**Digital Rights Management**-

**Digital rights management (DRM)**is a way to protect copyrights for digital media. This approach includes the use of technologies that limit the copying and use of copyrighted works and proprietary software.

In a way, digital rights management allows publishers or authors to control what paying users can do with their works. For companies, implementing digital rights management or processes can help to prevent users from accessing or using certain assets, allowing the organization to avoid legal issues that arise from unauthorized use. Today, DRM is playing a growing role in data security.

With the rise of peer-to-peer file exchange services such as torrent sites, online piracy has been the bane of copyrighted material. DRM technologies do not catch those who engage in piracy. Instead, they make it impossible to steal or share the content in the first place.

**How Digital Rights Management Works**

Most of the time, digital rights management includes codes that prohibit copying, or codes that limit the time or number of devices on which a certain product can be accessed.

Publishers, authors, and other content creators use an application that encrypts media, data, e-book, content, software, or any other copyrighted material. Only those with the decryption keys can access the material. They can also use tools to [**limit or restrict**](https://www.vera.com/product/) what users are able to do with their materials.

There are many ways to protect your content, software, or product. DRM allows you to:

* Restrict or prevent users from editing or saving your content.
* Restrict or prevent users from sharing or forwarding your product or content.
* Restrict or prevent users from printing your content. For some, the document or artwork may only be printed up to a limited number of times.
* Disallow users from creating screenshots or screen grabs of your content.
* Set an expiry date on your document or media, after which the user will no longer be able to access it. This could also be done by limiting the number of uses that a user has. For instance, a document may be revoked after the user has listened ten times or opened and printed the PDF 20 times.
* Lock access only to certain IP addresses, locations, or devices. This means that if your media is only available to US residents, then it will not be accessible to people in other countries.
* Watermark artworks and documents in order to establish ownership and identity.

Digital rights management also allows publishers and authors to access a log of people and times when certain media, content, or software was used. For instance, you can see when a particular e-book was downloaded or printed and who accessed it.

**Digital Rights Management Use Cases**

In today’s digital world, digital rights management is increasingly important, not only for digital content creators but also for companies and individuals that make use of digital assets licensed or purchased from third-party creators. Here are a few common use cases for digital rights management:

1. Digital rights management allows authors, musicians, movie professionals, and other creators to [**prevent unauthorized use**](https://static.helpsystems.com/Vera/pdfs/Infographics/vr-entertainment-in.pdf) of their content. It can also protect their bottom lines and control the distribution of their products.

2. Digital rights management can help companies control access to confidential information. They can use these technologies to restrict access to sensitive data, while at the same time allowing it to be shared securely. Furthermore, having DRM technologies makes it easier for auditors to investigate and identify leaks. When used in a business setting, digital rights management may be called by a different name, such as information rights management or enterprise rights management. [**Healthcare organizations**](https://digitalguardian.com/blog/healthcare-security-understanding-hipaa-compliance-and-its-role-patient-data-protection) and [**financial services companies**](https://digitalguardian.com/solutions/financial-services) turn to DRM to meet data protection regulations such as [**HIPAA**](https://digitalguardian.com/blog/what-hipaa-compliance) or [**GLBA**](https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act).

3. Digital rights management ensures that digital work remains unaltered. Creators often want their work to be distributed in its original form to serve its intended purposes. [**The FDIC uses digital rights management**](https://federalnewsradio.com/hearings-oversight/2016/05/fdic-pursuing-data-rights-management-technology-protect-information/) to prevent the unauthorized redistribution of sensitive digital information, for example.

4. Many companies in the manufacturing, technology, and biotech sectors store sensitive patents, trademarks, customer information, and processes across multiple storage platforms, both on-prem and off-prem. To protect that data and IP, they would need a digital right management tool to secure those files wherever they may reside.