



Whitepaper Document Security

Track Readers. Kill Documents.
Control Content Even After the Send.

RPostDocs.io

Contents

RDocs™ by RPost® Document Security.....	3
The Digital Rights Management LandScape.....	3
Traditional Approaches to Enterprise Digital Rights Management for Documents.....	5
The New Fourth: Ubiquitous Access.....	7
The Dusk of PDF – Portable Document Format.....	7
The Dawn of RPD™ – Rights Protected Document™	8
RDocs™ Service Acts as the Conversion Engine to Generate RPD Files.....	9
Access Controls.....	10
Content Protection: Who, What and When.....	11
Location, Location, Location.....	11
Social Documents, Collaboration Re-Invented.....	11
Maintaining Control Post-Distribution.....	13
AI-Infused File-Lock: Automatic Cybersecurity”	13
Goodbye One-Size-Fits-All, Hello Tailor-Made Security.....	14
Track Views: Level 1 Security.....	14
Track Readers: Level 2 Security.....	15
Restrict Readers: Level 3 Security.....	17
Use Cases.....	17
Legal Bliss: A Deal Room Without the Room.....	17
Enhanced Governance and Compliance.....	18
Targeted Marketing on Steroids.....	19
Signoff Workflows Simplified.....	20
Example Use Cases.....	20
Conclusion.....	22
About RPost.....	23
FAQs.....	24

RDocs™ by RPost®

This whitepaper examines RPost's revolutionary approach to Digital Rights Management for documents that honors its lifelong commitment to feature-rich, affordable security-centric software services that are intuitive and easy to use for all parties involved.

RPost thrives on being artisans and experts in everything we do: secure and certified email encryption for privacy and compliance; e-signatures and web forms to ease digitization of workflows; e-delivery tracking to prove important communications; managed file transfer to simplify secure sharing of large documents and sets of files; document-level digital rights management to empower control of document access even after transmission; and AI-infused apps to prevent data leaks by minimizing human e-security errors.

RDocs™ technology is therefore a natural continuum of our mission: to help our customers worldwide communicate and transact electronically in a secure, compliant, and productive manner and to continuously innovate to support our customers' evolving needs.

This is why more than 25 million users have enjoyed RPost software services for two decades in 193 countries. Those software services, in addition to RDocs™ Document Security, include RMail® email security, Registered™ ecompliance, RSign® electronic signatures, and RForms™ click-build e-forms.

The Digital Rights Management Landscape

There is a category of **information rights management** or **digital rights management** software applications that are designed to add power to track and manage access to files after they have been transmitted onward, such that they can be entirely controlled, revoked, unsent, or expired by the file originator.

This technology has become ubiquitous within the online entertainment industry to protect copyrights related to music and video file intellectual property. This technology enables, for example, consumer-centric online video “renting” where the video may be streamed or downloaded by an end user and expired after a set period of time. Important to note: these videos or music files require compatible software by the viewer to play – and thus for the copyright enforcer to be able to revoke or expire access.



As enterprise technology has been incorporating trends from the consumer landscape, and especially with the outburst of the Covid-19 pandemic accelerating remote work everywhere, the business world has witnessed an unparalleled demand to distribute documents outside of the corporate firewall (to home offices, for example). And so, the ability to share digital files securely, protect sensitive information even after the share and control who can access what, where, and when, has become a general necessity.

Further, with the changed work environment, there has been a demand for more work with limited human resources. This has increased the risk of human e-security errors that often lead to sensitive information being accidentally distributed to the wrong recipients. In addition, sophisticated social engineered cyberattacks like impostor lures and Business Email Compromise are now more widespread than ever. Thus, today there is a greater need to control access to a document after the send – to “unsend” -- in case a sensitive attachment to an email is misaddressed (accidentally or through a cyberthief lure).

With relation to “unsending” documents, the recently released functionality by Apple that allows users to, precisely, “unsend” messages is of utmost relevancy in this market. Although Apple did not invent the functionality (avant-garde consumer apps like Telegram released it years ago, and were followed by Meta’s Whatsapp, Facebook Messenger and Instagram Messenger), it is no secret that Apple’s go-to-market strategy often relies on releasing functionalities only after they have been thoroughly tested by other companies, and once there is high demand for them in the mass audience, as opposed to only tech-savvy early adopters. With this in mind, the

fact that the “unsend” functionality has now been released for iPhone users is very telling about

the **maturity of the mass consumer’s concern about the future life of the content generated by them.** Technology-wise, text messages are traditionally stored in centralized servers, and as such, it could be argued the capability to “unsend” has been there all along, although only recently it has been made available at the UI level for end-users. Differently, in Digital Rights Management world, storing content in a centralized location is hardly recommendable as it would pose severe risks for compliance with GDPR and other data privacy laws and regulations. In this respect, RDocs™ technology is truly groundbreaking as it allows to revoke access to a document that has already been downloaded and stored in the recipient’s local device.

Lastly, tracking popularity of a music or video shares/streams after distribution, or tracking and cataloging who is viewing what when, empowers content originators or distributors with insights that they can use to further market, re-target viewers, or otherwise monetize. This same power can be provided to document originators through the use of digital rights management technologies for documents. Following iPhone’s release of consumer data protection features (“Ask App Not to Track”), the ability for companies to gain insight into their consumers’ online behavior has been severely affected. Meta alone is expected to lose ten billion US Dollars, and similar figures are reported for Alphabet, Snap and Twitter. This new scenario adds another layer of relevancy for services like RDocs™ technology that allow for capturing consumer interest for marketing efforts.

Traditional Approaches to Enterprise Digital Rights Management for Documents

There are three traditional types of information rights management or digital rights management software employed in the market for documents, and now a new unique fourth. The three traditional systems have been commercialized within categories that we refer to as (1) Same Licensing Plan, (2) Install App, and (3) Centralized Storage.

1. Same Licensing Plan

“Same Licensing Plan” refers to those digital rights management software applications where viewers need to use not only the same software as the file originator, but also have the proper licensed access to the software in order to view the rights protected document, and sometimes be nested inside the same organizational structure. An example of digital rights management software that requires the intended viewer to have the same software and the proper licensed access level is Microsoft’s Azure Information Rights Management software.

Microsoft IRM operates under a specific constraint where both document owners and readers must subscribe to the same licensing plan. While this feature upholds stringent security within an organization, it becomes less practical for scenarios involving external collaborators. This limitation highlights a significant barrier when organizations aim to maintain high levels of document security in diverse collaboration environments.

Another major shortcoming of these systems is that a vast number of them often impose software installations and premium licensing costs on the viewer. As such, all originators and viewers need to be in a software environment where there is a central IT organization managing software licensing with the proper license structures per user. While this may be practical for some companies, for many it is not. Further, when communicating documents to external parties outside of the corporate network, the originator has the added complexity of not knowing which of their recipients might have the proper software and licensing plan to access.

Determining which viewers have what software versions and who should be billed for the cost of upgrading to the proper licensing plans for access to view is a scenario that is even more untenable if opting to transmit to external parties out of the control of the originator’s organization.

2. Install App

“Install App” refers to solutions that require viewers to install a proprietary app – also called “companion software” -- to access shared documents.

A major shortcoming of “Install App” companion software systems is that viewers must learn how to use obscure third-party software to access the files. This scenario is even more untenable if the intended viewer is in an organization that restricts unvetted downloads of software to company devices, which is often the case in professionally managed IT organizations.

3. Centralized Storage

“Centralized Storage” refers to applications intended to store documents in a shared, access-controlled repository; with those documents viewable in that repository after a designated viewer creates an account and logs in.

A major shortcoming of these systems is that they require viewers to create an account, which may cost the file originator extra platform access “per user” fees. In addition, “Centralized Storage” applications often do not provide protection against unwanted downloads or do not provide visibility as to what happens to the documents if downloaded or after further transmitted, and there is no mechanism to track sharers of screen captures or printed versions.

Furthermore, with these systems, the Originator may need to ensure that the particular rights-controlled files are in a separate isolated storage directory from other documents to ensure the intended viewers do not have access to view unintended documents - a scenario that is even more untenable if the intended viewer is viewing documents from multiple different senders or associated with multiple different projects and/or the Originator is managing multiple types of documents intended for a variety of viewer types.

These systems also challenge senders to keep track of who has access to what folder and with which documents, where an error can cause the Originator to fall out of compliance or fact of storage of the documents may be forgotten (left online) and cause future potential embarrassment or ongoing storage costs.

A crucial point to consider in the use of link share features is the necessity of storing corporate data on third-party platforms. This requirement often poses significant challenges for organizations, as many have policies restricting the use of external data storage services. Furthermore, storing sensitive corporate information on third-party platforms can lead to potential compliance issues, making it a less viable option for businesses that prioritize data sovereignty and internal data governance policies.

The New Fourth: Ubiquitous Access.

The fourth approach – a new age for digital rights management for documents -- we call “Ubiquitous Access”. RDocs™ Document Security by RPost offers the only “Ubiquitous Access” digital rights management system for documents in the market. It’s patented and patent pending technology solves challenges of the traditional approaches by allowing organizations to share documents securely, controlling every aspect of the who, what and where even after the share. RDocs™ technology

- (1) does not require any software or special licensing for the viewer,
- (2) does not require any special companion software for the recipient, and
- (3) is a decentralized model – providing for all of the controls of, for example a “data room” but with no need to have centralized storage (which is a significant advantage for compliance with data privacy regulations).



RDocs™ technology is able to do all of this and more, thanks to its home grown, patent pending **Rights Protected Document™** files, also referred to as an **RPD™** files.

The Dusk of PDF – Portable Document Format

For years, businesspeople converted documents into PDF files, mainly with the intention to signal that the document was in final form, not intended to be editable, with its formatting and content integrity preserved. For many, PDF file meant un-editable, protected, and formal.

With today’s ubiquity of PDF editing and other software tools, PDF files have lost the public’s notion that it is a protected un-editable format.

In addition, PDF files historically afforded many advanced controls that could be programmed into the PDF file with Javascript, but which require the viewer to use PDF “reader” software – special companion software for the reader/viewer. In recent years, PDF “viewer” technology has become ubiquitously built into web browsers, and as such, a generation of computer users stopped installing PDF “reader” special companion software. As a result, today there is low level of adoption of PDF “reader” companion

software, a trend that is expected to continue in the coming years. As such, senders can no longer count on people that receive PDF files to have the right companion software to make the advanced PDF programmable behaviors function. Not knowing if the viewer has the proper experience makes reliance on these unworkable when communicating to external parties.

Most of what has been traditionally distributed as PDF files – whether manually or with output management or document builder tools - would be better served to be sent as RPD files. Why? Simply put, RPD files visually look the same to a viewer as PDF files opened in a web browser, yet RPD files build in the protections that many believe are native to PDF files but are not really available to PDF files.

While PDF files allow for some level of protection, such as limiting copying, printing or requiring a password to access (all of which are often defeated with no traceability as to, if defeated), once shared, the document is out of the control of the originator. This poses severe limitations for PDF files in the case that a document is accidentally misaddressed, misdirected, distributed without authorization, or if the originator would simply like to end availability.

The Dawn of RPD™ – Rights Protected Document™

RDocs™ technology overcomes the above-mentioned challenges by use of its inventive RPD™ file construct where security and controls that the file originator prescribes are built into and are self-contained inside the RPD file itself; which displays to readers as an .HTML file, and can be saved and stored just like any file, and opened in any browser or .HTML file viewer.

There are a number of benefits to RPD files for both document originator and viewer:

- Viewers can access the shared content without downloading or installing special companion software or plug-ins, and without creating an account or incurring added licensing costs
- Originators can at any time revoke access temporarily or permanently, kill a document entirely even after delivery, including all traces of the transaction.
- Documents are delivered directly to each recipient – there is no storage of documents by a third-party, which reduces compliance and data loss risks.
- Originators receive real-time insights as to who is viewing what document, when and where; with optional tallies of reader sentiment or feedback related to the content. These are document-level insights (vs. email delivery and opening or link click insights).
- Originators may choose to protect the content in the document with document-level security, which persists while inside the recipient's email inbox, and persists regardless of whether an email or file transmission is secure.

Further, there is an entire industry of Enterprise Output Management (EOM) software that deals with the organization, formatting, management and distribution of data that is created by enterprise applications like banking information systems, insurance information systems, ERP (Enterprise Resource Planning systems), CRM (customer relationship management), document builders, PDF-generation, document scanning, document electronic faxing, retail systems and many others.

These systems construct a file from inputs and often prepare that file as a document compiled in PDF format for storage in a web system, transmission by API or transmission by email.

In the early days of output management systems, these files would become images of a document in a TIFF format which is a static format. Then PDF files became the standard, which includes the ability to apply some basic static controls to the document (like password protecting).

RDocs™ document security, with its RPD file, provides a new output file type option for output management software. This marks the dawn of a new era -- of powerful security, access control, viewer insights, and document-level interactivity that is tied to output management systems.

The enterprise output management systems, as they are compiling the document from various data sources, can generate the output file as an RPD file type (vs. a PDF file type) with the controls information required for that file as prescribed by the situation. The result is a generated RPD file returned into the output management system and dropped into whatever file repository or transmission process normally occurs for storage and/or transmission to a recipient.

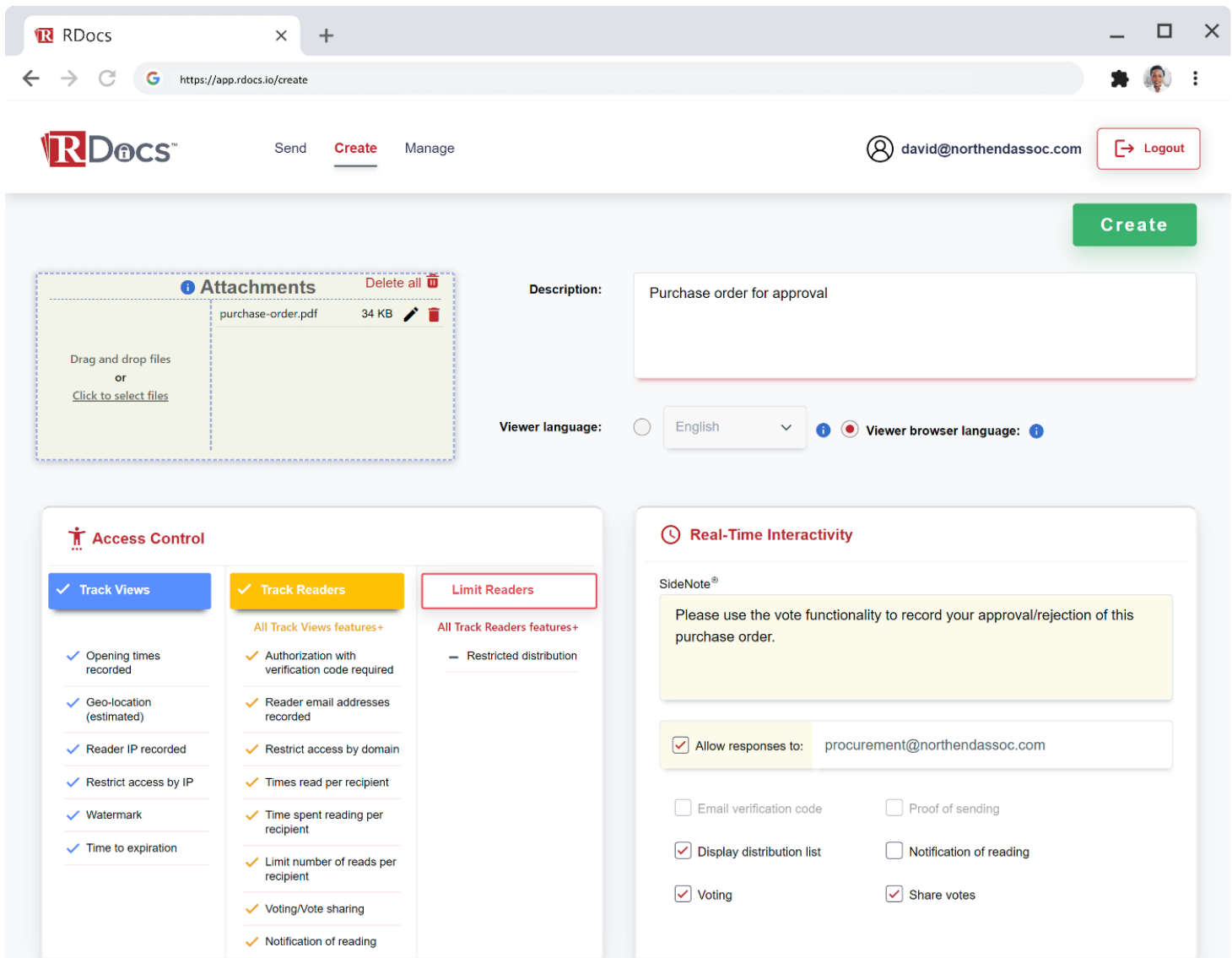
Since any document, presentation or PDF can be converted into an RPD file with a few clicks or automatically, and to a viewer the user experience is the same as viewing a PDF, one would be hard pressed to think of a situation where there would be effort to convert a high value document into a PDF file and not want to have the tracking, visibility, access and other controls, or interactivity afforded by an RPD file.

RDocs™ Service Acts as the Conversion Engine to Generate RPD Files

The RDocs™ service empowers users to convert any document or presentation file (e.g., .DOC, .PPT, .PDF) into an RPD file. It additionally permits the document originator to tailor the controls associated with the RPD file.

From a user perspective, there are two roles: file originator and file viewer. Controls are set up by the file originator and are imposed on the file viewer.

The originator can use a web user interface to set their default controls or may set controls on a per message basis. The originator may opt to (a) send the file attached to a message with the indication of which controls to apply to the file, and have the file uploaded or attached to an email message, and transformed into an RPD file en route to the recipient (viewer); or (b) submit the file to be converted with the indication of which controls to apply to the file, and have the file returned (downloaded) to the originator transformed into an RPD file for later sharing. These two user experiences may be built into apps, output management systems, or web user experiences using API connections to the RDocs™ servers.



The screenshot shows the RDocs web application interface. At the top, there's a navigation bar with the RDocs logo, 'Send', 'Create' (highlighted), and 'Manage' buttons. A user profile for 'david@northendassoc.com' and a 'Logout' button are on the right. A green 'Create' button is in the top right corner.

The main content area is divided into several sections:

- Attachments:** A dashed box containing a file named 'purchase-order.pdf' (34 KB) with a 'Delete all' button. Below it, instructions say 'Drag and drop files or Click to select files'.
- Description:** A text input field containing 'Purchase order for approval'.
- Viewer language:** A dropdown menu set to 'English'.
- Viewer browser language:** A button with an information icon.
- Access Control:** A section with three tabs: 'Track Views' (selected), 'Track Readers', and 'Limit Readers'.
 - Track Views:** Includes checkboxes for 'Opening times recorded', 'Geo-location (estimated)', 'Reader IP recorded', 'Restrict access by IP', 'Watermark', and 'Time to expiration'.
 - Track Readers:** Includes checkboxes for 'Authorization with verification code required', 'Reader email addresses recorded', 'Restrict access by domain', 'Times read per recipient', 'Time spent reading per recipient', 'Limit number of reads per recipient', 'Voting/Vote sharing', and 'Notification of reading'.
 - Limit Readers:** Includes a checkbox for 'Restricted distribution'.
- Real-Time Interactivity:** A section with a 'SideNote®' box containing the text 'Please use the vote functionality to record your approval/rejection of this purchase order.' Below this, there are checkboxes for 'Allow responses to:' (set to 'procurement@northendassoc.com'), 'Email verification code', 'Proof of sending', 'Display distribution list', 'Notification of reading', 'Voting', and 'Share votes'.

The controls that the originator may apply to the file are broadly grouped as follows:

Access Controls

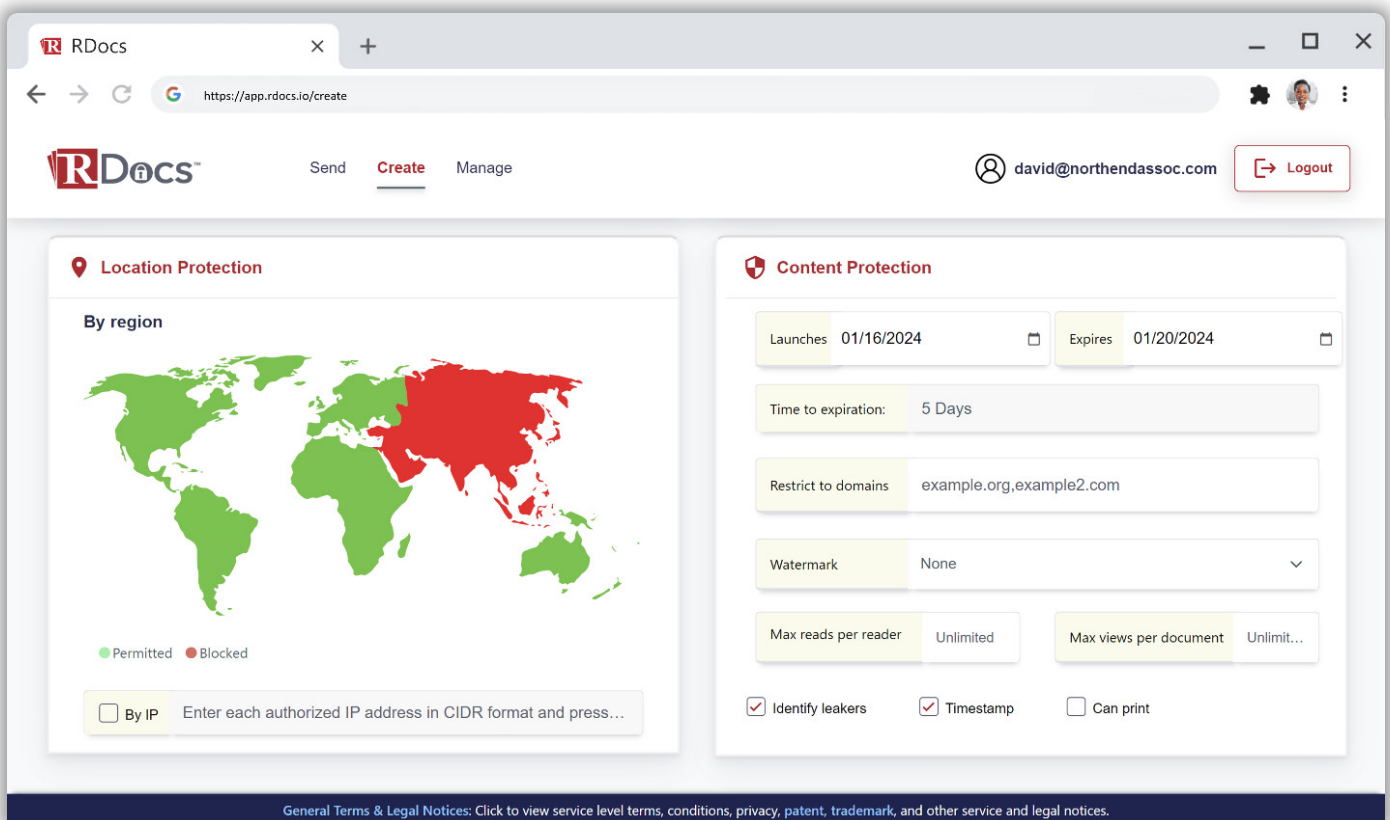
RDocs™ technology converts any presentation or document into a Rights Protected Document (RPD™) file, which empowers the sender with insights and provides peace-of-mind with security. Depending on the level of access controls, the sender can track popularity of a document, track specific reader activity, or restrict access to certain designated viewers – all with no companion software download or logins for readers.

Content Protection: Who, What and When

Senders can make a document self-destruct on a timer, on a specific date, after a number of views, or at the click of a button at the originator – for example, to “unsend” a misaddressed sensitive attachment. RDocs™ service further allows the originator to add dynamic watermarks that are associated with each viewer to discourage unauthorized sharing, or ultimately to track a leaker. Originators can even restrict or track screen captures and printing.

Location, Location, Location

RDocs™ tool makes it easy for the file originator to send or generate an RPD™ file and restrict the geography where it can be viewed, make it viewable only for staff inside a company, or define the internet locations where it can be accessed – by reader domain, IP range, or geographic region.



Social Documents, Collaboration Re-Invented

The coolness of social media now meets electronic documents. RDocs™ technology has built the power of social interaction into documents. Not only can users track who viewed what, when and where, and for how long, but can also append notes into the document and tally viewers’ votes, likes, and feedback in real time. Users can gauge the popularity of documents in many new ways.

RDocs

Send

Create

Manage

david@northendassoc.com

Logout

Search by Access Control, Document ID, Email, Status, Subject

Kill Selected

<input type="checkbox"/>	Type	Created (UTC)	Subject	Document Name	Initial Recipients	Status	Access Control
<input checked="" type="checkbox"/>		01/18/2024 14:31		purchase-order	david@northendassoc.com	Active	Track Readers

Control Status

Document ID:

074016426899FDAE5949ABAC

Owner:

david@northendassoc.com

Original file name:

purchase-order.pdf

Pages:

2

Sent:

01/18/2024 14:31 (UTC)

Launches:

01/18/2024 (UTC)

Expires:

Restrict to domains:

Allowed IP:

Max reads per reader:

Unlimited

Max views per document:

Unlimited

Allow responses to:

procurement@northendassoc.com

Watermark:

None

Banned regions:

☒ Timestamp
 ☐ Can print
 ☒ Display distribution list
 ☒ Voting
 ☒ Share votes
 ☐ Identify leakers

Track Interactivity

Address	First Read (UTC)	Reads	Total Minutes	Vote	Active/Banned
megan@northendassoc.com	01/18/2024 15:20	1	3		Active
jennifer@northendassoc.com	01/18/2024 15:18	1	5		Active
matthew@northendassoc.com	01/18/2024 14:50	1	26		Active

Total: 3 0

Summary

First Read (UTC)	Reads	Total Minutes
01/18/2024 14:50	3	34

Activity Log

Event	Reader	Time (UTC)	IP	Location	Country	Network
Opened	matthew@northendassoc.com	01/18/2024 14:50	190.12.116.239	Boston, MA	United States	T-Mobile
Opened	jennifer@northendassoc.com	01/18/2024 15:18	201.190.251.250	La Jolla, CA	United States	ATT
Opened	megan@northendassoc.com	01/18/2024 15:20	190.12.116.239	Boston, MA	United States	T-Mobile

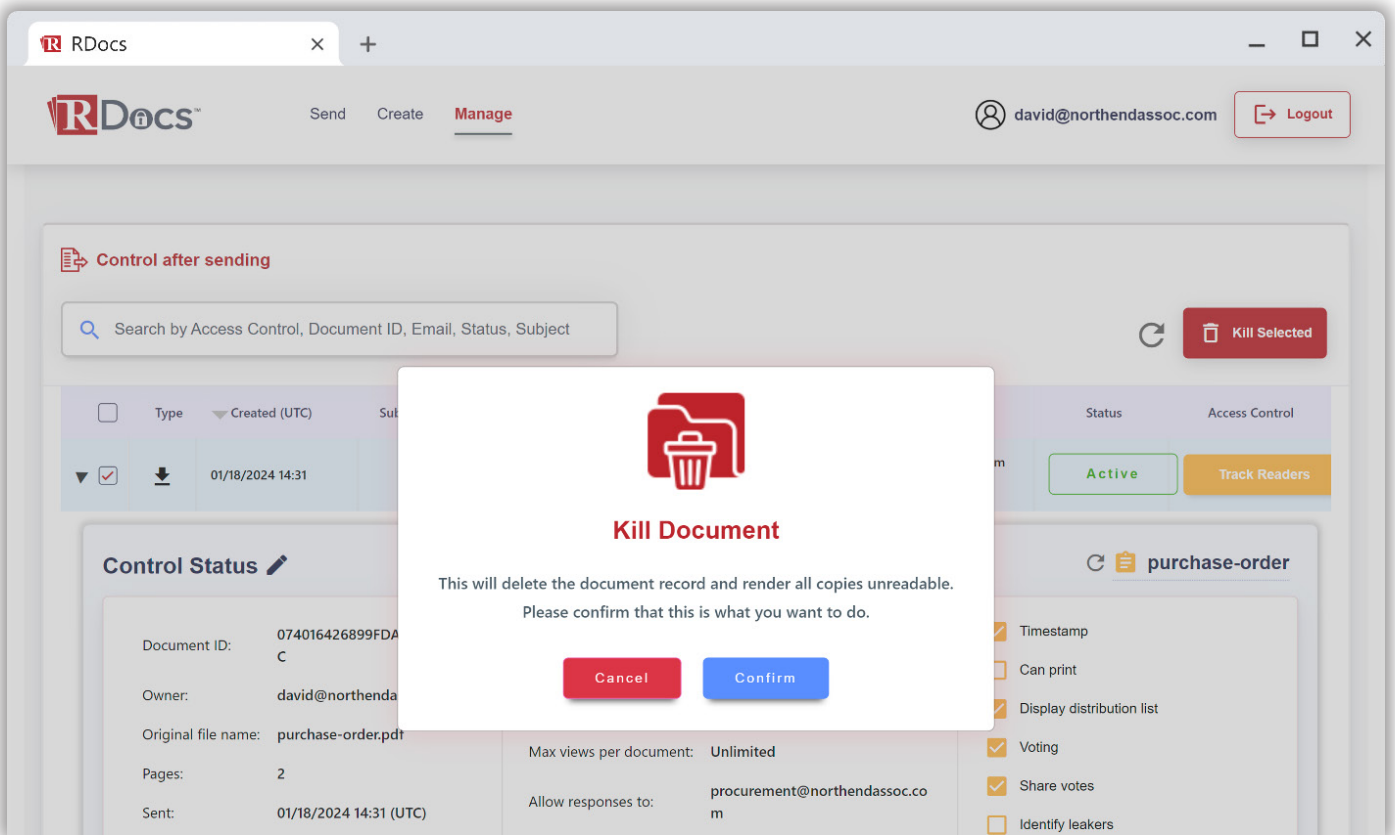
Location: registered location of the detected network

Maintaining Control Post-Distribution

RDocs™ technology enables senders to maintain full control over their sent documents. If you accidentally send sensitive data to the wrong recipient or decide a document should not stay in a recipient's inbox, you can kill it entirely or temporarily disable viewing for one, some or all readers.

Additionally, our platform allows senders to modify the settings of sent RPDs at any point. This includes adjusting automatic launch and expiry dates, limiting the number of reads per reader or document, enabling or disabling voting, changing the “reply-to” address, and enabling/disabling printing capabilities.

Senders also have the power to control access based on reader's domains and even specific internet or geographic locations. All these settings can be easily managed from the 'Manage' tab, offering enhanced control and security over your digital documents after they've been sent.



AI-Infused File-Lock: Automatic Cybersecurity™

RDocs™ service introduces an advanced security feature, the 'AI-Infused File-Lock,' leveraging RPost's Active Tracker™ technology. This innovative system is designed to intelligently detect anomalous and potentially hazardous activities involving a document. When such irregularities are observed, the AI-Infused File-Lock automatically locks the file, simultaneously alerting IT personnel and/or the document owner.

This feature is effective even at security levels 1 (Track Views) and 2 (Track Readers), which permit forwarding. RDocs™ AI engine intelligently assesses whether a document's activity is anomalous relative to standard business operations and expected document interactions. In instances where a potential security threat is detected — such as a compromised recipient account — the system preemptively locks the file. The originator is then provided with options to either unlock the file or kill access, coupled with an alert suggesting the possibility of a cybercriminal presence within the recipient's network.

Goodbye One-Size-Fits-All, Hello Tailor-Made Security

Delving into more specifics, with the RDocs™ RPD file converter/generation service, document originators can opt between three levels of security and customize everything from IP range availability to document expiry per viewer, even after the send.

All the settings described in this section can be automatically applied to a document attached to an email, while the email is in transit, or to a file that is converted to an RPD for storage or later sharing (simultaneously submitted as a document and retrieved as an RPD).

Track Views: Level 1 Security

With Level 1 Security there is no requirement at the recipient other than to open and view documents.

Document originators can opt to restrict viewing to certain geographic locations or other internet locations, such as only within their corporate network.

Document originators may additionally choose to protect the content by scheduling a precise document availability, and may apply additional advanced content protections to the document, including:

- Proof of sending,
- Watermarking the document with visible marks,
- Timestamping the original document,
- Print restricting,
- Permitting in-document message responses to the originator,
- Generating authorized reader identity-marking to track a photo-capturing leaker, and
- Killing a document and all of its traces.

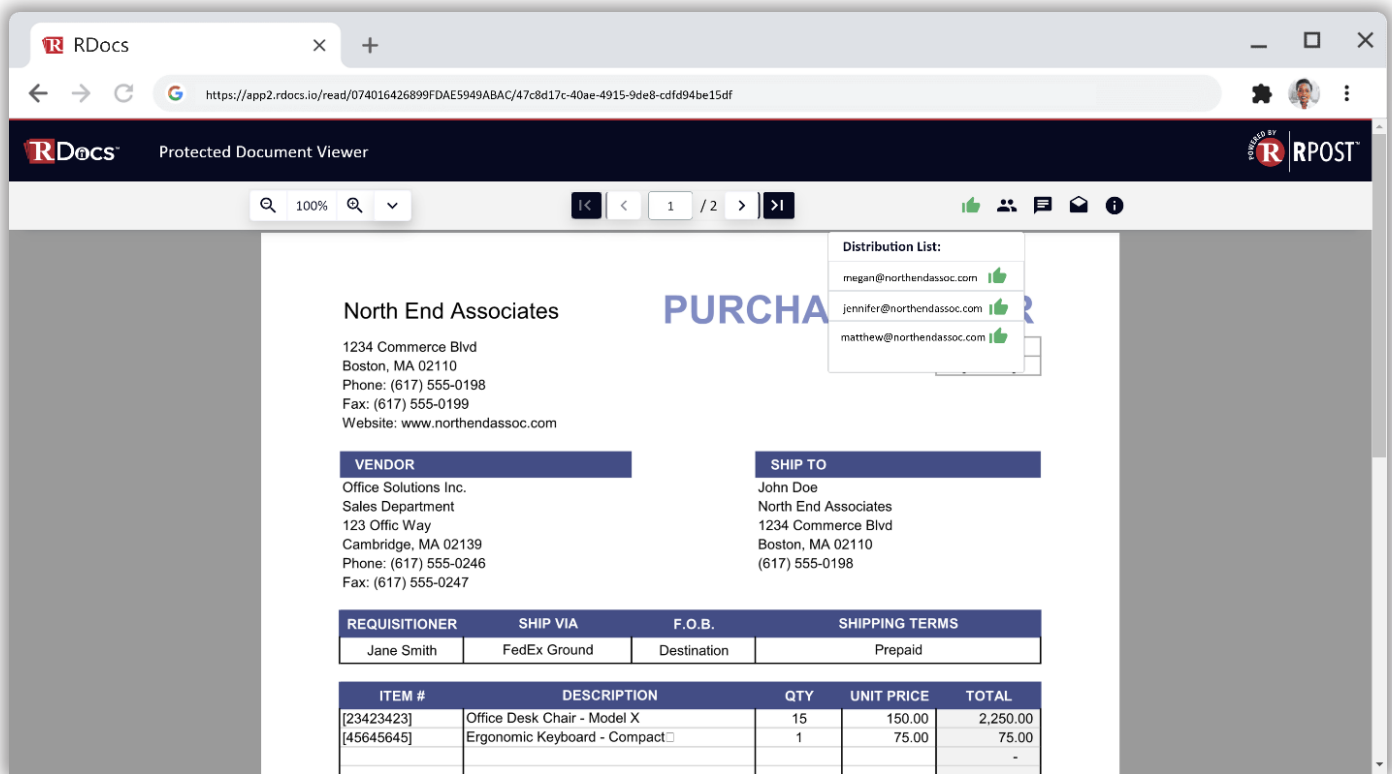
A common use for Track Views: Level 1 Security is to be able to have visibility into popularity of a document that may be transmitted or posted for download (number of times viewed, duration of viewing, etc.) and yet retain the ability to, at will, expire viewing for all viewers. This can also be used to create an aura of true urgency to view content before a deadline, for example.

Track Readers: Level 2 Security

Level 2 Security provides the original sender insights into how many times and in what geographic locations the document has been opened and viewed, with insights tagged to each reader.

Readers are identified, associated with their authenticated email address, and insights are displayed to the originator in a web-based activity log, displaying:

- Notification of reading,
- Who read what and when,
- Tracked distribution (forwards),
- How many times the original document was read,
- Time duration of each viewer’s reading, and
- Geographic IP location of each reading.



The screenshot shows a web browser window with the URL <https://app2.rdocs.io/read/074016426899FDAE5949ABAC/47c8d17c-40ae-4915-9de8-cdfd94be15df>. The page is titled "Protected Document Viewer" and displays a purchase order for North End Associates. The document includes contact information for North End Associates, a vendor section for Office Solutions Inc., a ship to section for John Doe, and a table of items with their descriptions, quantities, unit prices, and totals. A distribution list is also visible on the right side of the document.

North End Associates
 1234 Commerce Blvd
 Boston, MA 02110
 Phone: (617) 555-0198
 Fax: (617) 555-0199
 Website: www.northendassoc.com

VENDOR
 Office Solutions Inc.
 Sales Department
 123 Office Way
 Cambridge, MA 02139
 Phone: (617) 555-0246
 Fax: (617) 555-0247

SHIP TO
 John Doe
 North End Associates
 1234 Commerce Blvd
 Boston, MA 02110
 (617) 555-0198

REQUISITIONER	SHIP VIA	F.O.B.	SHIPPING TERMS	
Jane Smith	FedEx Ground	Destination	Prepaid	

ITEM #	DESCRIPTION	QTY	UNIT PRICE	TOTAL
[23423423]	Office Desk Chair - Model X	15	150.00	2,250.00
[45645645]	Ergonomic Keyboard - Compact	1	75.00	75.00
				-

Distribution List:
 megan@northendassoc.com
 jennifer@northendassoc.com
 matthew@northendassoc.com

Social Documents

RDocs™ technology enables in-document real-time interactivity by allowing the document originator to append notes to a document that are viewed by readers inside the document itself without altering document content, and to carry out reader polls (and tally reader like and dislike votes). Viewers can record their votes, comments or leave questions for the Originator.

Votes are recorded for each tracked reader and are tallied for the originator in a web dashboard visible to the originator so that the originator can easily track and view both the individual votes as well as the aggregate vote tally for each document.

The originator may further choose to permit each viewer to see how others with document access have voted individually and/or in total, or the originator may restrict the vote tally and vote details so that only the originator has view of the vote results.

Leakers Folly

RDocs™ technology empowers originators with robust tools to both discourage leaking and have actionable proof to identify those who disclose sensitive content (or for example, restricted content under non-disclosure agreements). This is accomplished with a combination of both visible dynamic watermarking and hidden steganographic markings.

- **Dynamic watermarking: Leak Prevention**

As reviewed in this document, RPD owners have a wide array of tools that help prevent unauthorized access to their content, like sharing as a Level 3 RPD, restricting access to certain domains, restricting access to specific internet or geographic locations, disabling printing, and more. RDocs™ Dynamic watermarking aims at further discouraging unauthorized content sharing by printing the reader's email identity tags dynamically across the document, like their email address, IP address, and more. This way, readers of sensitive content are visually reminded that if they were to share a snapshot of any one page or part of a page, they would be at risk of the leak being easily traced back to them. Although this functionality does serve the purpose of identifying potential leakers, by making the markings visible it is primarily designed to discourage malicious intent.

- **Steganography: Leaker Identification**

Rooted in ancient Greece, steganography is a method of secret communication based on the practice of concealing a message within another message. This method was traditionally used for transmitting confidential information without drawing attention, protecting intellectual property (widely used by artists and creators), and in the digital era it has become a crucial tool to trace unauthorized distribution of digital property. RDocs™ technology developed a proprietary steganographic method to hide codes within RPD documents, which are uniquely linked to each authorized recipient. This way, if a reader with malicious intent distributed content within a confidential RPD, the hidden steganographic markings would trace back to the leaker, providing the originator with robust forensic court-admissible evidence of the crime.

Restrict Readers: Level 3 Security

Incorporating all the capabilities of Track Readers: Level 2 Security, Level 3 Security takes your document control a step further, empowering you to define a specific audience for your RPDs.

Level 3 Security provides stringent access control, allowing only those readers explicitly authorized by the sender at the moment of RPD creation. This is ensured by a secure two-factor authentication process, confirming the reader's identity matches the one initially approved by the document originator.

This advanced security level affords additional layers of control, permitting you to:

- Limit document viewing to a specified viewer or a predefined list of registered viewers
- Disable document forwarding or distribution by authorized viewers

In addition, Level 3 Security accommodates the dynamic nature of business by enabling the addition of new readers post RPD creation. If at any point you wish to extend access to a new reader, there's no need to create a new RPD. Simply navigate to your Manage tab, and seamlessly add new authorized readers to your existing RPD. This way, RDocs™ service provides robust and flexible security, adapting to your changing needs.

Use Cases

Legal Bliss: A Deal Room Without the Room

Digital deal rooms have become increasingly popular in the legal sector, particularly in the digital era, and especially post-Covid pandemic. They facilitate faster deal closures, offer a fully digital experience to clients, and significantly reduce the time and costs associated with the transaction. However, these rooms are not without their challenges. The primary concern is the sensitivity of documents, including PII, PHI, and financial information, and their storage on third-party servers. This not only increases the risk of cyberattacks and data breaches but also raises serious compliance issues, especially in cross-border transactions where data sovereignty is crucial.



RDocs™ technology addresses this Achilles' heel effectively. Its revolutionary technology embeds security controls within the file itself, eliminating the need for content storage on the a third-party system. This innovation delivers *all the advantages of a digital deal room, minus the room itself*.

Moreover, digital deal rooms often force viewers to create accounts, learn new systems, and sometimes even purchase licenses. Many of these platforms are known for their complexity and lack of user-friendliness, posing challenges for less tech-savvy users and concerns for IT administrators. RDocs™ service surpasses these hurdles by delivering files directly to the reader, akin to receiving and opening a standard PDF. This simplicity and familiarity enhance user experience dramatically. Integration with existing systems is another area where RDocs™ technology excels. Traditional digital deal rooms can lead to inefficiencies, data silos, and security and compliance vulnerabilities due to their cumbersome integration processes. In contrast, RDocs™ technology is engineered for seamless integration, ensuring smooth operations and data consistency. It's even integrated seamlessly within the RPostOne ecosystem with both its applications for Microsoft Outlook and Microsoft Windows desktop, enabling users to automatically convert attachments to RPD file format within their normal email workflow or just by right-clicking a file. For IT administrators, RDocs™ service supports deployment with the RPost Cloud Security Gateway, allowing the creation of custom rules for automatic document conversion to RPD format with selected features. This facilitates a no-action-required approach from users, removing the need for user training while ensuring full security and compliance - a true IT bliss. Lastly, RDocs™ technology effectively meets legal and regulatory standards, including GDPR compliance, providing legal professionals with peace of mind. Its comprehensive audit trails ensure that all system actions are accurately recorded and attributable, an essential aspect of legal compliance and accountability.

Enhanced Governance and Compliance

In the modern landscape of data governance and compliance, the ability to manage, control and audit document access post-distribution is not just a convenience but a necessity. RDocs™ technology provides a powerful tool in this regard, particularly with its capability to 'kill' a mis-sent document. This feature is invaluable in mitigating the consequences of unintended document leaks.

If a document is sent erroneously, it potentially constitutes a data *leak*. However, the severity of this leak largely depends on whether the unintended recipient accessed the document and, more importantly, whether they viewed sensitive information within it. RDocs™ service elevates governance and compliance strategies by offering detailed access data. This data includes whether the document was opened, which specific pages were viewed, and for how long.

In scenarios where sensitive information is contained only on certain pages, RDocs™ technology's precise tracking can determine if those pages were accessed. This granularity is crucial in differentiating between a simple *leak* and a *reportable breach*. Should the sensitive pages be viewed, the incident escalates to a reportable breach, necessitating specific response protocols as per compliance regulations.

Moreover, the ability to instantly 'kill' the document upon realizing a mis-send adds a layer of proactive control. Organizations can swiftly act to prevent further unauthorized access, significantly reducing the risk of information compromise. This capability not only enhances data security but also aligns with stringent compliance standards, offering organizations a robust tool to maintain high levels of data governance.

Targeted Marketing on Steroids

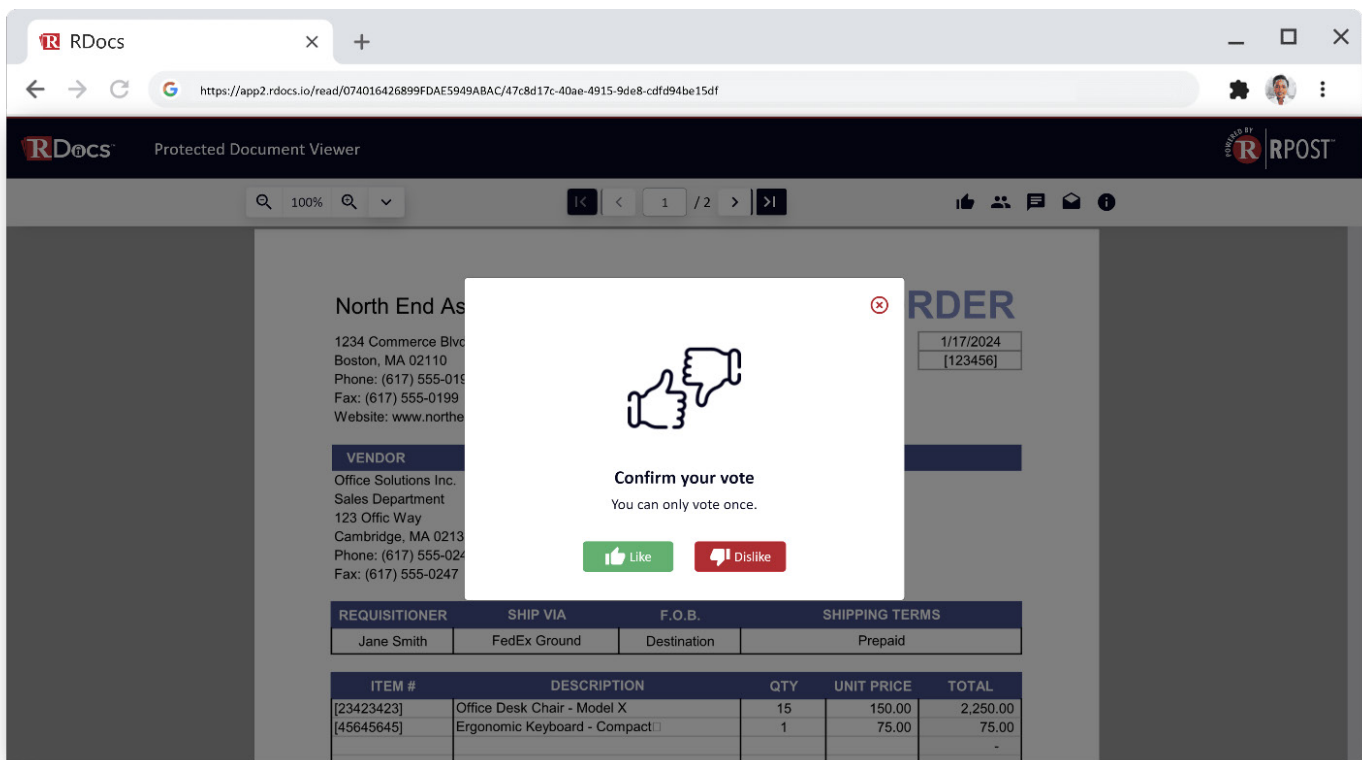
Typically, brochures, whitepapers, reports, and other pieces of sales and marketing content are posted for download behind a firewall, accessible after a form fill or a log-in to an intranet. However, the person who downloads the content might not read it at all, or, on the contrary, they could be so captivated that they forward it to their peers, who might in turn share it with others, and so on. This means that marketers are really gathering insights about downloaders, not actual readers, and are also lumping together users with very different behaviors and engagement styles, which severely compromises the accuracy of retargeting efforts and campaigns in general.



RDocs™ technology enables originators to track who is reading their content, when, where, how many times, for how long, and even which pages captivate their attention the most. This level of detailed insights about actual engagement with content is unprecedented, especially in a platform that also prioritizes security, compliance, and user experience. Moreover, these insights extend to secondhand readers and beyond. This detailed level of insight into actual engagement with content is unparalleled, and even more so in a platform that simultaneously prioritizes security, compliance, and user experience.

Signoff Workflows Simplified

RDocs™ technology revolutionizes the process of recording and tallying approvals through the ‘Vote’ function, simplifying signoff workflows significantly. This functionality becomes particularly useful in scenarios requiring collective affirmation on concepts, clauses, terms, or documents from both internal and external parties. RDocs™ service excels by creating an environment where all document-related activities, including voting, are meticulously recorded. This forensic audit trail includes critical details like timestamps, IP addresses, email addresses, geolocations, and network information. The comprehensive nature of this tracking enables RDocs™ technology to serve as a streamlined tool for internal approval processes, eliminating the need for complex workflow management solutions.



Example Use Cases

Some examples of high value content distributed as PDF files that would better serve the originator if distributed as RPD files include research reports and financial tip newsletters; non-public corporate, board or shareholder reports; funds transfer information; invoices; final versions of agreements related to highly sensitive transactions.

Each of these (and other) documents would be better served as an RPD, with different feature sets or access levels depending on the type of document or desired document-centric functionality.

Type of Document	RPD Security Level	Other RPD Features	Main Benefit vs. PDF
Research reports, financial tip newsletters, real estate market reports, subscription content	Level 3: Restrict Readers	ID Leakers, watermark, timestamp, expire on a timed schedule or after a number of views.	Prevents distribution to unauthorized viewers, protecting content license revenue.
Research reports	Level 2: Track Readers	ID Leakers, Watermark	Gather email addresses of “secondhand” viewers for future marketing and re-targeting.
Sales & Marketing content (product roadmaps, reseller battlecards, reseller price tables)	Level 2: Track Readers	Document time availability, IP restriction, reader domain restriction.	Allows sharing of content with controls to limit exposure of sensitive or strategic content to only intended recipients or those within their companies.
Sales & Marketing content (whitepapers, product brochures)	Level 2: Track Readers	Document time availability, voting, notification of reading	Allows to track who is reading what, when, how many times and for how long; capturing popularity of content at the document-level and creating marketing lists with secondhand tracked readers.
Funds transfer information, purchase orders, and invoices	Level 3: Restrict Readers	IP range restriction and domain restriction, notification of reading	Prevents unauthorized viewers, limits wire fraud or the potential of fake invoices. Key features: IP range restriction and domain restriction, notification of reading.

Non-sensitive internal documents and presentations	Level 1: Track Views	Watermark, document availability	Keep track of how many times and where your documents are accessed, providing insight into document popularity. Expire old presentations and brochures when new ones are available to limit use of outdated material.
Corporate board or shareholder minutes or resolutions	Level 2: Track Readers	Voting, Watermark, ID Leakers	Easily compile votes affirming acceptance of minutes or resolutions, with a tally aggregated conveniently for the originator. Disable access to the file after the vote for privacy.
Technical bulletins (release notes)	Level 1: Track Views		Make sure that these documents are read.
Technical documentation (software, pharmaceutical, etc.)	Level 1: Track Views	Custom document availability	Kill outdated information.
PII in general	Track Readers / Limit Readers	Watermark, ID Leakers, Custom document availability	Prevent data leaks. Automatically kill content after predefined timeframe.

Conclusion

The post-pandemic world has accelerated the future of work, and a future with focus on decentralization. As a result, technologies that were once revolutionary and full of possibility can no longer keep up with the new ways of doing business. Content shared only within office meeting and board rooms is now accessible out in the ether – often lacking same controls afforded in a controlled environment.

RDocs™ technology eliminates the need to control the environment and puts those controls right into documents themselves – protecting and controlling in the now and in the future at the originator's whim.

As such, being able to share information securely while safeguarding digital rights, digital lifespan, and

digital footprints of who is viewing what content and when, and retaining controls, has never been so crucial. Welcome to the new dawn of Digital Rights Management for documents; the next generation of Portable Document Format (PDF) will be Rights Protected Document™ (RPD). Welcome to the new age of ubiquitously accessible (yet access controlled) **RPD™** files.

About RPost

RPost® is the global leader in premium, feature-rich and cost-effective email compliance & security, e-signatures, and document security services, and we've been continuously innovating for our customers the world over since 2000. From within our three main platforms, RMail®, RSign® and RDocs™ Document Security, we're everything our customers need when it comes to transacting in the digital world in a secure and compliant manner. We thrive on ensuring that we are artisans and experts in everything we do: secure and certified email encryption for privacy and compliance; eSignatures and web forms to ease digitization of workflows; e-delivery tracking to prove important communications; managed file transfer to simplify secure sharing of large documents and sets of files; document-level digital rights management to empower control of document access even after transmission; and AI-infused apps to prevent data leaks by minimizing human e-security errors. This is why more than 25 million users have enjoyed our services for over two decades across 193 countries. Learn more at the [RPost website](#).

RPost was recognized as Hot Vendor and Most Innovative Vendor in Digital Transaction Management by Aragon Research in 2022.

"This recognition validates RPost commitment to providing organizations with the tools they need to embrace digital transformation, enhance customer experiences, and ensure the security and privacy of their digital interactions, not only for the 'today' but for organizations' journey of continuous digital transformation into their future."

Jim Lundy, CEO, Aragon Research

Learn more at the [RPost website](#).



Identifies **RPost** as

Most Innovative Software Provider

In Aragon Research Globe™

For Digital Transaction Management



Leader in eSign & e-Security

FAQs

1. How does RDocs™ technology enhance data security and control?

RDocs™ technology provides stringent access control, depending on the specific use case of the documents you share. With Security Level 3, senders can grant access to only those readers explicitly authorized at the moment of document creation. This is ensured by a secure two-factor authentication process, confirming the reader's identity matches the one initially approved by the document originator. RDocs™ technology allows you to limit document viewing to a specified viewer or a predefined list of registered viewers and disable document forwarding or distribution by authorized viewers. Moreover, RDocs™ technology accommodates the dynamic nature of business by enabling the addition of new readers post document creation. This way, RDocs™ service provides robust and flexible security, adapting to your changing needs.

2. How does RDocs™ technology compare to other options in the market?

Unlike traditional Digital Rights Management systems that require viewers to use the same software as the file originator and have the proper licensed access to the software, RDocs™ technology eliminates the need for additional software installations and premium licensing costs on the viewer. It provides a unique solution that allows control of document access even after transmission, thereby preventing data leaks and enhancing data security.

RDocs™ service also offers unique features like tracking readers, allowing voting, identifying potential leakers, automatically expiring documents, restricting access to certain domains or internet/geographic locations, and managing all the above even after the send. Senders can even kill documents entirely or temporarily ban individual or multiple readers.

3. How can RDocs™ technology help prevent data leaks in the case where an authorized reader with malicious intent shares their unique passcode AND the instructions to open the document?

RDocs™ technology has several mechanisms in place to prevent data leaks, even in scenarios where someone might share their unique passcode and instructions:

- **Dynamic Watermarking (fka Steganography):** RDocs™ technology applies dynamic watermarks that are associated with each viewer to discourage unauthorized sharing. If a viewer were to share a snapshot of any one page or part of a page, they would be at risk of the leak being easily traced back to them. And if a viewer were to share their access instructions with an unauthorized third-party, they would be at risk of having any leak associated to them.
- **Geolocation and Internet Addresses Restrictions:** The originator can restrict the geography and even the networks where the document can be viewed. This means that even if the passcode and instructions are shared, the document can only be accessed from specific locations. For sensitive content, these settings are strongly suggested.

- **After-the-Send Controls:** The document originator can make a document self-destruct on a timer, on a specific date, view once, after a number of views, or at the click of a button. This means that even if the passcode and instructions are shared, the document may be inaccessible (with the view once setting, in particular if the original intended recipient viewed the document already) and can be made inaccessible at the originator's discretion. If a viewer is suspected to have malicious intent, the owner of the document can revoke access or kill the document entirely with a simple click.
- **AI-Infused Auto-Lock:** The AI-Infused Auto-Lock system actively monitors for unusual or suspicious activity patterns related to document access. If it detects an anomaly – such as access from unexpected locations or atypical viewing patterns – it automatically locks the document, preventing further unauthorized viewing. This proactive approach is instrumental in mitigating the risks associated with internal threats or malicious intent, safeguarding the document even after the initial distribution.
- **Tracking:** RDocs™ technology allows the originator to track who viewed what, when, and where, and for how long. This means that any unauthorized access can be quickly identified and addressed.
- **Additional Security:** With the underlying technology the way it is, RDocs™ service can add more capabilities for additional security as customers/partners request, like those below.

These features make it very risky for someone to share their passcode and instructions, as any unauthorized access can be traced back to them. Furthermore, the document can be made inaccessible at any time by the originator, further reducing the risk of data leaks.

4. How does RDocs™ technology manage the lifecycle of sensitive documents, from creation to expiration, to ensure data privacy?

RDocs™ technology manages the lifecycle of sensitive documents by maintaining full control over the documents even after they have been sent. If a document is accidentally sent to the wrong recipient or if the sender decides that a document should not stay in a recipient's inbox, they can kill it entirely or temporarily disable viewing for one, some, or all readers. The platform allows senders to modify the settings of sent RPDs at any point. This includes adjusting automatic launch and expiry dates, limiting the number of reads per reader or document, enabling or disabling voting, changing the "reply-to" address, and enabling/disabling printing capabilities. Senders also have the power to control access based on the reader's domains and even specific internet or geographic locations. All these settings can be easily managed from the 'Manage' tab, offering enhanced control and security over digital documents after they've been sent.

5. How does RDocs™ technology provide actionable proof to identify those who disclose sensitive content, and how can this help in mitigating risks?

RDocs™ technology provides actionable proof to identify those who disclose sensitive content. RDocs™ service empowers originators with steganographic, dynamic, and in-motion watermarking that is uniquely identifiable to each authorized recipient. This discourages unauthorized sharing and provides court-admissible proof of who shared any unauthorized snapshot of a document. Readers visually see that if they were to share a snapshot of any one page or part of a page, they would be at risk of the leak

they would be at risk of the leak being easily traced back to them. This can significantly help in mitigating risks associated with unauthorized disclosure of sensitive content.

6. Can I use RDocs™ technology for marketing purposes?

Yes. RDocs™ technology enables originators to track who is reading their content. This empowers content originators or distributors with insights that they can use to further market, re-target viewers, or otherwise monetize. This ability to capture consumer interest for marketing efforts is especially relevant in the current scenario where traditional methods of capturing consumer online behavior have been affected by data protection features. RDocs™ service is able to capture this information in a completely compliant manner.



Contact us to get started!

www.RPostDocs.io

US: +1-866-468-3315

UK: +44 003 6333505