PRE-Crime™ Preemptive Security

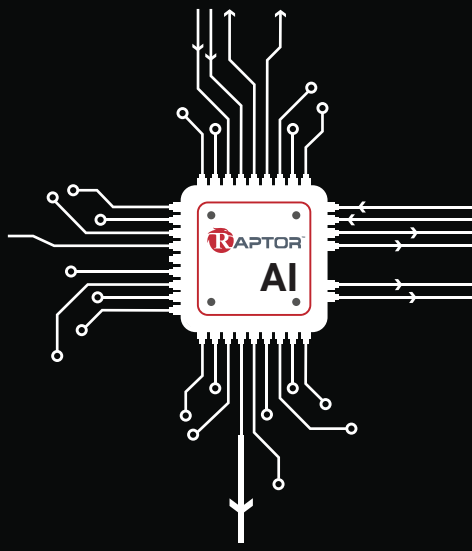
The Best **Defense** is a Strong **Offense.**
RPost is **Offensive** Security.

RPOST™
Cybersecurity Meets AI

- **Counter Third Party Risk & Leaks:** Remote Control Un-Leak Data at Compromised Third Parties
- **Counter Insider Threats & Leaks:** Deter Naïve and Malicious Leakers

PRE-Crime is Unlike Traditional Security Approaches. PRE-Crime™ offensive security adds cyber attribution and AI agents to preemptively un-leak leaks even outside of your endpoints. This is unlike traditional inbound/gateway security approaches; RPost is fundamentally different from today's status quo. In short, PRE-Crime provides what others can't and what others haven't even considered.

Context is King. Adversaries, threat actors and cybercriminal cabals use GenAI tools to conduct reconnaissance outside your secure internal network, at less resourced coalition partners, suppliers, and contractors. Their aim is to gather ***context*** about who is communicating with whom about what when. With GenAI impersonation programs plus ***context***, these threat actors can lure your third parties or internal team members in your ecosystem. With ***context*** plus GenAI, your adversaries can build at scale, hyper-contextual, hyper-targeted impersonation lures that often result in data exfiltration, fraud, ransomware, and mission compromise. Most tools only alert ***after*** an attack begins or ***inside*** internal systems. PRE-Crime powered up with **RAPTOR**™ AI preempts attacks by agentically, remotely, pre-emptively killing leaks wherever they maybe.



Live Cybercriminal Impersonation

Current Tactics Do Not Counter Today's Nefarious. **RAPTOR**™ AI combines analytical AI models with AI assistants and AI agents to expand your security perimeter ***beyond*** your network endpoints - without requiring third-party participation – to kill empowering ***context*** by un-leaking leaks automatically.

Zero Trust 2032 — Today. Achieve advanced state Zero Trust Pillars 4 (Data), 6 (Automation), and 7 (Visibility) now.

A New Attack Vector Being Exploited. Trust RPost, Agentically Un-Leak Leaks.
'See the Unseen', leaks inside AND outside of endpoints, at third parties. 'Un-leak Leaks' 24x7.

> **"Deny adversaries context they need. Hunt, un-leak, disrupt reconnaissance before an attack.**

www.RPost.com

RPost PRE-Crime™: Preemptive Cybersecurity for CISOs

RPost's PRE-Crime preemptive cybersecurity solution, powered by RPost proprietary **RAPTOR**™ AI, delivers a proactive, multi-layered approach to mitigate advanced phishing, business email compromise (BEC), and email account compromise (EAC). These threats, if left unchecked, can lead to significant financial loss, data exfiltration, reputational harm, and operational disruption.

Unlike traditional defensive reactive security tools, PRE-Crime provides **offensive** cybersecurity even hunting outside of your endpoints; identifying and preemptively neutralizing threats before they escalate. Here's how it works across five key phases.

The Five Phases of PRE-Crime™ to Preempt Cybercrime

1. Mass Metadata Collection Outside Endpoints

Gathers behavioral data from insider and external third-party interactions with emails and documents—both inside and outside your organization's endpoints.

2. AI-Powered Risk Analysis

Uses custom AI models—including natural language processing (NLP) and machine learning—to assess risk tied to insiders, third parties, and content itself.

3. Agentic Leak Remediation

Proactively kills compromised content—email messages or documents—based on detected risks, and provides evidence leaks were un-leaked, not seen, therefore mitigating reportable breach notices.

4. Threat Actor Reconnaissance Data Curated

Captures threat actor data breadcrumbs from both insider and external cybercriminal reconnaissance activities, even those occurring outside your network perimeter, and organizes for deep AI analysis.

5. Cyber Attribution Mapping

Attributes threat to threat actors—insiders or external attackers—and target people and content via AI curated data and proprietary LLM attribution methods. Forensically ID impersonators, cybercriminal cabals, and state-sponsored threat actors.

Real-World Impact for Security Teams

PRE-Crime can uncover and cure with AI:

- Cybercriminals reviewing content – even at third parties – in real-time and in account compromises
- GenAI powered impersonations (e.g., voice/video clones, lookalike domains, reply-hijack, multi-party)
- Insider leaks through screen captures that bypass traditional DLP

PRE-Crime hooks into existing email, email gateways, DLP, DMS, other applications.