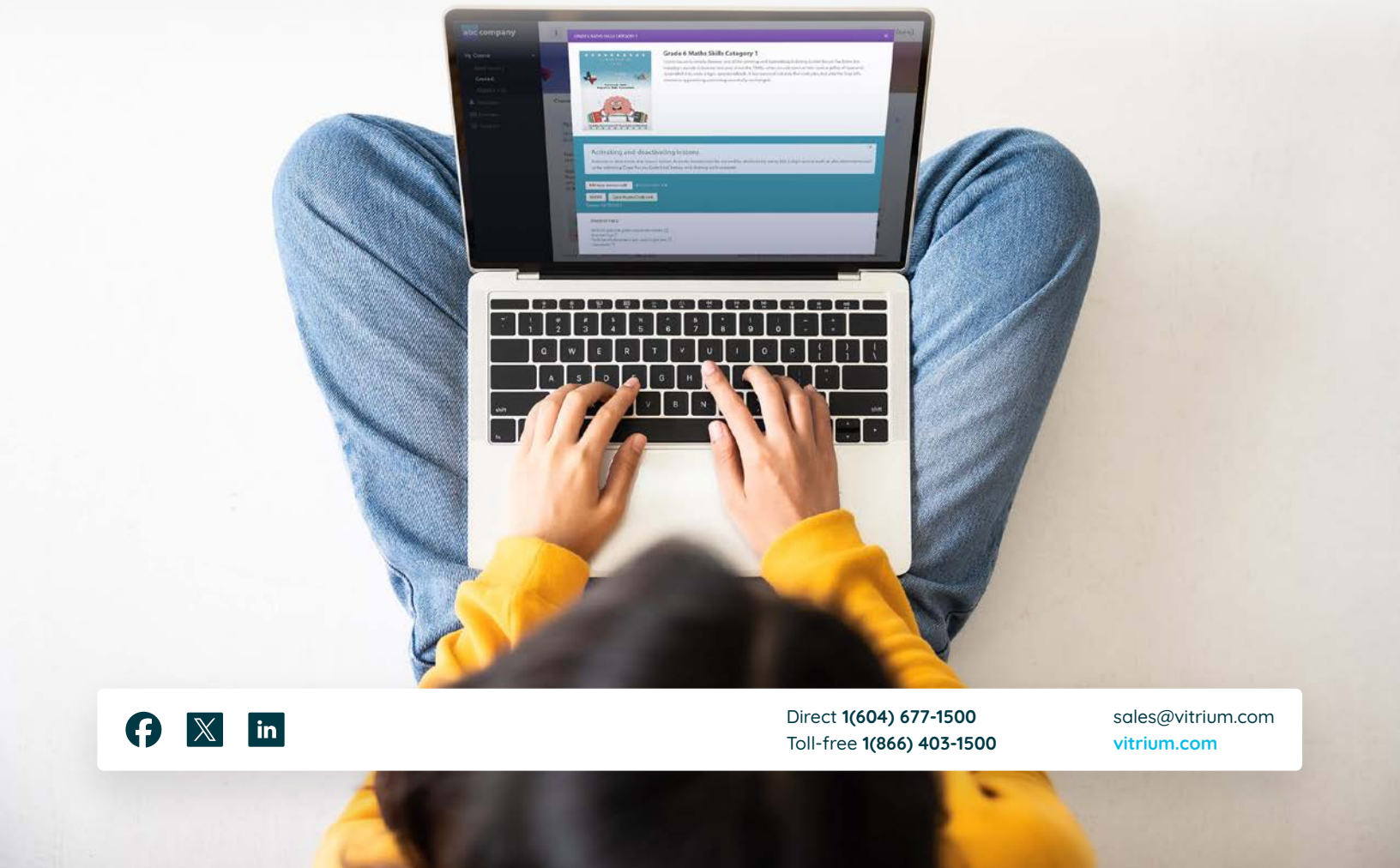
vitrium

White Paper

A Beginner's Guide to Document Protection and Rights Management



Direct **1(604) 677-1500**
Toll-free **1(866) 403-1500**

sales@vitrium.com
vitrium.com

Table of Content

Introduction to Protecting Documents 3

Common Risks to Documents and Publications 3

1. Leaks and unauthorized sharing (intentional or otherwise) 3
2. Hacks and attacks 4
3. Copyright or patent infringement 4
4. Piracy 4

Factors to Consider when Protecting Documents 5

What industries need document protection most? 5

What kind of document should I protect? 6

- Revenue generating content 6
- Intellectual property 6
- Copyrights 7
- Trade Secrets 7
- Scientific Research, Literary, Technical, and Artistic Works 8
- Presentations 8
- Designs 8
- IT Systems and Methodologies 8
- Confidential sensitive data 9
- Research and development 9

About Vitrium Security 10

Benefits of Vitrium Security 10

How Vitrium Security works 11

Start Your Free 7 Day Trial of Vitrium Security 11

Introduction to Protecting Documents

At Vitrium, we have worked with thousands of organizations of all industries over the years, that create, publish, and distribute a large variety of documents. When addressing the need for document protection and rights management, these companies always start with a thorough assessment of the value of the documents and data contained within them. The next step is to consider some scenarios that can, and do, occur that would undermine the value acquisition of the content to the organization.

Time for a change.
Be proactive to establish your company's strategy to secure vital information

Common Risks to Documents and Publications

1. Leaks and unauthorized sharing (intentional or otherwise)

In today's rapid changing digital technology, the way we access and distribute documents continues to evolve, moving towards efficiency and convenience. Widespread file sharing tools like website downloads, Dropbox, Google Docs, or simply emailing valuable content have become predominant methods of distributing and enabling access to critical business information, but also exposing organizations to risks, such as:

- Unsecured documents and data are found on a lost or stolen device.
- Buyers of content distribute it to non-buyers or upload to sharing websites.
- Documents are sent to the wrong "unauthorized" person by mistake, either via email or other means
- Documents are intentionally misdirected for malicious and/or fraudulent purposes – either for monetary gain, extortion, or to damage a company's reputation.
- Documents and information are leaked by employees (or other "bad" actors) to the media, antagonists, or competitors.
- Poor security or infrastructure on protected networks have left documents and data vulnerable to unauthorized sharing.

2. Hacks and Attacks

There is an underlying assumption that only very large companies are attractive to hackers. As documents and data become more ubiquitous and accessible, hackers are finding small and medium-sized companies (with their relatively few hardened security protocols) attractive targets. Hackers may probe your networks for vulnerabilities, specifically targeting documents without wrap-around security, documents in transit, those synced to devices, in cloud-storage, or in unsecured emails.

The tools and trade of the hacker have become highly sophisticated, and companies large and small must now take steps to prevent threats, including:

- Database and network intrusions
- Permission theft, misuse and loss
- Communication intercept attacks like MITM1 and Relay2 attacks
- Denial/disruption of service attacks for blackmailing, or extortion purposes

3. Copyright or patent infringement

Organizations apply considerable efforts and expense to produce original content, including those patented or copyrighted to protect the original investment or revenue streams attached to it. If you have copyrighted material, unprotected work can be:

- Copied or duplicated without permission.
- Modified or manipulated without authorization.
- Used in ways that were not the original intent or without proper authority.

4. Piracy

Online pirates aren't just interested in music, movies and stolen software. Your course material, eBooks, company data, board minutes, research data, maps, specs and all manner of information are valuable resources of information. Content can end up in illegal file sharing sites where over 90%3 of the material is copyrighted and should, by law, be protected.

Factors to Consider when Protecting Documents

The nature of today's digital marketplace has enabled company to find revenue sources through the online sales and distribution of documents and publications. When considering a document protection plan, determine whether or not your company has data, information or content that is worth protecting. Determine what would be the consequences to your business in terms of:

- Revenue - losses and damage that might occur now and in the future
- Reputation - trust and confidence in your brand
- Compliance, or non-compliance with regulations and privacy laws

What industries need document protection most?

The table below illustrates what industries need protection based on the type of documents that are heavily used within these industries.

Industry	Types of Documents
Publishing	eBooks, manuscripts, draft works
Research, Development, Sciences, Pharmaceuticals	Abstracts, reports, studies, analysis, dissertations
Associations	Membership data, confidential & paid reports
Education/eLearning	Learning materials, eBooks
Corporations & Business	Corporate training materials, financial documents
Financial	Investment reports, tax info, statements, personal and/or business data
Management Consulting	Confidential market data and analysis
Legal	Contracts, wills, agreements, and any sensitive legal documents
Healthcare	Confidential patient information, reports
Oil & Gas, and Mining	Drilling sites, maps, specs and plans
Non-Profit	Member data, confidential and paid reports
Manufacturing and Technology	Innovations, patents, design specs or sensitive trade secrets
Advertising & Design Agencies, Architecture	Design briefs, compositions, plans, or sensitive trade secrets
Any Industry and Company	Confidential materials to send to the Board

Not mentioned? There are thousands of companies who can benefit from protecting their files - why not get in touch with us and surprise us with your use case.

Any organization that markets publications or documents in the online marketplace, or that relies on digital documents to distribute sensitive information, must consider a document security strategy. Organizations can take advantage of software solutions that empower them to control how content is accessed, used, and distributed. A software solution that ensures that publications are sold in a personal and non-transferable manner, through a workflow that assigns publications to the appropriate user, while protecting access to these materials from unauthorized users. This is where document protection and digital rights management (DRM) comes in.

What kind of documents should I protect?

Revenue-generating content

Any documents, files or assets that generate revenue should be considered in your protection plan. For many types of organizations, large portions of their revenues will come from training or educational materials, standards and manuals sales, as well as intelligence and research reports. These assets are labor and expertise intensive, and intrinsically carry their value. When they are distributed illegally, creators or distributors of these materials have no recourse to recoup the worth of their efforts. When determining the risk to your business if these files were leaked, hacked, distributed online, through social networks, to media, or to competitors, it's important to consider all the effort and money that went into creating the content.

There are many examples of revenue-generating content that are sold online. Some examples include; expensive research or market data reports, training materials for online courses, eBooks, and financial reports that one may receive as part of a membership to an investment service.

Intellectual Property

Intellectual property are works or inventions created as a result of creativity, such as a manuscript or design, to which one has rights to. These can include works for which a patent, copyright (more on this in the next section), trademark or other type of legal protection may apply. For companies creating or managing these types of content, the value is contained within the original idea, that has been expanded into a creative effort. With these types of work, value comes from releasing the content first and having time to collect revenues before the ideas enter the collective consciousness. Some examples of these types of documents may include patents, inventions, scripts, stories, books, dissertations, theses, eBooks, white papers, newsletters, or even internal corporate materials that include confidential or highly sensitive information. I

Copyrights

The most important information that can be protected by DRM is copyrighted material, which can only be used or distributed by the company that owns the rights to the work. Copyright is at the heart of most intellectual property debates or lawsuits, so such creations should feature passwords and other security tools whenever possible.

Ultimately, even the largest of companies couldn't afford to retain lawyers to litigate every single instance of copyright infringement. This is especially true thanks to the fluid nature of the Internet. As such, document passwords and digital protection are the best ways to lock up content and media to avoid losses from unauthorized distribution. Any documents, files or assets that make you money should be considered in your protection plan. Of these assets, determine the risk to your business if the information in these files was leaked, hacked, distributed online, through social networks, to media, or to competitors.

Trade Secrets

Distributed internally, trade secrets need to be protected whenever possible to avoid falling into the hands of other companies. Information contained in such documents is profitable (though unpatented or trademarked) and should be kept from prying eyes at all costs. Many data breaches are due to insider theft, choose a system that protects at the document level so access is restricted to the document - not just the location on the network.

The Forrester report, Understand the State of Data Security And Privacy: 2013 to 2014(iv) states that **insiders are responsible for 36% of all incidents of data breaches occurring in a company.**

Scientific Research, Literary, Technical, and Artistic Works

Authors and painters are not the only people who need to worry if their materials are going to be taken by unscrupulous parties or inattentive professionals. There are also writers and even video editors who can have their work stolen and used for extralegal purposes. Scientists also need to be aware of the danger that their papers, analyses, reports and dissertations could be at risk.

Presentations

Presentations can be considered intellectual property, such as lectures, talks, videos, recordings and other sorts of instructional videos. This is also true for transcripts of such media, so take that into account when deciding what files should have document protection attached to them.

Designs

Companies that work closely with clients to design machines, processes, buildings or branded collateral didn't have to worry in the past about their ideas being taken and corrupted until they'd already put them into action. Today, all the information that flows between organizations can be easily snatched from the digital world. Smart designers, engineers and architects know that high profile projects and clients deserve to have protection at the source. A good DRM system can prevent theft by applying encryption, controlling who access to who can open the file, and even expiring the document after a certain time.

IT Systems and Methodologies

Even IT departments can share documents internally that might be detrimental if leaked outside of the network (via a mobile device) or the networks were hacked. Network architecture schema, diagrams, password files, list exports, logs, mind maps, and other information on internal security protocols should be considered critical information that should be secured, not just within a secure network, but with wrap-around document-level protection, and especially if it is to be shared externally for any reason (vendors and other suppliers).

Confidential sensitive data

We've all heard stories about sensitive financial or private personal information getting stolen by database intrusions by hackers, but sometimes this data is in documents that are unintentionally shared outside the network, or found on a lost or stolen device.

Also, board minutes and information for shareholders is often confidential. This information can affect a company's value - and prove profitable to competitors. A good DRM system can protect these documents individually to ensure that no one gets their hands on it who isn't authorized.

Research and development

Oil and gas companies, mining, research, pharmaceutical companies and other industries that must keep their operational information and reports deeply secret.

Research and development firms also need to protect their reports and other information from getting leaked. In any industry where there is a great deal of effort and value in these reports, companies should consider protecting these documents.

Documents to Protect

- Revenue-generating content
- Intellectual property
- Copyrights
- Trade Secrets
- Confidential data
- Scientific research, literary, technical, and artistic works
- Presentations
- Designs
- IT Systems and Methodologies

1 See Man-in-the-middle attack.
2 See Stream cipher attack
3 See Online Piracy in Numbers - Facts and Statistics.

About Vitrium Security

We invite you to explore some of the benefits of using Vitrium Security.

Our popular document protection software can help you limit the risk of your content being copied, leaked, shared, or stolen. Your PDF and Office files are instantly protected, ready to be distributed, and easily viewed by your audience. You can choose to publish the secured content to a user portal, send via email, or post to your own website, document management system, learning management system (LMS), eCommerce site, or other portal. Whatever method you choose, the files always remain secured no matter where they go.

Vitrium Security is trusted by hundreds of companies around the world to protect their documents and millions of readers have accessed our secure documents.

Benefits of Vitrium Security

Easy to use, for you and your audience.

Vitrium's intuitive software lets you manage your files, set up users and groups (this can also be managed through a separate system or database), define DRM policies, choose your distribution method, and access real-time analytical reports. Your audience easily accesses your content on any device, without the need for plug-ins or apps.

Distribute your files with confidence.

Your files are secured with Vitrium's **military grade 256-bit AES encryption**, and the layers of protection travel with your file, online or offline, so that even in case of theft or leak, your content remains secured. After uploading your files to Vitrium Security, you will have access to a secured PDF or a secured Weblink to share with your audience.

Your content, your power to decide.

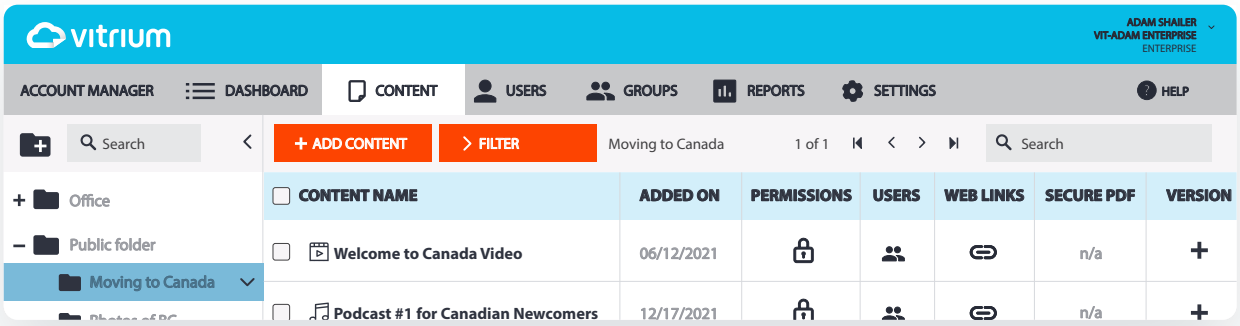
Vitrium Security gives you full control over your content - you can block printing & copying, set browser limits, apply dynamic watermarks, set expiry dates, and more. You can also retain this control after the content has been distributed as you can revoke a document at any time, replace the content, or deactivate a user – all within the Vitrium admin panel.

Set up your own customizable content portal.

Securely distribute your documents via Vitrium Security's customizable user portal, where authorized audience accesses all documents associated with their account in one place. Provide the best experience to by customizing with your colors and logo, and a customizable URL.

Improve the way you do business.

With Vitrium Security's dashboard and analytical reports, you can track the activity of your users and their behaviors, providing you insight into your business. Know which files are being accessed, what pages are being read, and which users are truly engaged. With Vitrium's new User Portal, your document store is instantly created and tracked.



How Vitrium Security Works

Add Files

Add your files to Vitrium's cloud-based ontent security software. We also offer an installed, on-premise version. Acceptable file formats include PDF, Word, Excel and PowerPoint. Video and images to come in 2017.

Add Users & Groups

Select the audience for your content. Decide who can access your secured files, place them in user groups, or leave them as individual recipients. Vitrium can also be integrated with your own user credential system.

Apply Security & Controls

Protect your files with military-grade 256-bit AES encryption and control access by setting various limits – viewing, browser, date, IP address limits and more. Block printing & copying, and insert dynamic watermarks.

Share With Users

Publish and share secured content as attachments or secured weblinks in a customizable user portal, through your own web portal, eCommerce site, or any other system such as document management system, association management, ECM, LMS, or via email.

We can help you integrate Vitrium Security with any system you might be using.

Next Steps

To learn more about Vitrium Security visit www.vitrium.com and start using Vitrium Security today.

Start a Free Trial ›

www.vitrium.com/start-free-trial

Schedule a Demo ›

Visit www.vitrium.com/demo