

Prioritizing Your Data Protection Program

**Data Loss Prevention, Encryption,
and Digital Rights Management**



Prioritizing Your Data Protection Program:

Data Loss Prevention, Encryption, and Digital Rights Management

As the demand to better protect enterprise data from external attack, insider abuse, bad business processes, or simple mistakes, security professionals are gaining a growing arsenal of tools and techniques for data security. Three of the most powerful technologies for protecting data are Data Loss Prevention (DLP), file and folder encryption, and Digital Rights Management (DRM). However, understanding when and where to use these technologies can be difficult. Encryption and DRM are powerful preventative controls but practical realities often make them difficult to manage on an enterprise-wide basis. DLP, on the other hand, is specifically designed for comprehensive deployments to evaluate risk and determine where other remediation efforts are effective. Most enterprises find that starting with DLP allows them to save costs and more efficiently protect their sensitive information. In addition, DLP enhances existing encryption and DRM deployments—increasing their scope and effectiveness.

Encryption

How it works

File and folder encryption is the process of taking data and running it through a process that makes it unreadable unless you have the right key to decrypt it. Encryption is the electronic equivalent of an invincible lock box—once you put something inside of it, you can't gain access without the proper key. But unlike a lock box, you can make as many copies of it as you'd like, and as many keys as you'd like. Encryption does an excellent job of protecting data as it moves, physically or virtually, and may be useful to protect data against administrators but once a user decrypts the data, all protection is lost. Encryption for data at rest is normally a manual process and can be applied at the media, file/folder, database, or application levels.

When to use it

File and folder encryption should be used in two cases:

1. When data moves physically or virtually. This includes situations such as portable media (like USB drives or CD/DVDs) or emailing files.
2. For separation of duties. This includes situations such as encrypting sensitive files on a system to protect against administrators or encrypting a directory on a shared server.

Some use cases span these two situations. For example, a workgroup might use encryption to protect their files on a shared server, on their laptops, and as they email the files.

Limitations

Encryption offers no protection once an authorized user accesses a file. If they copy content and paste it into another document, then email it, the content is completely exposed. File and folder encryption is also very manual. Since encryption tools do not understand the content, data is either encrypted manually by the user or automatically based on where it's stored. If you save the file on the desktop instead of the protected directory, it's completely exposed. Few organizations deploy encryption beyond encrypting entire laptops or a small percentage of emails due to these limitations. As we'll see, you can use DLP to enhance the scale and security of encryption through content-based automation.

Digital Rights Management (DRM)

How it works

DRM is a combination of encryption and metadata that describes who is allowed to access the data, and exactly what they are, or aren't, allowed to do with it. It's the equivalent of a bodyguard that travels around with the data making granular decisions on how it can be accessed and used. Rights include actions like read, change, cut/paste, email, copy, move, save to portable storage, and print. DRM is extremely powerful but can be difficult to implement on a large scale.

When to use it

Today, DRM is most useful for protecting extremely sensitive data at the workgroup level where granular control is most needed. It includes situations like engineering teams, unstructured customer data, future product plans, and specific engineering, product, or other technical content. Organizations typically use DRM to protect data from both external theft and internal abuse from authorized users.

Limitations

DRM requires extensive integration with enterprise applications—anything that touches the file, such as word processors, needs to be extended to understand the DRM and access the file. DRM is also extremely manual and difficult to implement on a wide scale. Users need to understand what rights apply to what users on what content—a level of complexity that usually results in employees ignoring the DRM and leading to unsuccessful projects that don't improve security. As with encryption, enterprises have to rely on manual judgment to apply rights, since the DRM tools have no ability to understand content. Successful DRM deployments are typically limited to small workgroups of highly trained users. It is generally unsuitable for large enterprise deployments due to this complexity. As with encryption, you can use DLP to focus your DRM initiatives and ease some of the manual processes that inhibit wider deployments.

Data Loss Prevention (DLP)

How it works

DLP solutions eliminate the limitations of encryption or DRM through a deep understanding of enterprise content. DLP solutions use central policies to identify, monitor, and protect data at rest, in motion, and in use through extensive content analysis. Rather than being applied manually to data, as with encryption and DRM, DLP solutions scan inside the content and use advanced techniques to determine how to protect the information. For example, you can set a policy to block any outbound email containing customer credit card information, or to find any document on any unapproved server or endpoint with all or part of a new product plan. Advanced DLP solutions such as the Vontu Data Loss Prevention solution from Symantec can identify sensitive content based on central policies, and then automatically relocate this content to a secure location to intelligently drive encryption or DRM efforts.

When to use it

DLP is suitable for any organization that wishes to discover, classify, and protect sensitive content on the network, in storage, and on endpoints based on central policies. By understanding where sensitive information is stored and how it's being used, most organizations reduce their risk of unmanaged data with DLP while more efficiently applying other security controls, like encryption or DRM.

Where To Start Your Data Protection Program

Organizations should start by deploying Data Loss Prevention to understand their risks and evaluate remediation targets. Once you know where your greatest exposures are, you can deploy encryption or DRM when the data needs those additional protections. If you already use encryption or DRM, you can use DLP to validate and enhance those existing programs. Where possible, leverage DLP so you can intelligently drive encryption and DRM protection based on central, content-based policies, rather than relying on the user to apply controls or save files to a specific location. By starting with DLP, enterprises eliminate the need for completely manual, error-prone procedures, while knowing exactly where their information needs protection.



Vontu, Now Part of Symantec

475 Sansome Street, Suite 2000

San Francisco, CA 94111

Tel: +1.415.364.8100

Fax: +1.415.364.8190

info@vontu.com

www.vontu.com