VITRIUM.COM

eBook:
8 Reasons To Implement a Content Protection and DRM Solution

1.604.677.1500 (direct)
1.866.403.1500 (toll-free)

sales@vitrium.com
www.vitrium.com

Table of Contents

For some types of content, companies want as many views and impressions as possible - for marketing content, advertisements, social media posts, press releases, and so on. But there are some types of content that companies only want certain 'authorized' individuals or organizations to view - for educational content, training manuals, design specs, research reports, price sheets, financial documents, board materials, and so on. This type of content requires some level of protection and control. In this article, we outline 8 different reasons why you might want to consider implementing a content protection and digital rights management (DRM) solution to protect different types of content.

There are some types of content that companies only want certain 'authorized' individuals or organizations to view - like educational content, training manuals, design specs, research reports, price sheets, financial documents, board materials, and so on

1. To Protect Revenue Streams

Content can be the source of revenue for many companies including associations, educational providers, research and advisory firms, standards organizations, and other content publishers or providers. Whether the revenue stream comes from direct sales of eBooks, standards, research reports, training videos, or from paid memberships or subscriptions, these digital assets need to be protected and controlled from unauthorized access. If left unprotected, they can easily be re-shared, printed, copied or mass distributed and thus, you lose out on the potential revenue you could have earned. Even if you hide the content behind a secured website, portal, LMS or other system, you're only protecting the 'house' where the content is located....you're not protecting the actual content or individual files. A good content protection and DRM software allows you to apply file-level control and user-level control to prevent unauthorized access, sharing, downloading and even printing, ensuring that only your paid clients can access the content, giving you the control you need to protect your revenue streams and help you earn more revenue too!

Even if you hide the content behind a secured website, portal, LMS or other system, you're only protecting the 'house' where the content is located....you're not protecting the actual content or individual files!

2. To Increase ROI and Profit

Creating engaging content that generates revenue through sales, subscriptions, or membership fees is often costly as it requires a significant amount of time, money and other resources to develop. Don't let this go to waste! Protect the return on your investment and your bottom line by ensuring you protect this type of content. If you're not earning the revenue that you feel your content deserves or you're not reaching your desired ROI, don't blame the content team. It's not the writers' or designers' or marketing team's fault. It may simply be that people have found a way NOT to pay for your content. Maybe a highly valuable research report, or standard document, or training video was accidentally posted on a social media site, or maybe those single user licenses that you've been selling have actually been shared among entire organizations, thus resulting in lost revenue from selling corporate licenses. The fact is, unless you protect and control your content, your buyers or members will share that content around, thus eating into your profits. A content protection and digital rights management software can help you eliminate this type of unauthorized access or inadvertent sharing and ensures that only those paid customers will receive the content they have paid for, and impose the limits you have set.

If you're not earning the revenue that you feel your content deserves or you're not reaching your desired ROI, don't blame the content team. It's not the writers' or designers' or marketing team's fault. It may simply be that people have found a way NOT to pay for your content.

3. To Protect Intellectual Property (IP)

Intellectual property (IP) is a term that encompasses a wide range of content. Whether it's a patent, copyrighted content, training or educational materials, market reports, data intelligence information, price reports, or whether your content is in text, video or audio format, it's intellectual property and it needs to be protected, controlled and tracked. Many content owners believe that intellectual property protection is equal to registering for a patent, trademark or copyright, but that's just the beginning. Registration of your IP doesn't prevent hackers, pirates, competitors or other individuals from infringing on your copyright and redistributing the content. The key to truly effective IP protection for your digital content is to add a file-level content protection and digital rights management (DRM) solution to prevent all sorts of unauthorized access and leaks. Today's DRM solutions don't have to be cumbersome for the user either. Consider a solution that doesn't require the end user to download any 3rd party plug-ins or apps to view the protected content. Consider options that allow your users to access your protected content through a custom-built secure portal or through a learning management system (LMS), an e-commerce site, association management system (AMS), content management system (CMS), or a system of your own choosing.

Registration of your IP doesn't prevent hackers, pirates, competitors or other individuals from infringing on your copyright and redistributing the content.

TO EARN MORE REVENUE THROUGH MULTI-TIERED SUBSCRIPTIONS

4

4. To Earn More Revenue Through Multi-Tiered Subscription

The subscription business model is on the rise and many businesses that have traditionally offered a one-time 'forever' purchase are switching to selling subscriptions, whether monthly, annually, or for a specified time period. Although the subscription model has many virtues over one-time sales, there are some critical measures to consider to earn more revenue: offering multi-tiered subscription levels and prices. If you offer different price points for different subscription levels (and ensure each level offers different services or options), you should see your revenues start to ri subscription se. If you don't offer different pricing options, you may find yourself losing to the competition who may be doing this already. When selling your content as part of a subscription model, a time-based restriction is one of the more obvious choices to control access to your content to coincide with the subscription period, but there are numerous other DRM controls to consider as well. For a lower priced subscription tier, you could set a restriction on the number of files that a subscriber can access, control the number of times one can open or print your content, restrict access to 1 device only, or 1 IP address. Then, for a higher priced subscription tier, you can offer more files for the user to access and allow them to view the content from more devices, and so on. By implementing a sophisticated digital rights management (DRM) solution , you can customize and tailor your subscription plans with different DRM controls for different subscription tiers.

When selling your content as part of a subscription model, a time-based restriction is one of the more obvious choices to control access to your content to coincide with the subscription period, but there are numerous other DRM controls to consider as well.

TO GAIN MORE MEMBERS AND MEMBERSHIP REVENUE

5

5. To Gain More Members And Membership Revenue

Many businesses such as associations and non-profit organizations offer premium content to attract new members and raise their membership enrollments. However, once members access and download the content they're looking for, they can easily cancel or won't renew their membership. Or some individuals will sign up for the less expensive single-user membership but then share their login with friends, colleagues or others from their organization, resulting in you losing out on the additional revenue streams you could have earned. This combined loss of members and membership revenue could be reversed if you implemented a content protection and DRM solution that can allow you to protect your individual content files but also allow you to roll out different DRM policies for different membership types. For example, you could implement a more strict 1-device limit and no download policy for an individual member who pays a smaller fee but then offer a more lenient policy of 10-devices and unlimited downloads for a corporate-level membership. You could take this one step further and introduce more subscription tiers to both your individual and corporate memberships. Just remember: if you leave your content unprotected for one member, they can then download, copy and possibly re-distribute that content to potentially thousands of other people. Protecting your content and applying different access controls to different types of members will actually help you earn more revenue from your content.

Once members access and download the content they're looking for, they can easily cancel or won't renew their membership. Or some individuals will sign up for the less expensive single-user membership but then share their login with friends, colleagues or others from their organization.

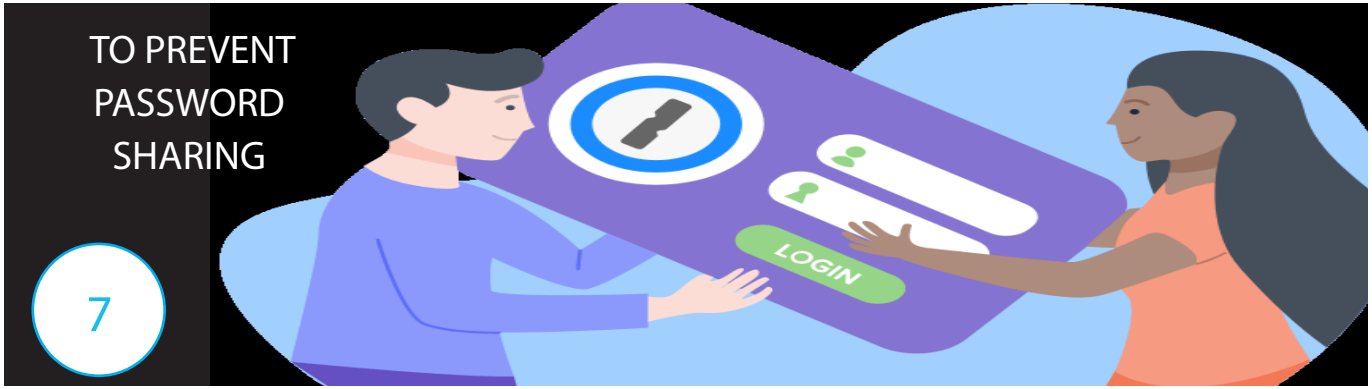
TO RESTRICT
UNAUTHORIZED ACCESS

6

6. To Restrict Unauthorized Access

Content such as trade secrets, design specs, board documents, price lists, internal manuals, and other confidential or sensitive types of content are designed to only be seen by a specific audience and perhaps for only a limited time. This type of content can be highly prone to unauthorized sharing, insider theft, or other type of digital leaks. A digital rights management (DRM) solution can help you protect this type of content from potential threats as you can grant access to only the specified audience with certain restrictions placed on the content (no printing, no copying, no sharing) or certain limits imposed on the user (device limits, IP address limits, open limits). You can also control the access with expiry dates or revoke access at any time if you suspect any fraud or malfeasance.

Content such as trade secrets, design specs, board documents, price lists, internal manuals, and other confidential or sensitive types of content are designed to only be seen by a specific audience and perhaps for only a limited time.



7. To Prevent Password Sharing

It's a common belief that gating your content with a strong password could protect it from others gaining unauthorized access. However, even the strongest passwords can still easily be shared with others and opens the gate to anyone whom that password is shared with. According to Yubico 2019 password and authentication security behaviors report, 2 out of 3 individuals share passwords with colleagues to access accounts. The best tool to overcome password sharing is to implement Digital Rights Management (DRM). A comprehensive DRM solution Vitrium allows content owners to go beyond applying the typical authentication methods and allows you to set granular file-level control with access rights assigned to the individual or group. Some examples of this granular control include setting device limits, IP address limits, print limits, country and state restrictions, and more. For example, let's say you assigned a recent subscriber with a 1-device limit to view your content and even if that person was able to share his password with his friend or colleague, that 2nd person would be denied access due to the limit you've imposed on him. And even if you chose not to set such restrictive limits, you can always reference the detailed user activity logs in your DRM software to track the details of who's opening your content, from which IP address, which device, and more. Good DRM solutions will also include more granular analytics reports allowing you to drill in to see which users are spending the most time with your content, what pages they've read, how long they've watched the video, and more!

Even the strongest passwords can still easily be shared with others and opens the gate to anyone whom that password is shared with

8

TO PREVENT CONTENT PIRACY

8. To Prevent Content Piracy

Digital piracy is an endless threat to content in any format. A while ago, in the era of the second generation of cellular network (2G), when data transmission systems were not capable of handling complex data like videos, piracy was very rampant. While for many, accessing expensive content without paying was the main purpose of piracy, others enjoyed the sense of possession and saved files in their hard drives. With the advent of cloud storage, adequate streaming technology and most importantly public access to broadband internet and 4G devices, many experts predicted piracy would be over. It seemed like even pirates would rather subscribe to a content provider like Netflix for a couple of dollars a month than undergo costs and hassles of storing huge amounts of data in local drives. As a result, many content providers switched to the subscription model and more subscription businesses entered the market. With the proliferation of content subscriptions, now users must subscribe to various apps in order to access the content they're looking for which end up spending the same amount they spent before. This again aroused pirates' motivation and brought piracy back to the forefront. The Global Innovation Policy Center estimates that global online piracy costs the U.S economy at least $29.2 billion in lost revenue each year. Don't let the pirates get your content! Protect it with military-grade encryption, apply various DRM controls such as device limits, IP address limits, country and state restrictions, print limits, expiry dates, and more. And don't forget to track the usage of your content. Analytical insights can be just as powerful as the protection and control that you apply to it.

With the proliferation of content subscriptions, now users must subscribe to various apps in order to access the content they're looking for which end up spending the same amount they spent before. This again aroused pirates' motivation and brought piracy back to the forefront.