



RPOSTONE™



RPOSTONE™ FOR LAWYERS

RAPTOR™ AI Layers for Legal Email, Content, Compliance, and Workflow Protection

Law firms and legal professionals work at the center of sensitive communications, privileged documents, client instructions, financial transactions, signatures, filings, negotiations, and deadlines. RPostONE for Lawyers brings together RPost's RAPTOR™ AI-powered email security, content protection, compliance proof, document control, eSignature, and secure file sharing capabilities in one modular platform that can be used inside Microsoft Outlook, Office, Exchange, email gateways, APIs, and MCP-connected AI workflows.

RPostONE can be deployed as a complete package or as selected modules, allowing firms to add the protections they need without forcing attorneys, staff, clients, or outside parties to change how they work.

Analyst Accolades



Layer 1: **RAPTOR™** AI Cybersecurity

Protect legal communications before, during, and after the attack path.

This layer helps law firms defend against phishing, impersonation, account compromise, wire fraud preparation, misdirected communications, data leakage, and suspicious third-party access to sensitive legal content. It is especially important for law professionals because cybercriminals target legal matters for their context: who is involved, what is being negotiated, what money is moving, and which documents carry value.

RMail® Edition - AI-Powered Core Email Security

RMail adds advanced email security, encryption, compliance, and content intelligence to help protect legal email without slowing down legal work.

Main features:

- AI-powered phishing and impersonation analysis
- Semantic analysis of email content, prompt injection, and intent
- URL risk detection and suspicious link analysis
- AI content classification for sensitive legal information
- Email encryption for privileged and confidential communications
- Policy-based protection for compliance-driven workflows
- Designed to work inside Microsoft Outlook and common email systems

Why it matters for law firms: email remains the primary channel for legal advice, document exchange, client instruction, and payment-related communication. RMail helps secure that channel while keeping the user experience simple.

PRE-Crime™ Edition - Cyber Counterintelligence Before the Strike

PRE-Crime hunts for signs that cybercriminals are studying legal communications, documents, and transaction workflows before launching fraud, impersonation, or data theft.

Main features:

- Detection of cybercriminal reconnaissance before the attack
- Visibility beyond firm endpoints into third-party content interactions
- Identification of suspicious access to emails, links, and documents
- Threat actor fingerprinting and pattern recognition
- Intelligence around compromised third parties, affiliates, or clients
- Pre-strike risk detection for wire fraud, impersonation, and data theft

Why it matters for law firms: attackers often compromise a related party first, then study matter context before acting. PRE-Crime helps firms detect the preparation phase before the fraudulent instruction or data theft attempt arrives.

Double DLP® Edition - AI Watcher and Content Auto-Locker

Double DLP helps prevent sensitive legal content from being sent to the wrong person, exposed after sending, misused at third parties, or ingested into unauthorized AI tools.

Main features:

- AI-assisted detection of misdirected emails and attachments
- Right-recipient checking before sensitive legal content is sent
- Auto-locking of exposed or stale shared content
- Protection against impersonation-driven sending mistakes
- Controls to reduce unauthorized AI ingestion of sensitive documents
- Post-send protection even when content has left the firm
- Leak reduction for compromised third-party environments

Why it matters for law firms: legal risk often comes from human error, not just hackers. Double DLP helps prevent accidental disclosure, privilege exposure, and sensitive document leakage after content is already in motion.

Zero-Day ICES™ Edition - Continuous Inbox Defense

Zero-Day ICES continuously analyzes inbox content to detect advanced threats that may pass through traditional inbound defenses.

Main features:

- Real-time analysis of messages already in the inbox
- Detection of hyper-contextual phishing
- Lookalike domain and aged-domain risk detection
- DNS-swapping and post-delivery link-change detection
- Reply-chain and impersonation risk analysis
- Continuous monitoring for threats that emerge after delivery

Why it matters for law firms: sophisticated attacks often look legitimate because they borrow real context from legal matters. Zero-Day ICES helps identify threats that become dangerous after they arrive or after the attacker changes tactics.

Layer 2: **RAPTOR™** AI Governance, Risk, and Compliance

Prove delivery, preserve records, and control sensitive legal content wherever it goes.

This layer helps law firms create stronger records of delivery, privacy compliance, and content control. It is especially important for legal professionals because proving who sent what, when, to whom, and with what protections can matter as much as the communication itself.

Registered™ Edition - Proof of Legal Delivery and Encryption Compliance

Registered Email™ returns a Registered Receipt™ that can prove time, content, and delivery without requiring recipient action.

Main features:

- Registered Receipt™ proof of time, content, and delivery
- Court-accepted proof record for legal notices and communications
- No recipient registration or portal action required for proof
- Replacement for many certified mail or confirmed-delivery workflows
- Registered Encryption™ privacy audit record, proof of encryption level at each hop
- Records that support compliance, dispute resolution, and legal defensibility

Why it matters for law firms: lawyers often need to prove that a notice, document, instruction, or communication was sent and delivered. Registered Email services give firms an electronic proof record without adding friction for clients or recipients.

RDocs® Edition - Document Rights and Remote Control

RDocs gives content owners control over sensitive documents after they are shared, including access, printing, screen capture, viewing, and document kill.

Main features:

- Control access to documents after sending
- Page-level and viewer-level permissions
- Restrict printing, screen capture, and forwarding
- Kill or expire obsolete documents wherever they reside
- Auto-lock viewing inside compromised or suspicious environments
- Identify potential leakers and unusual access behavior
- Protect sensitive PDFs, spreadsheets, deal documents, and legal work product

Why it matters for law firms: once a legal document leaves the firm, traditional control is often lost. RDocs helps preserve control over privileged, confidential, draft, and high-value documents even after they move outside the firm.

Layer 3: **RAPTOR™** AI Secure Workflow Automation

Make legal transactions faster while keeping security, proof, and control built in.

This layer helps law firms streamline eSignatures, secure file sharing, data room activity, and client-facing workflows while preserving security and auditability. It is especially important because firms are under pressure to move faster without increasing risk.

RSign® Edition - Secure eSignature and Digital Transaction Management

RSign adds a complete eSignature platform for legal approvals, client documents, engagement letters, authorizations, forms, and transaction workflows, with elegant integrations into iManage, NetDocuments, Teams, Office 365, Outlook, Salesforce, API/MCPs, and more

Main features:

- Full electronic signature workflow platform
- Authentication, identity, and signer controls
- Secure document routing and approval workflows
- Templates for repeatable legal processes
- Audit trails and transaction records
- Designed for legal, compliance, and high-assurance workflows
- Recognized by analysts as a world-leading eSignature solution

Why it matters for law firms: eSignature is no longer just convenience. Legal teams need signing workflows that are fast, defensible, secure, and easy for clients and counterparties to complete.

FileShare Edition - Secure Large File Sharing and Data Room Protection

FileShare enables secure large file transfers, controlled sharing, data room protections, and post-share access management.

Main features:

- Secure large file sharing up to 1GB per transmission
- Data room-style protections for sensitive legal content
- Post-share access controls, ability to kill or expire shared files
- Auto-lock if a link is accessed in anomalous ways
- Secure sharing for clients, experts, opposing counsel, and third parties
- Protection for large evidence files, deal rooms, closing packages, and discovery materials

Why it matters for law firms: legal work often requires sharing large, sensitive files with people outside the firm. FileShare helps make that process simple, controlled, and safer than ordinary attachments or unmanaged links.

Why RPostONE for Lawyers

RPostONE for Lawyers is designed for the way law firms actually work. It protects email, documents, signatures, file sharing, legal notices, privileged content, and third-party interactions without requiring a patchwork of disconnected tools.

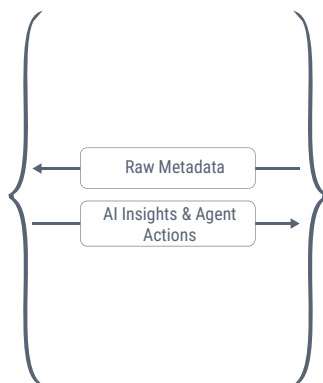
Firms can use RPostONE as a complete platform or add individual modules where risk is highest. The result is a practical legal technology layer for AI-era cybersecurity, compliance, privacy, proof, document control, and secure workflow automation.

RPostONE helps legal professionals:

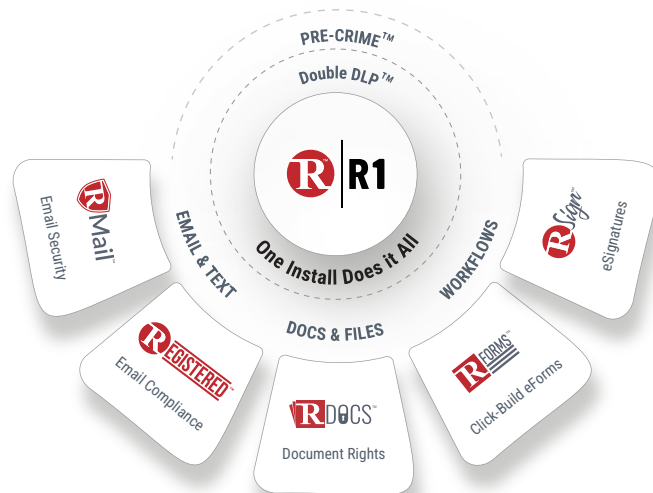
- Protect privileged and confidential communications
- Pre-empt wire fraud, impersonation, and third-party reconnaissance
- Reduce mis-sends and sensitive document leakage
- Prove legal delivery and encryption compliance
- Control documents after they leave the firm
- Secure eSignature and client workflows
- Share large files and data room content safely
- Use AI-era productivity tools with stronger safeguards

RPostONE for Lawyers: secure legal work in motion -- email, documents, signatures, files, proof, and protection, all in one.

INTELLIGENCE



CONTENT + SECURITY



ABOUT RPOST

RPost is PRE-Crime AI resilience. RPost helps CIOs, CISOs, and GRC leaders extend cyber resilience beyond traditional email security, shifting from recovery after disruption to preemption before impact. In an AI-vs.-AI world, reactive defenses are no longer enough. Powered by **RAPTOR™ AI**, **RPostONE™** adds a preemptive intelligence layer that helps spot cybercriminal reconnaissance even beyond endpoints, hunt for third-party risk, and protect exposed content before fraud, business email compromise, impersonations, data loss, or disruption strikes.

RPostONE brings AI-era threat defense and observability, integrated email security, data protection, compliance, and eSignature workflows into one platform. Designed to extend common email gateways and applications without adding complexity, RPost complements existing security stacks by adding visibility and controls where conventional tools often stop - after content leaves the organization, enters third-parties, or becomes part of a high-value transaction. Handcrafted in California and named a **Leader, Visionary, and Pioneer by analysts** including Gartner Research, Aragon Research, and IDC, RPost has served customers the world over for more than a decade. RPost is PRE-Crime™ AI resilience.