RAPTOR™ AI
POWERED BY RPOST

RPost Booth
#765

CYBER COUNTERINTELLIGENCE

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

Bottom Line for Law Professionals

RPost's **RAPTOR™ AI** introduces **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 becomes threat actor intelligence.

Most cybersecurity tools monitor what enters the 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 clients, 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, human operators 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. For document share repositories and file-sharing platforms, it can integrate through APIs and MCPs.

Patented: US12506756B2; US12602506B2, more at www.RPost.com/patents

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

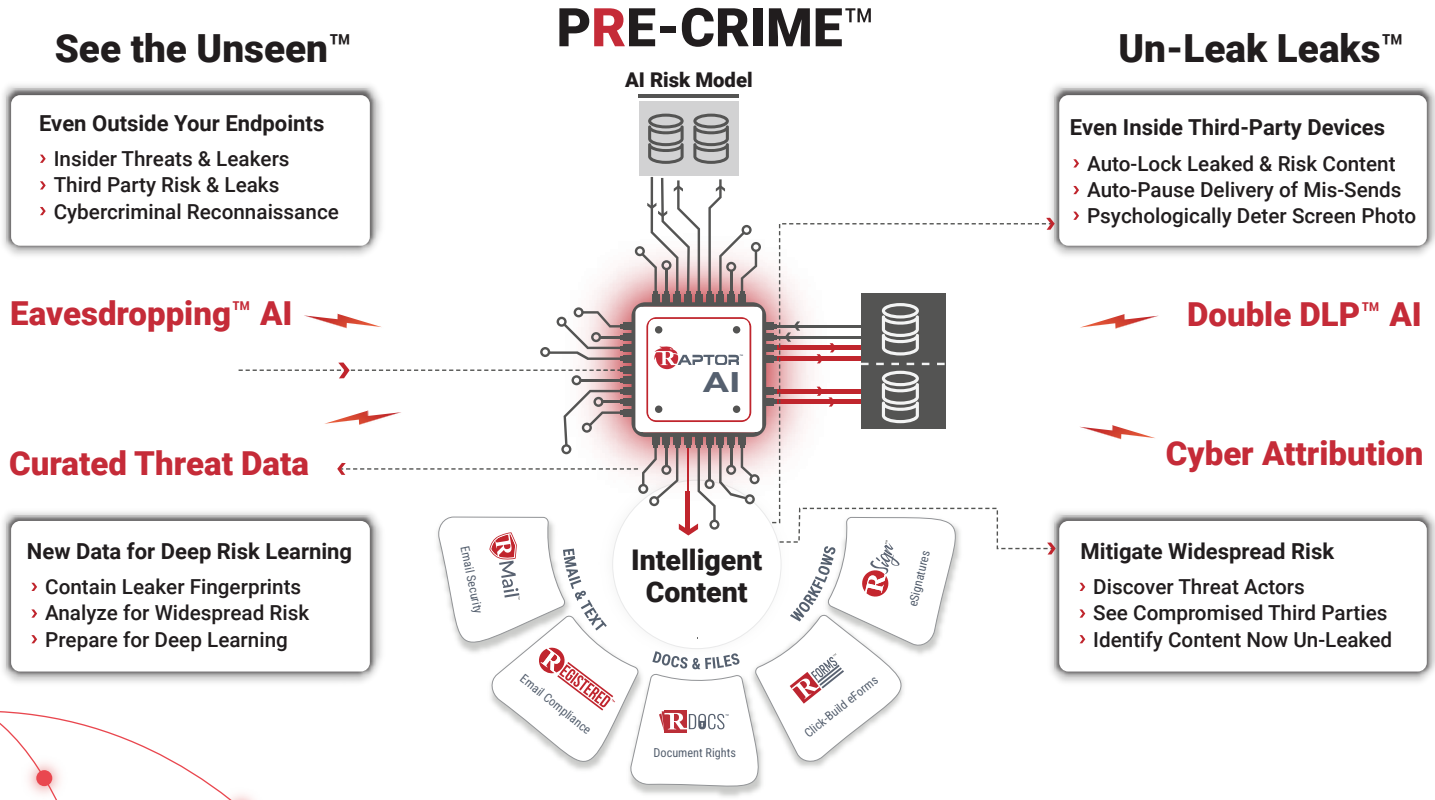
RAPTOR does more than identify that a leak may exist. It can help determine: whether the exposed content was actually viewed; who or what interacted with it; which third party may be compromised; what infrastructure and behavior characterize the observer; whether the same fingerprint appears elsewhere;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



Patented: US12506756B2; US12602506B2, more at www.RPost.com/patents