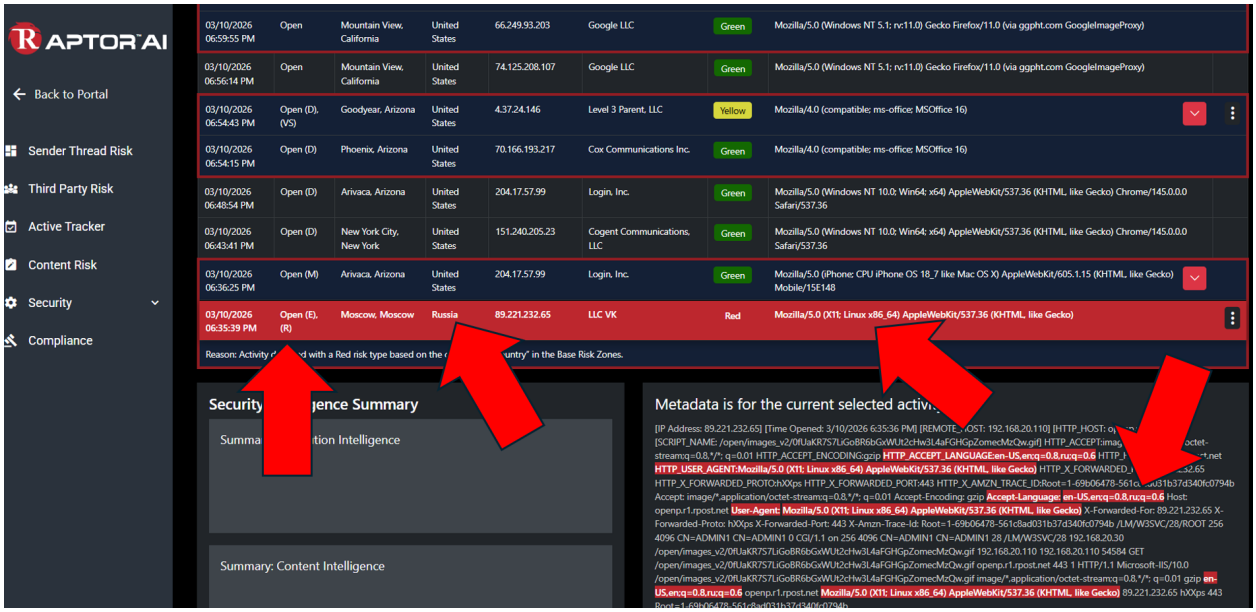
- Infrastructure: Moscow, Russia (LLC VK ASN)
- Device Profile: Linux / X11 browser
- Language Artifacts: English primary, Russian secondary (en-US,en;q=0.8,ru;q=0.6)
- Behavioral Indicators:
    - Direct access (not proxy-rendered)
    - No Outlook/consumer email referrer
    - Language blending consistent with non-native English operator

Assessment: This event represents the earliest non-benign interaction with the message and is highly indicative of automated reconnaissance operations on an application that was interacted with by a human which exposed the geolocation and browser fingerprint anomalies.

RPOST RAPTOR AI TRANSACTION ID: 5B75B6DAA0ACD98163D53B2C4AC421B041677490



[...]



2. Persistence & Monitoring Phase (Proxy / VPS / Masking Layer)

- Geolocation: Primarily New York (Cogent / VPS-style infrastructure)
- Behavior:
    - Repeated access over multiple days
    - Outlook Web referrers present
    - Consistent desktop Chrome fingerprints

Characteristics: Infrastructure consistent with commercial VPS or anonymization layers. Repetition suggests continued monitoring rather than one-time access. This phase reflects sustained visibility into the mailbox, likely via continued unauthorized access to the compromised account with automated monitoring via session/token persistence.

3. Late-Stage Access Event (Nigerian Origin / Operational Exposure)

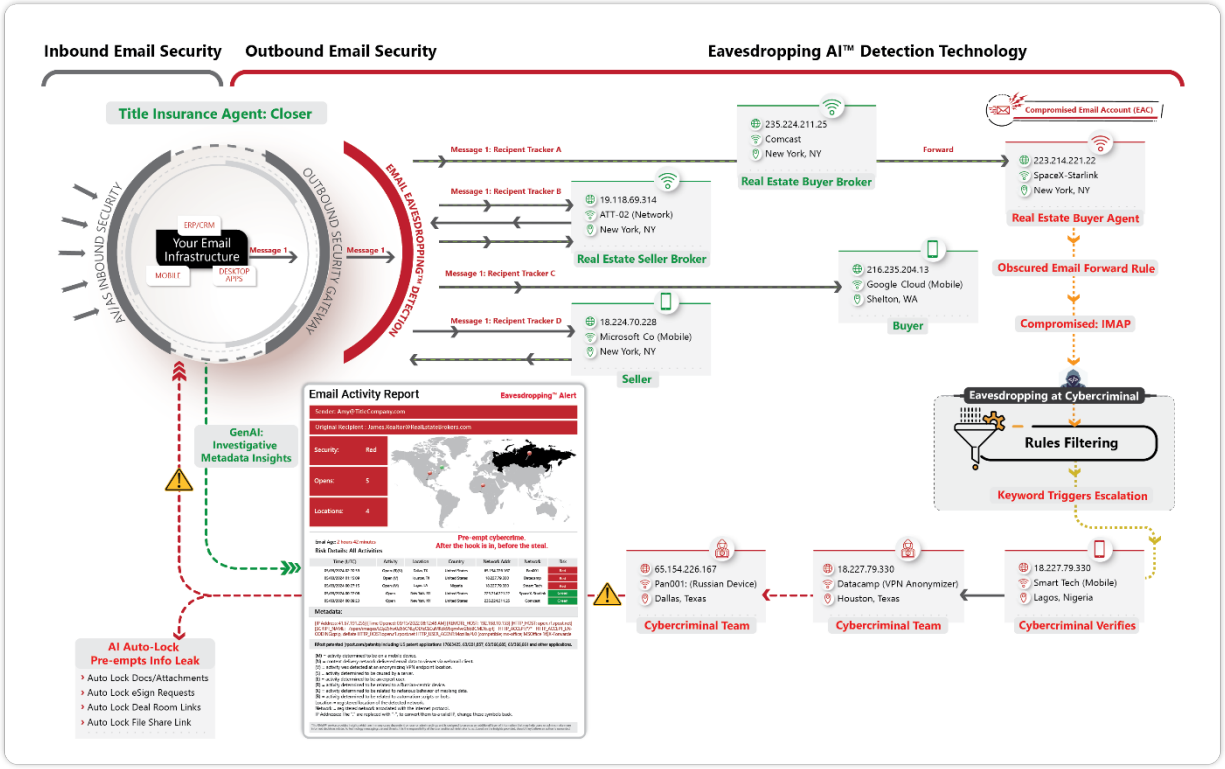
- Geolocation: Lagos, Nigeria
- Device Profile: Nearly identical to prior VPS access patterns

Key Observation: User-agent similarity to earlier New York infrastructure.

Assessment: This event is significant due to geographic divergence combined with technical similarity, indicating same toolset or session reused from a different location, transfer of access credentials/session to a second operator and operational security failure exposing true operator location.

This demonstrates the extent of cybercriminal use of DarkAI to Identify vulnerable targets then Broker those Leads to Specialized Threat Actors

EXAMPLE FLOW



Title Insurer Pre-Empts Cybercrime-in-Progress with RMail (rpost.com)
Outbound AI Security Stack – RMail

Observed Pattern: Multi-Actor, Multi-Stage BEC Ecosystem

1. **Target Identification Layer** (Likely Eastern European / Russian Nexus)

- Early detection of high-value escrow-related email content
- Manual inspection of message context
- Potential use of Keyword triggers (“escrow,” “wire,” “closing”) and mailbox auto-parsing tools

2. **Infrastructure Abstraction Layer** (Proxy / VPS Masking)

- Continued access routed through U.S.-based infrastructure
- Purpose likely includes:
  - Avoiding geo-based detection controls
  - Maintaining persistence without exposing origin
  - Creating false attribution signals

3. **Monetization / Execution Layer** (West African Nexus)

- Later access from Nigeria aligns with:
  - Known BEC operational hubs
  - Financial fraud execution (wire diversion, social engineering)
- Likely roles:
  - Victim engagement
  - Payment redirection
  - Money Mule local US bank account coordination and funds re-direction

Why Russia and Nigeria Access the Same Email?

Access Brokerage Model (Most Likely): Russian-based actor identifies and validates high-value transaction email. Access (credentials/session/token) is sold, leased, or shared. The Nigerian actor receives the lead notification with access for fraud execution phase.

Implication: This reflects an organized and specialized cybercrime nexus, where reconnaissance and monetization are decoupled.

Why Shared BEC Platform / Multi-Tenant Tooling?

Email account is ingested into a BEC-as-a-service platform. Multiple operators access the same mailbox through centralized dashboards and remote browser environments. Geographic variance reflects distributed user base of the platform. Criminal tooling is evolving toward SaaS-like environments enabling collaboration across regions.

Why Operational Handoff Following Target Qualification?

Each cybercriminal organization has a specialty. The initial actor determines that the transaction is lucrative and a wire opportunity exists. The target is escalated to a more specialized fraud team with regionally-aligned actors (e.g., English-speaking West African groups with a money mule network in the U.S.). This indicates tiered fraud workflows, similar to call center escalation models.

Was this a Cybercriminal Operational Security Failure (Critical Signal)?

Awareness of the Nigerian access may represent the threat actor forgetting to enable masking/proxy with direct login outside protected infrastructure. The near-matching user agents from the Nigerian and New York VPS instances suggest that the same toolset was reused without anonymization. These were likely subtle cybercriminal SecOps failures that RAPTOR™ AI exposed. **This provides rare visibility into true operator geography, otherwise hidden.**

Assessment: This activity is consistent with a globally distributed BEC ecosystem attributed to an international cybercriminal organization or loosely groups leveraging (1) **upstream infrastructure** (e.g., BulletProofLink-type phishing-as-a-service platforms), (2) **initial recon** industrialized by Eastern European/Russian cybercrime ecosystems with recon access maintained through anonymized infrastructure, (3) **fraud impersonation execution** performed by a separate West African nexus threat actor (e.g., Black Axe) with sector-related financial fraud specialization, and (4) **international money mule network** for the money flow into lookalike US bank accounts and the cash out flow relay to international banks. This reflects a mature cybercriminal economy characterized by division of labor, access commoditization, and cross-border collaboration.

Risk Implications: This case illustrates a critical evolution in BEC tradecraft. Threat actors are no longer operating in isolation. **Compromised email accounts themselves are becoming tradable assets**. Financial transaction emails are being discovered, monitored and transferred between actors before exploitation.

Particularly in **supply chain, investment management, consumer lending, law firm settlement, M&A transactions, and real estate transactions**, this creates extended dwell time risk, where adversaries may monitor communications for weeks before acting at the optimal moment (e.g., just before invoices are paid or a transaction is closing). The average recon dwell time is reported to be 292 days.

Bottom Line: Threat actors are evolving from single-operator fraud schemes to coordinated, multi-actor ecosystems. The presence in this data sample of both Russian reconnaissance access and Nigerian follow-on access within the same compromised email account strongly suggests a linked operational chain rather than coincidence.

Whether through access brokerage, shared platforms, or staged handoffs, the result is the same; a high-value financial transaction was quietly exposed to a distributed cybercriminal network preparing for potential wire fraud.

Detection Insight: This activity would likely evade traditional controls and not exposed but for RAPTOR™ AI by RPost because infrastructure appears benign (VPS, U.S.-based IPs), activity mimics legitimate email and email security scanner access patterns, and only temporal + geographic correlation + behavioral deviation reveals the threat.

The decisive signal is not a single indicator of compromise, but the relationship among multiple signals that the technology like RAPTOR is built to detect and act in time averting potential damage.

RPOSTONE™

---

www.RPost.com