vitrium

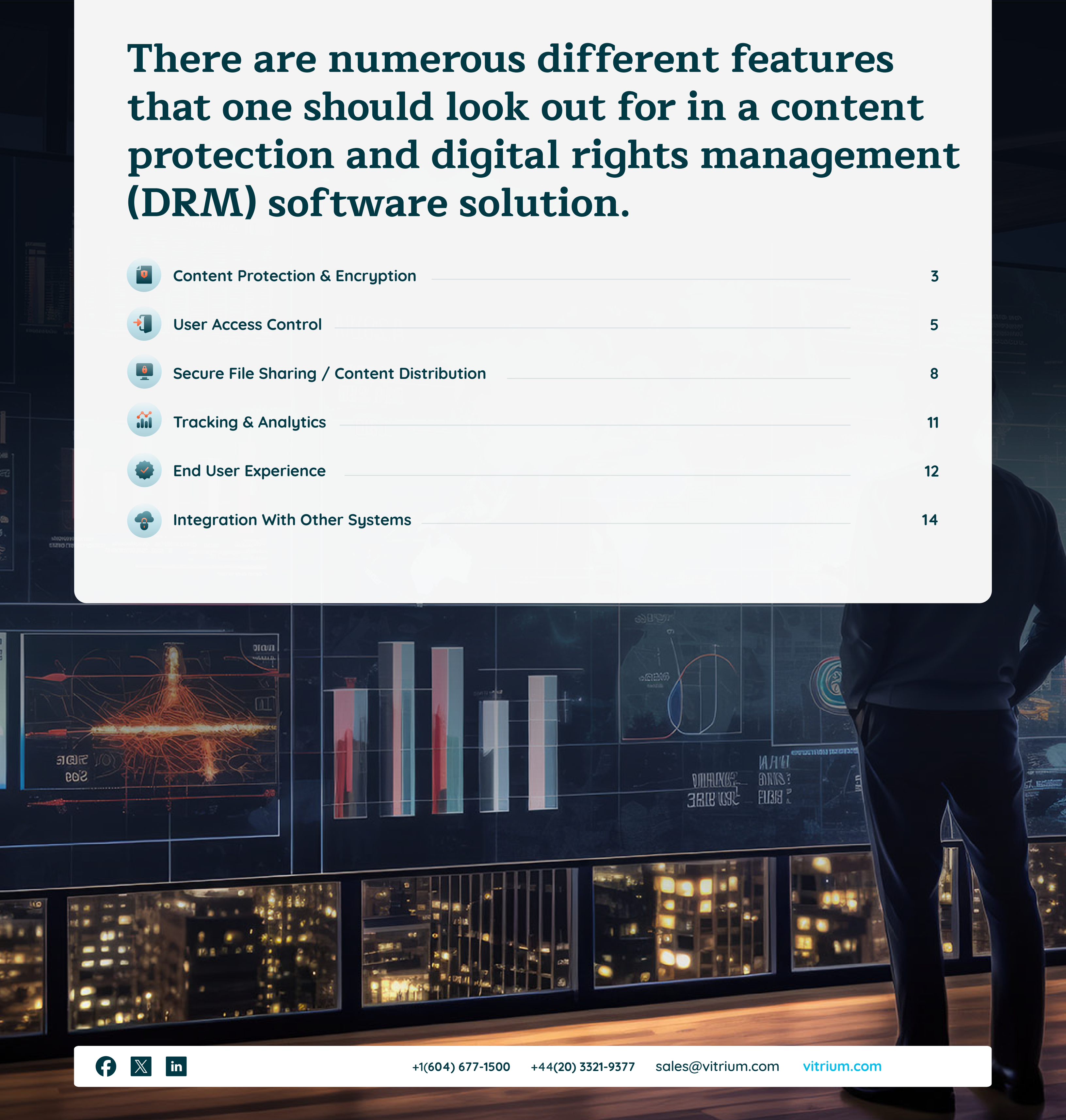
White Paper

The Ultimate Guide to a Robust Digital Rights Management (DRM) Solution

+1(604) 677-1500
+44(20) 3321-9377

sales@vitrium.com
vitrium.com

There are numerous different features that one should look out for in a content protection and digital rights management (DRM) software solution.



Content Protection and Encryption

Any content that can be easily copied, printed, or shared is prone to many threats like piracy, intellectual property (IP) infringement, mass redistribution, leaks, plagiarism, data breaches, and so on. Particularly vulnerable is content that generates revenue for a business or contains confidential information, trade secrets, financial information, or content that is otherwise sensitive in nature. So in this digital age, what are firms to do?

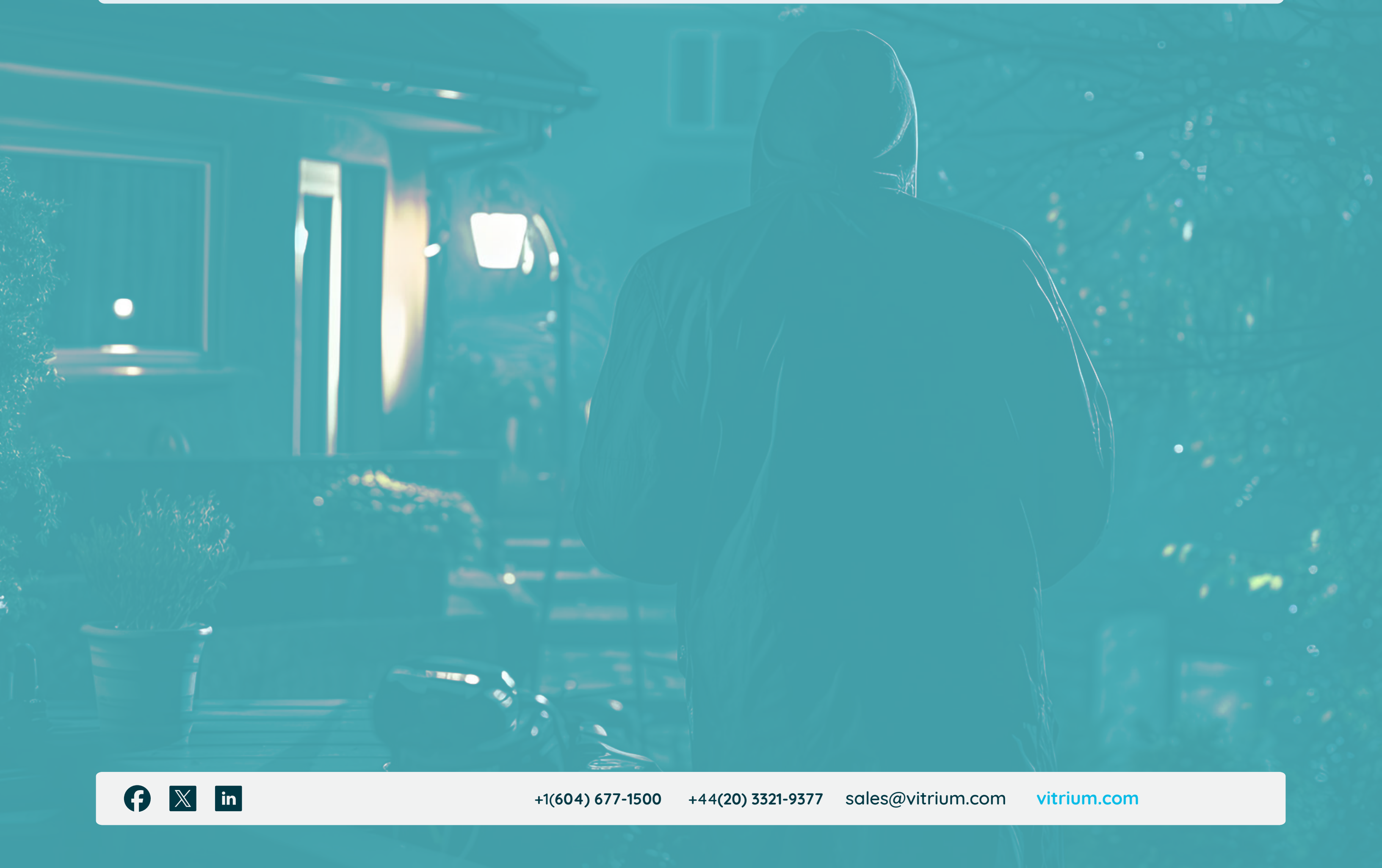
The first line of defense that comes to mind is to add password-protection on a file. Although passwords can restrict file access, they are often easy to share, easy to crack, and difficult to manage for more than a single user.

Watermarks are also considered and they're an excellent feature to deter copyright infringement, but not restrictive enough on their own. Adding a dynamic watermark that includes user identifying information such as a user name, user ID, company name, etc. definitely takes things a step further, but again, not restrictive enough on its own.

The best measures are to add strong, military-grade encryption. With this option, you're essentially converting your unprotected content to a non-readable, encrypted format that can then only be unencrypted when you receive the encryption keys or you've been authenticated against another system. The most common encryption level offered by many file sharing and virtual data room providers is disk-level encryption. At this level, only the directory containing the files is encrypted while individual files remain unprotected and still vulnerable to leaks, unauthorized sharing, piracy and other potential hacks.

Vitrium Content Protection Features	Benefits
Password-protection or 3rd party authentication options	Grants access to only authorized users
Secure portal and file-level encryption*	Keeps both the house (portal / data room) and the individual files protected to prevent hacks, leaks, unauthorised sharing, and other attacks or malicious use
Copy and print protection including print limits	Prevents plagiarism, piracy, and re-distribution
Multiple dynamic watermarks	Prevents copyright theft, plagiarism, and re-distribution
Hidden watermarks	If visible watermarks are cropped out of a screenshot, decoding a hidden watermark can help you identify the culprit

A great analogy for disk-level encryption is protecting your house with a lock and security system, but leaving all your valuables inside unprotected. A robber could bypass the lock and security system, and then gain access to whatever they find in the house. However, by applying file-level encryption and control in addition to the disk-level encryption is analogous to having a robust digital rights management (DRM) system like Vitrium which protects both the house (or portal / data room where the content resides).



User Access Control with DRM

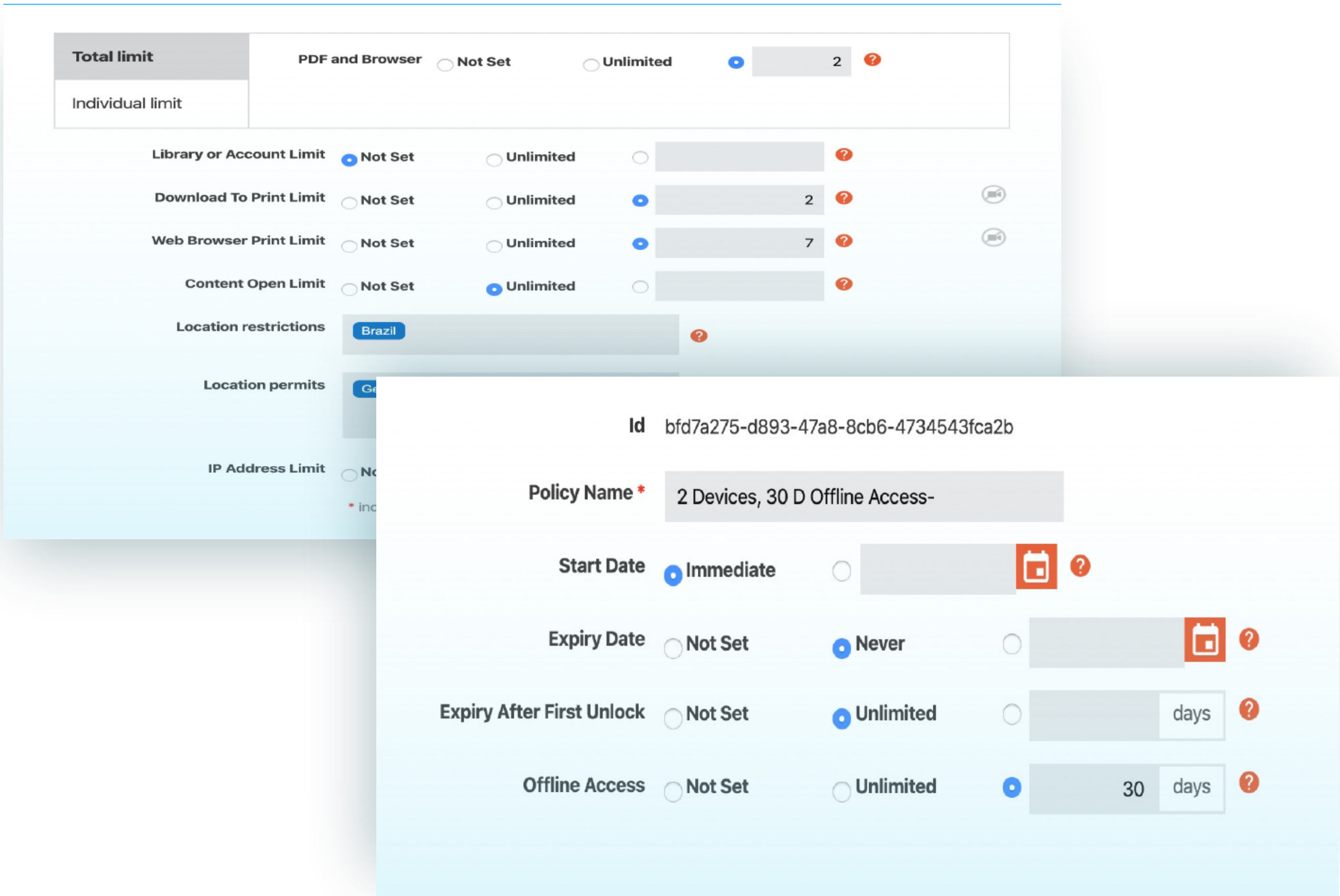
User access control is not a zero or one concept anymore. Digital rights management (DRM) technology allows content owners to determine how different audiences could access different files. Granular DRM policies have empowered many content producers and publishers to offer multi-tiered subscriptions and membership plans to meet different segments' needs, increase their revenues, and stay competitive. That's great for revenue-generating content but how does it help for confidential or sensitive files that don't generate revenue for a business but are still equally important to protect?

User Access Control with DRM Due to their sensitive nature, confidential files may also require different types of user access controls. For example, you may want to provide different levels of access control for companies that are in different stages of a merger & acquisition (M&A) deal. Maybe for those companies that are in the early stages of a deal, you decide to only provide them 1-week access to content and you set a 1-device limit for each file in your data room, but then for companies that are in the later stages (say the due diligence phase), then you provide 30-day access and a 5-device limit for each file knowing that content needs to be shared among more people within the company. When it comes to user access control, the first and most critical function is the ability to grant and revoke access anytime, no matter where a file resides or who it is shared with. Once you are assured that your content is within your control all the time, another valuable function is the ability to set up more granular restrictions.

The reason that clients choose Vitrium Security over other companies that offer virtual data room solutions, is that we add much-needed layers of ironclad protection and control to your content. When you set up your virtual data room with us, the content you place inside it is instantly encrypted and secured. Within minutes you can protect your digital assets and share with authorized users, without worrying about unwanted sharing or distribution.

A comprehensive digital rights management (DRM) system like Vitrium encompasses numerous different user access controls including:

- Expiration limits - a specific date or number of days when content should expire
- Start date - a date when a user can first access the content (ideal for subscriptions, the start of a school term, or the start of an RFP process)
- Device / browser limits - how many devices (or browsers) a user can open content on
- Print limits - how many times a user can print content
- Open limits - how many times a user can open or view content
- IP address limits - how many IP addresses a user can open content from
- Specified IP address - which IP address (or range of IPs) a user can open content from
- Country or state limits - which country(ies) and/or state(s) a user can open content from or, the opposite, which country(ies) and/or state(s) users cannot access content from



Total limit	PDF and Browser	○ Not Set	○ Unlimited	● 2
Individual limit				

Library or Account Limit	● Not Set	○ Unlimited	○	
Download To Print Limit	○ Not Set	○ Unlimited	●	2
Web Browser Print Limit	○ Not Set	○ Unlimited	●	7
Content Open Limit	○ Not Set	● Unlimited	○	
Location restrictions	Brazil			
Location permits	Ge			
IP Address Limit	○ No			

* inc

Id	bfd7a275-d893-47a8-8cb6-4734543fca2b			
Policy Name *	2 Devices, 30 D Offline Access-			
Start Date	● Immediate	○		
Expiry Date	○ Not Set	● Never	○	
Expiry After First Unlock	○ Not Set	● Unlimited	○	days
Offline Access	○ Not Set	○ Unlimited	●	30 days

Leveraging flexible DRM controls, you can define different access control policies for different audiences or stakeholders. For example, you may only want your certified partners to access certain confidential or IP-related materials such as new price sheets and technical guides associated with a new product line you're about to release. You can provide access to those certified partners based on their IP addresses and perhaps also limit them to opening the content on a certain number of devices. Alternatively, if you have a select few other contacts that you would like to provide access but they have not been designated a 'certified partner' yet, you can assign them permission to the content but apply a more restrictive policy such as access on 1 device only, no printing, and no copying based on their non-partnership status.

This flexibility can be extremely valuable for companies that operate with a subscription-based model. Let's take the example of a research firm that distributes a highly-sought price reports for the commodities sector. They offer 3 different subscription plans to their clients, all with different price points and different offerings: (1) Bronze, (2) Silver and (3) Gold. Here is an example of how tiered subscription plans like this can take advantage of flexible DRM access controls.

Gold

In the "Gold" plan, users pay a hefty premium fee but they receive unfettered access to the commodities reports with unlimited device use, unlimited printing capabilities and access across the globe.

Silver

In the "Silver" plan, users pay a premium fee but not as hefty as the Gold plan and they receive access to the reports on 10 devices, 5 prints and access in 5 countries of their choice.

Bronze

In the "Bronze" plan, users pay a standard fee and they receive access to the reports on 2 devices, 1 print and access only in 1 country of their choice.

The more comprehensive and flexible your DRM access controls are, the more diverse permission levels you can set, and the more revenue you could earn by up-selling to the more lucrative subscription plans.

Vitrium DRM Access Control Features	Benefits
Allow or revoke user access anytime	Provides full control of your content all the time
Define different access control policies for different types of users	Offers granular controls and different permission levels for different stakeholders or groups Supports use of multi-tiered membership or subscription models
Choose a start date and set different expiration methods (specific date or number of days after first access)	Protects content within your specific period of time Allows you to control when and how long your clients or audience has access to your content Aligns with subscription plans and membership renewal periods
Set device (browser) limits, open limits, print limits and IP address limits	Eliminates password-sharing Prevents unauthorized sharing or redistribution of your content Enhances your ability to upsell to higher-tiered subscription or membership plans if policies such as 1 print or 1 device access can be enforced
Restrict or allow access to/from certain countries or states/ provinces	Prevents redistribution of your content Reduces risk of content piracy Supports global or regional subscription or membership plans

Secure File Sharing and Content Distribution

Undoubtedly, a solid content protection and DRM software like Vitrium makes file sharing a secure and straightforward process. A secure digital file sharing and content distribution system like Vitrium diminishes printing and shipping costs while streamlining the delivery of content. Vitrium converts files into two encrypted formats:

- A secure web viewer that can be viewed or accessible in a web browser on any device
- A protected PDF file that can be downloaded and viewed with Adobe Reader

The Bonus: neither format requires the end user (recipient) to download any plug-ins or third-party apps to view the content.

CONTENT DISTRIBUTION FEATURES

- Secure web viewer
- Protected PDF File
- Virtual Data Room / Secure Portal
- Leverage SSO with Your Website or System

Secure web viewer

With Vitrium's secure web viewer, it's a simple, yet very secure URL that can be easily shared from one person (or company) to another. It can be included in an email, posted on a website, or embedded in a system like a learning management system (LMS), association management system (AMS), eCommerce system, or other system where content is distributed to users. **Vitrium's secure web viewer not only makes file distribution simple but also eliminates the hassles and costs of file storage.**

Protected PDF File

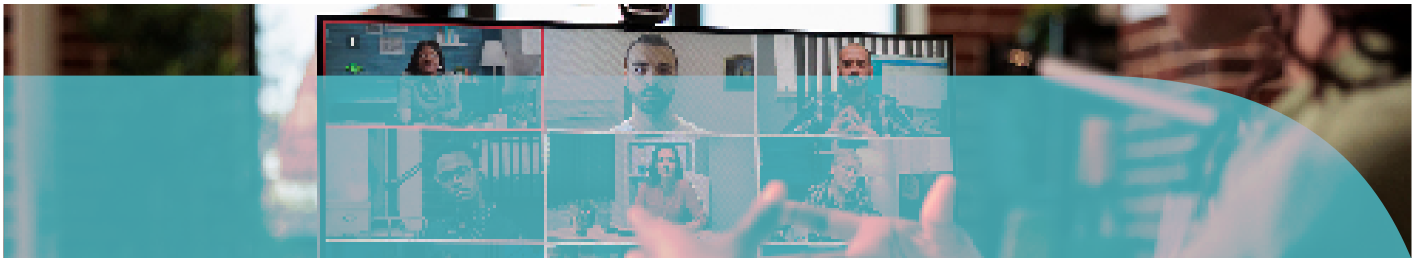
Despite the rising demand for and the wonderful benefits of the secure web format, there are still people who prefer the traditional PDF format, maybe because it's what they've always known or they simply like the idea that they can 'see' the file within their possession on their local hard drive or company network. To serve this type of audience, Vitrium also converts documents into a protected PDF format. The benefit is that the security remains with the protected PDF files no matter where they're downloaded or saved. These secure files can also be distributed by email (if they're small enough), or added to a website, or third-party system mentioned above (LMS, AMS, eCommerce, etc.) and downloaded by authorized users to their local machine or favorite cloud account. Since the security travels with the protected PDF files, you can be assured that you still maintain full control of your content no matter where this file resides. "How", you ask? Well that's our secret sauce! But we can let you in on some of the secrets if you call us.

Virtual Data Room / Secure Portal

If you'd like to offer your clients a central, secure place where users can access multiple files in once place, you can take advantage of Vitrium's virtual data room (VDR) or secure portal as some may call it. You can even make it your own by adding your logo, brand colors and even use your own domain URL. Many VDR and data room providers in the market make you set up different data rooms which can be a hassle, especially if many of them require the same content to be shared. With Vitrium, you only need to create data room or portal. On the administrative side, you can add your content into different folders for different clients and assign permissions to specific users (or clients) at each folder level so the user only sees the content for which they've been assigned permissions to view.

Leverage SSO with Your Website or System

Vitrium's Enterprise Edition integrates with virtually any website or third-party system like eCommerce systems, learning management systems (LMS), content management systems (CMS), association management systems (AMS), CRM systems, and more. By integrating Vitrium with your existing business systems, offering users single sign-on (SSO) functionality, and tying the content distribution (secure file sharing) methods with your existing workflows, this can go a long way to streamline your entire workflow process, especially for the end users who may be your clients, subscribers, members, students, partners, or others.



Vitrium File Sharing / Content Distribution Features	Benefits
Content converted to secure web viewer (secure URL)	› Simple and easy distribution via web link › Ability to embed URL on your website or in your third-party system (LMS, CMS, AMS, etc.) › Compatibility with any web-enabled device › No apps or plug-ins required to download › No need to download files, saving yourself storage costs › Save shipping costs if you're moving away from hard copy distribution
Content converted to protected PDFs	› Send a protected PDF in an email as an attachment › Upload protected PDFs to your website or third-party system (LMS, CMS, AMS, etc.) for users to download › Users can open protected PDFs with the popular Adobe Reader application (no plug-ins required)
Content distributed via secure client portal / virtual data room	› Provides a secure branded platform that can be customized with your logo, brand colors and domain URL › Allows users / audience to access all protected content in one central place › Send one URL to all your end users (or clients) but, spending
Content distributed via your website or third-party business system	› Users are already familiar with the environment › Leverage single sign-on (SSO) functionality › Automate your processes and workflows

User and Content Tracking and Analytics

An indispensable element of good content protection and digital rights management (DRM) solutions is its tracking and analytics capabilities. After you've protected your content, assigned the right DRM access controls and distributed your content, you'll then want to track the usage and monitor how your content is being consumed by your audience (your clients / subscribers / members / students).

Vitrium provides you with some of the most extensive user activity reports and detailed drill-down analytics in the market among DRM or virtual data room providers. The most important report is the User Activity Log where you can track who has accessed your content, which files, on what date and time, from which IP address, browser or application, and even their operating system (OS). This level of user activity tracking not only provides you with insightful data about who your most active users are or which content is most popular but it also allows you to spot any suspicious activity. For example, if you notice that a user has tried to access your content from several different countries or IP addresses in a short amount of time, this could be a sign of unauthorized sharing or distribution, or worse, content piracy. Of course, you can eliminate this from occurring by setting more restrictive DRM access controls such as applying device limits, IP address limits and setting country restrictions (i.e. only allowing access in the USA for example).

User and Content Tracking and Analytics With Vitrium's detailed analytics reports, it opens your eyes about how your users are engaging with your content. You can find out which content has the highest read-through-rate (for documents), view rate (for videos), or which users are the most actively engaged with your content. Vitrium's analytics can provide you valuable insight for your business and drive you to make strategic decisions to lead to more

Vitrium Tracking & Analytics Features	Benefits
Content tracking and user activity	Track who, when, and where your content has been accessed Monitor for any suspicious activities Modify your DRM access controls if necessary
Drill-down analytics	Gain valuable insights into how users engage with your content Make informed business decisions by finding out who or what's the most: › **Popular content** › **Active users** › **Engaged users** › **Active regions/ countries**

Smooth and Seamless End-User Experience

A controversial area that challenges content publishers and distributors is whether content protection and digital rights management (DRM) measures disrupt the end user experience. DRM solutions of the past have indeed posed challenges especially if they required the user to download some form of plug-in, app or third-party proprietary software to view or decrypt content. And some of those providers are still around

Vitrium's offering is not that as the company's focus for the past 15 years has been finding the right balance between the needs of content publishers/owners/distributors to protect their confidential content or intellectual property with the needs of users who just want to access their content immediately, seamlessly.

A sophisticated content protection and DRM software like Vitrium prevents unauthorized users from accessing content while providing the authorized users (the right audience) with a smooth and seamless experience. If you decide to use Vitrium 'out-of-the-box' with no third-party integration, all the end user needs to do is enter their login credentials. These can be supplied by you or you can force the user to create their own when they first access content. If you use Vitrium's Enterprise Edition and you have the software integrated with your website or third-party system with single sign-on (SSO) set up, then the user just accesses their content through their usual methods (maybe via an email with a link to the content, or via their My Orders or My Content page of your website) and the content will immediately 'authenticate' the user and the permissions are passed through API calls. The users themselves don't often realize there's protection or DRM controls put on the content they're accessing… it's that seamless! However, if they try to share the content with someone who isn't authorized, that person will be denied access, providing you the level of protection and control that you need. All of this is tracked in your Vitrium User Activity Log as well.

Don't disrupt your audience, whether it's your clients, partners, subscribers, members, or students with clunky and messy plug-ins or 3rd party apps. Downloading, installing, updating and other compatibility issues exhausts people and they will lose interest in your content. Vitrium's "no plug-ins or apps" approach lets you and your users enjoy a seamless experience.

Moreover, Vitrium's secure web viewer allows end users to access your content on any device via the Internet with all the highlighting, note-taking and other annotation tools they may need. End users don't need to worry about saving files or using up storage on their hard drives or cloud accounts. And they can even access the content while offline with Vitrium's unique 'save-to-browser' feature! For those more traditional folks who just need to 'see a file'..... you can send them the protected PDF and they can download this file to their local machine, company network or cloud account. The document is protected at all times giving you peace of mind but it can be viewed by the authorized user with the popular Adobe Reader application.

Vitrium End User Features	Benefits
No apps or plug-ins required	Provides hassle-free and seamless end user experience
Content access via a secure web links.	› Compatible with any device via an Internet browser › No need to save files and prevent storage hassles › Included popular highlighting and notetaking tools › Users can still view content offline as well
Content access via protected PDF file	› Offers traditional users with that file that they can 'see' and download › Compatible with Adobe Reader on PC & Mac desktops
Self-registration, password reset and forgot password options	› Allow your end users to control what passwords they want to use › Provide method for new users to sign up for your content (you still have the ability to vet them before they get access though) › Reduce administrative burden for users who forget their passwords
Single-sign-on (SSO) options available	› Minimizes hurdles to access protected content › End users only need to log into one system › Eliminates unauthorized sharing
Offline access capabilities	› Provides content access for users when they don't have Internet / Wifi access › Available in both web viewer and protected PDF options

Integration With Other Systems

If you've read this entire article (firstly, good for you!), then you'll have read already about how important it is for a content protection and digital rights management (DRM) solution to be able to easily integrate with a wide variety of third-party business systems. After all, many types of companies across different industries create, publish, and distribute content that needs to be protected. And therefore, the DRM system needs to be able to integrate with a variety of different systems including:

Learning management systems (LMS)

Content management systems (CMS)

Association management systems (AMS)

Customer relationship management (CRM) systems

eCommerce systems

And more!

With industry-standard REST APIs, Vitrium's Enterprise Edition software has been integrated with numerous off-the-shelf, custom and proprietary systems falling into one of the categories above. Integrations are ideal if you wish to automate any of your content workflow processes - the contention protection process, the user administration process, but the number one reason is to enable single sign-on (SSO) functionality in order to make the content access for your end users as seamless as possible. After all, if you already manage users (let's say students) in a learning management system (LMS) and you have your content within that system, why would you want students to enter a separate login to access said content? It's much better if the content has been protected with Vitrium and the user simply clicks on the content with the LMS and is automatically authenticated and authorization permissions are passed to the user.....all within milliseconds, without the user even realizing what just took place!

Vitrium Integration Features	Benefits
Offer single sign-on (SSO) access	Provides seamless access for your end users (clients / students / subscribers / members)
Automate content protection process	Streamlines process if you publish or distribute content frequently
User administration, authentication & permissioning	Streamlines the creation of new users and assigns them with permission to the content they purchased or signed up for

See Vitrium Security in Action!

Schedule a Demo