Overview

Many companies seeking to counter modern IP theft threats are currently evaluating digital rights management (DRM) technologies. A companion brief, “Keeping Secrets: Is it time for DLP or DRM?” offers a thorough analysis of modern IP theft threat vectors and examines the abilities of data loss prevention (DLP) and DRM to combat these threats.

Enterprise digital rights management (E-DRM), also called information rights management (IRM), is the utilization of DRM technology to control access to corporate documents such as Word, Excel, PDF, or emails. E-DRM is intended to prevent the unauthorized use of proprietary documents, for example, industrial or corporate espionage, or inadvertent release. Some industries traditionally favor DRM to protect secret data (for example, the entertainment industry favors DRM for films prior to their release), while other industries favor DLP (for example, the financial industry favors DLP when demonstrating compliance with GLBA). DLP is commonly found in audited environments that must show compliance with stated regulations and frequently remind users of appropriate behavior. DRM has been favored in environments where even one leak has the potential to be highly damaging.

DRM technologies allow for several levels of security. Functionality offered by DRM usually comprises:

- Prevention of unauthorized access to documents by strongly encrypting all instances of a file by default, and by granting permission only to those explicitly authorized by the document owner.
- Strong in-use protection, such as control of copy and paste, prevention of document screen shots, and limitations on printing.
- A rights model or policy that allows for easy mapping of business classifications to information.
- Offline use allowing for users to create or access DRM-sealed documents, without needing network access, for configurable periods of time.
- Full auditing of access to documents and of changes to the rights or policy by business users.

DRM works best in a disciplined organization that produces or controls a small number of very high-risk documents. Even if documents end up on personal clouds, or are stolen, their secrets remain hidden. There are instances where those tasked with protecting trade secrets may have to legally prove that they took reasonable care to protect them; when implemented correctly, modern DRM solutions protect document contents effectively. However, all copies of a document being secured must be protected throughout the document’s life cycle, since the loss of any unprotected version of the document has the potential to be highly damaging.
NSS Labs Findings

• Regulation and fear of litigation have been key drivers of DRM and DLP technologies. DLP is common in regulated environments that are frequently audited, while DRM technologies are commonly deployed in scenarios where data leaks are considered catastrophic.
• A document classification matrix is the foundation of a successful DRM launch.
• DRM is best suited for situations where sensitive documents will leave strictly controlled environments and will be shared with a small number of external users.
• Many DRM usability issues have been resolved, such as cross platform support, mobile support, external user authentication and offline reading mode.
• DRM possesses several strong document-centric controls that are superior to those of DLP (see “DRM Benefits” section of analyst brief “Keeping Secrets: Is it time for DLP or DRM?”).

NSS Labs Recommendations

• Ensure that the precursors for a successful DRM implementation are in place before attempting to launch a solution. Such precursors include a document classification matrix, IP location risk analysis, IP theft threat analysis, security awareness training, and buy-in from senior management.
• Implement user acceptance testing (UAT) of the DRM solution on all required platforms (PC, Mac and mobile) prior to solution purchase, as users are likely to circumvent onerous security technologies. Ensure that DRM policy infractions are appropriately dealt with.
• Enterprises that need to show compliance with regulations and also fully protect trade secrets will need to deploy both DLP and DRM systems.

Analysis

DRM is any technology that inhibits uses of digital content that are not desired or intended by the content provider. Modern DRM solutions embed protections directly into the documents themselves, in order to protect, control and track the documents on any device, in any location. Many DRM providers leverage DRM technologies that have been made available by Microsoft.

DRM Best Practices

Many of the best practices for DRM are similar for DLP (see analyst brief “12 Steps To DLP Best Practices”). To protect against data loss, it is critical that users receive training and take ownership of their data, that there is strong executive sponsorship, and that IT or IS has the ability to identify and protect current confidential data.

1) Prior to implementing a solution, create a document classification matrix. This should classify document types according to risk and is usually composed of either three or five classifications, with public data having a score of 1 and highly classified material having the highest rating. Each data classification should include mandatory controls that cover data protection while at rest and when in motion, with more sensitive data requiring
rigorous access and audit logs. Integrate this classification matrix with existing authentication systems, such as password, multifactor authentication (MFA) or single sign-on. This will ensure that only active accounts are able to access sensitive documents, and will also provide an audit trail from an official system of record (SOR).

2) Begin user education to obtain employee buy-in. This is critical to ensure protection of existing data and of newly created data. A risk-based approach is favored here, where those with regular access to confidential data should be thoroughly trained in their responsibilities. Users must understand the risk of data loss and the repercussions to their organization as a result of this data loss. Data owners must be responsible for appropriate labeling and protection of their data, and they should be familiarized with the relevant management-endorsed policies. In advance of deploying DLP or DRM systems, enterprises should attempt to manage contractor, partner and/or employee use of public cloud systems (for example, Dropbox and iCloud) for the storage of corporate data.

3) Identify where the existing data resides and how this data is classified. Interview executives and peers to understand data flows within and without the network. Examine controls and data stores currently in place. Seek out unprotected copies of confidential data; this data should be protected or deleted. Focus on first protecting the most sensitive category of data. In large enterprises, it is advisable to start with those highest risk documents that are most likely to be exposed to greater risk (for example, be sent to an outside entity, which is not fully trusted). Only when the most sensitive category of data has been protected throughout the enterprise, is it safe to move to the next tier.

4) Identify top data loss scenarios. Knowledge of where data is, what form it takes, and who has access to this data, will enable creation of tailored controls. These controls reduce the risk of data loss and lessen the damage of such data loss scenarios. This step requires a thorough understanding of business needs and practices, regulatory requirements, risk and likely repercussions of data loss. Be sure to clearly define the classes of violation, with real repercussions for offenders. Have documentation from HR, legal personnel, and senior management, which supports the stipulation that rule violations will result in appropriate penalties. Users working with highly sensitive data must ensure that all confidential work is protected by DRM, even when documents are in draft stage.

5) Ensure that data owners and IT can easily monitor sensitive file usage; this monitoring of usage will increase knowledge of data usage within the organization. DRM tools should also be leveraged to gain visibility over data flowing across internal networks and to the Internet.

6) DRM must be user-friendly. Requiring license verification each time a document is opened is good practice for high security documents, or for documents that need to be revoked instantly. However, be aware that requiring license checks creates access issues, since these documents can never be used offline. There is an element of risk in that a previously unauthorized user is able to access the documents during this window of time. Time windows should be configured according to a document’s sensitivity, and to an organization’s appetite for risk.

7) Review logs and alerts regularly and address suspicious events. Modern DRM solutions enable control of documents even after they have been sent outside the enterprise or downloaded to a recipient’s end-device. Document control enables users to specify granular control, which includes enabling or restricting recipients from viewing, printing, and copying content. Document permissions are dynamic (the document calls home to obtain updated permissions), and can be modified by the DRM administrator or document owner at any time. Document tracking enables users to follow documents after they have been sent. A full audit log details who opened the document, when, where, and on which device. Some solutions provide a geographic display that
shows exactly where a document is being opened. This feature helps prompt investigation if, for example, a sensitive document being accessed by a user at HQ is simultaneously being accessed using the same credentials at a different geographic location.

8) Regularly carry out a gap analysis that details the differential between the organization’s current risk level for data loss and the organization’s acceptable risk level. In DRM, it is often difficult to decide if there is an appropriate balance between protecting sensitive documents and keeping permissions appropriate. If additional rules, policies, training, procedures or technology are warranted, these can be implemented, once they are endorsed by executive stakeholders.

**Reading List**

*Keeping Secrets: Is It time For DLP or DRM?* NSS Labs
[https://www.nsslabs.com/reports/keeping-secrets-it-time-dlp-or-drm](https://www.nsslabs.com/reports/keeping-secrets-it-time-dlp-or-drm)

*12 Steps To DLP Best Practices.* NSS Labs
[https://www.nsslabs.com/reports/12-steps-dlp-best-practices](https://www.nsslabs.com/reports/12-steps-dlp-best-practices)
Contact Information

NSS Labs, Inc.
206 Wild Basin Rd
Building A, Suite 200
Austin, TX 78746 USA
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com

This analyst brief was produced as part of NSS Labs’ independent testing information services. Leading products were tested at no cost to the vendor, and NSS Labs received no vendor funding to produce this analyst brief.

© 2013 NSS Labs, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the authors.

Please note that access to or use of this report is conditioned on the following:

1. The information in this report is subject to change by NSS Labs without notice.

2. The information in this report is believed by NSS Labs to be accurate and reliable at the time of publication, but is not guaranteed. All use of and reliance on this report are at the reader’s sole risk. NSS Labs is not liable or responsible for any damages, losses, or expenses arising from any error or omission in this report.

3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY NSS LABS. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY NSS LABS. IN NO EVENT SHALL NSS LABS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

4. This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet the reader’s expectations, requirements, needs, or specifications, or that they will operate without interruption.

5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.

6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.