Making IRM work for you

HP Atalla Information Protection and Control
# Table of contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Why Information Rights Management (IRM)?</td>
</tr>
<tr>
<td>3</td>
<td>IRM engines vs. IRM enabler solutions</td>
</tr>
<tr>
<td>4</td>
<td>Tip 1: Choose your IRM engine vendor wisely</td>
</tr>
<tr>
<td>4</td>
<td>Tip 2: Take the user out of the equation (when possible)</td>
</tr>
<tr>
<td>5</td>
<td>Tip 3: Keep security in-line with enterprise policy</td>
</tr>
<tr>
<td>5</td>
<td>Tip 4: Maximize your coverage</td>
</tr>
<tr>
<td>5</td>
<td>Tip 5: How much integration is acceptable? Zero!</td>
</tr>
<tr>
<td>5</td>
<td>Tip 6: Make sure it’s application-agnostic</td>
</tr>
<tr>
<td>5</td>
<td>Tip 7: Entitlement management integration</td>
</tr>
<tr>
<td>6</td>
<td>Tip 8: Compliance is king. Bow down!</td>
</tr>
<tr>
<td>6</td>
<td>Tip 9: Do not hinder ECM and DMS productivity.</td>
</tr>
<tr>
<td>6</td>
<td>Tip 10: Is protection dynamic?</td>
</tr>
<tr>
<td>6</td>
<td>Tip 11: The content that was</td>
</tr>
<tr>
<td>6</td>
<td>Tip 12: Must have: powerful reporting tools</td>
</tr>
<tr>
<td>7</td>
<td>Tip 13: SIEM/SOC compatibility</td>
</tr>
<tr>
<td>7</td>
<td>Tip 14: Anti-tampering</td>
</tr>
<tr>
<td>7</td>
<td>Tip 15: Continuous health monitoring</td>
</tr>
<tr>
<td>7</td>
<td>Tip 16: Antivirus and antimalware</td>
</tr>
<tr>
<td>7</td>
<td>Tip 17: It’s a BYOD world</td>
</tr>
<tr>
<td>7</td>
<td>Tip 18: Get the most for your money</td>
</tr>
<tr>
<td>10</td>
<td>The HP Atalla IPC Solution</td>
</tr>
<tr>
<td>10</td>
<td>The HP Atalla Information Protection and Control</td>
</tr>
</tbody>
</table>
HP Atalla Information Protection and Control

HP Atalla Information Protection and Control (IPC) Suite solves the complex challenge of providing data classification and data security by providing organizations the means to bring protection to the data itself. HP Atalla IPC applies protection at a point where information is created and makes that protection persistent, so it follows the information wherever it goes. This protects sensitive data no matter where it actually resides.

Why Information Rights Management (IRM)?

Never before has enterprise IT enabled such extreme productivity. In the borderless social enterprise, more data is shared between more people in more places, resulting in a radically more creative and collaborative work environment. This open world of sharing has facilitated a revolution both in business and society.

It has also created unprecedented dangers. Because the consumerization and externalization of IT have made traditional information security models obsolete. Perimeter defenses were relevant when IT environments could be segregated. Today, where information resides and from what device it is accessed is irrelevant. The only relevant question is: Who can access it?

As the unique dangers of the borderless enterprise became apparent, forward-thinking chief information security officers (CISOs) have turned from perimeter-centric information security paradigms like data leakage prevention (DLP) to data-centric security paradigms like Information Rights Management (IRM). IRM relates to the security of data as data, wherever it is—in motion, at rest, or in use.

IRM engines vs. IRM enabler solutions

If you are reading this, you are probably either considering or already implementing an IRM system. And you are probably also aware that existing IRM platforms lack many key attributes that you would expect to see in an enterprise-level tool that provides security without impeding productivity.

The good news is that there’s a reason for this. Existing IRM platforms like Microsoft® Active Directory Rights Management Services (AD RMS) are just that: platforms. We call them IRM Engines, because they are the engine of the car, not the amenities.

To complete the vehicle, you need to add the seats, steering wheel, air conditioning, and thousand other bells and whistles that turn the IRM vehicle from a locomotive that is captive on predefined tracks into a Cadillac that can convey you over any road in safety and comfort. We call this package of amenities—many of them truly mission-critical amenities—the IRM Enabler Solution.

There are numerous IRM Enabler Solutions on the market. The challenge is to choose the solution that can be most effectively integrated into your existing business processes and IT environment, without hindering workflow or productivity. To help you choose an IRM Enabler Solution that will work for you, and not the other way around, we have put together the following list of tips.
Tip 1: Choose your IRM engine vendor wisely

Before we even talk about your IRM Enabler Solution, let’s consider what IRM Engine you choose.

By definition, you will be granting the “keys to your castle” to your IRM Engine vendor. Make sure the company you choose is reliable, stable, and known. More importantly, make sure your vendor has shown a long-term, unwavering commitment to IRM.

Some big players, notably Oracle, have abandoned the model, and left invested users hanging.

Other smaller players have great technical and attractive business models—but can you be sure they will be around tomorrow? In reality there is only one player that can currently answer all these criteria: Microsoft.

Tip 2: Take the user out of the equation (when possible)

From both a security and usability point of view, IRM protection should be seamless and automatic, whenever possible.

To this end, choose a classification-based IRM Enabler Solution. Classification should be intelligent and flexible enough to deliver the full scope of data classification and data protection options—from automatic classification, which can identify data seamlessly, through content and context attributes, via system recommendations, including user-based classification and empowering authorized data owners to be responsible for applying their own appropriate classifications.
Tip 3: Keep security in-line with enterprise policy

Everything your enterprise does is driven and defined by policy. Security, and specifically your IRM solution, should be no different. To achieve the precise level of protection that your organization requires and keep security in-line with business goals, your IRM Enabler Solution should be policy based. In addition to being driven by enterprise decisions, your solution of choice should be flexible and agile enough to align with both data classification and policy standards—current and future.

Tip 4: Maximize your coverage

There is life beyond Microsoft Office. Your IRM Enabler Solution should cover information from all enterprise productivity tools.

IRM protection should be applied to all types of sensitive information—from any source, at any stage of the data lifecycle—not just from Microsoft Office applications. Your IRM Enabler Solution should of course protect unstructured information. Moreover, it should be able to deal with the reality that even structured information does not necessarily remain structured. For example, you may be confident that your customer resource management (CRM) system is effectively protected. But what about reports generated by that system? Are there other enterprise-level systems whose day-to-day usage puts your sensitive information at risk?

Tip 5: How much integration is acceptable? Zero!

Especially for broad-scope end-user systems like IRM-integration with existing and future systems is a resource drain and productivity-killer.

It is mission-critical for your IRM solution to work seamlessly and scalable with any existing and future enterprise systems. Sensitive information can originate in hundreds or even thousands of applications—from Enterprise Resource Planning (ERP) systems like SAP®, through CRMs like salesforce.com, to Enterprise Content Management (ECM) repositories, on premises or off premises, and beyond. Make sure your IRM Enabler Solution is based on a model that can seamlessly integrate with any possible source, and any number of diverse sources, today and in the future.

Tip 6: Make sure it’s application-agnostic

Many IRM solutions are completely application-dependent and not enough applications in use are IRM-ready.

Secure content needs to be accessible, and seamlessly usable, by authorized parties even in non-IRM-enabled applications. Make sure your IRM Enabler Solution delivers transparent access to sensitive information to authorized users of any application—without clumsy workarounds like changing file extensions and without affecting workflow.

Tip 7: Entitlement management integration

Protect your investment in entitlement management!

You may have already invested, or be considering investing, in entitlement management software. Alternately, you may be using the existing entitlements module of your line of business (LOB) apps. Either way, IRM can still be an excellent complement to your security toolbox, helping administer the complex world of enterprise authorizations, privileges, access rights, permissions, and rules.

However, you need to make sure that the same access and permissions that are used in the application, share, or document library (or other entitlement sources) will propagate also to IRM-protected data assets—without replicating permission models.
Tip 8: Compliance is king. Bow down!

Everything you do needs to be compliance-ready, including IRM.
When choosing an IRM Enabler Solution, make sure IRM-protected content can still be indexed and searched by journaling software like Symantec Enterprise Vault, HP Autonomy, and other compliance-focused products.

Tip 9: Do not hinder ECM and DMS productivity.

Safeguard investments in enterprise content management (ECM) and document management systems (DMS), and keep workflows moving.
To maintain security and compartmentalization, sensitive information should remain protected even when stored in secure ECM/DMS systems like Microsoft SharePoint, OpenText, Documentum, and more. This is especially clear in light of recent authorized super-user breaches that happened in a leading security agency. However, to maintain peak productivity, make sure your IRM-protected content can be seamlessly indexed, searched, and accessed via these systems.

Tip 10: Is protection dynamic?

As context changes, the sensitivity of information changes.
Once protected by your IRM Enabler Solution, make sure your sensitive information can be made more widely available when relevant—automatically and according to centrally managed policy.
For example, can the security and data classification of corporate financial statements be automatically revised enterprise-wide once a “quiet period” has passed, or does this need to be done manually? Can the protection of a document be extended transparently when a data owner sends it to a third party, who was not originally included in the permission list?

Tip 11: The content that was

There was life before IRM.
You have millions of files in your repositories, generated long before your IRM solution came online. What about them? Your IRM Enabler Solution of choice should seek out and protect content generated in the past, as well ensuring the data security of newly generated items.

Tip 12: Must have: powerful reporting tools

For auditing, compliance, and policy-making—powerful reporting capabilities are crucial.
In today’s regulatory and security environment, keeping data security policies in-line with real-world usage, quantifying exposure (internal and external) for effective risk assessment, and maintaining strict auditing, usage trend analysis and forensics capabilities are mission critical.
Make sure your IRM Enabler Solution is up to speed from a reporting point of view.
Tip 13: SIEM/SOC compatibility

Ensure that your IRM Enabler Solution works with your security dashboard.

To avoid multiple points of control for key security systems, you have probably invested in a security information and event management (SIEM) or security operations center (SOC) solution. Treat your IRM Enabler Solution just like any other mission-critical security system, and make sure it integrates seamlessly with your SIEM/SOC of choice.

Tip 14: Anti-tampering

Any security solution needs to be secure itself.

To enforce any kind of policy-derived security, it is important to eliminate the possibility of end user tampering. Make sure your IRM Enabler Solution has solid anti-tampering mechanisms that systematically ensure continuous operation, and alert you if end users try to disable agents—whether maliciously or accidentally.

Tip 15: Continuous health monitoring

Policy-derived security has to run 24x7x365.

Since your IRM Enabler Solution will be performing mission-critical enterprise functions, make sure that it contains health and operation monitoring components to maintain maximum control over all IRM modules from a centralized location.

Tip 16: Antivirus and antimalware

Network threats still exist, even when information is protected.

Viruses and malware can exploit the use of IRM-protected data to disguise malicious actions, and targeted attacks could easily do the same. Make sure your IRM-protected content remains fully accessible to key network- and host-based data security utilities like antivirus and antimalware.

Tip 17: It’s a BYOD world

Ensure seamless productivity in the bring your own device (BYOD) IT environment.

In the BYOD era, you need to guarantee that IRM-protected content can be accessed on any device, including mobile. Also, to ensure maximum productivity on the go, your IRM Enabler Solution needs to work seamlessly with mobile device management (MDM) solutions like Good Technology, AirWatch, MobileIron, and others.

Tip 18: Get the most for your money

Like any high-end purchase, your IRM Enabler Solution should exceed expectations.

In today’s budget-sensitive IT climate, flexible, multi-purpose solutions that deliver the most “bang for your buck” are the rule. Make sure the IRM Enabler Solution you choose can do more than “just” IRM. A multi-purpose IRM Enabler Solution should be able to offer hybrid, borderless DLP functionality. It should offer cloud security, secure collaboration, and information sharing. And, it goes without saying that it should be organically compatible with the whole of your perimeter-free security environment.
The HP Atalla IPC Solution

In today’s tight security climate, it is commonly agreed that effective data protection requires encryption, and that access should be restricted “on a need-to-know basis.”

The IQProtector engine makes use of an innovative security paradigm: on creation or usage data classification, and enforcement. Interception, classification, enforcement, and discovery, all take place at data creation, whether by applications or by users and at any user interaction with data. At the moment, that data is created or manipulated, on user’s endpoints or on servers. IQProtector intelligently identifies and classifies the data based on context and content criteria (the Atalla IPC information classification prism) and according to a centrally governed security policy.

IQProtector leverages Microsoft Active Directory Rights Management Services (AD RMS) to apply IRM protection to the data according to the policy.

Persistent file protection

IQProtector embeds protection within the data itself at the moment of creation—instantly identifying, classifying, and persistently tagging all new, modified, or accessed sensitive data from any origin.

Context and content-sensitive IQProtector applies data classification and AD RMS protection to emails, documents, or other files tagged as sensitive—applying AD RMS according to a customizable security policy. Leveraging existing Microsoft AD RMS and encryption frameworks, Atalla IPC intelligently generates, applies, and enforces encryption policies enterprise-wide.
For example, early stages of a new design are classified as such and the protection limits the access to a limited group of authorized users. As the project develops to more advanced stages, its classification is also adjusted, and due to that, its protection is adjusted to include a larger and different group of authorized users. Such changes to classification and information protection are applied in a managed way by authorized personnel or automatic processes. This enables an organization to achieve any desired balance between security needs and business continuity.

- All sensitive information and reports that are exported from any design, manufacturing, or sketching application can be intercepted automatically—even before the end user gets hold of it—and according to the defined organization policy be classified, encrypted with usage rights enforced.

- IQProtector data classification and protection policy is dynamic and adaptive, and may be configured to change throughout the data's information lifecycle according to changing security risks and business needs.

The HP Atalla IPC concept is channel and medium agnostic, meaning you stop running after the data that exists and perform plumbing-like activities, trying to stop sensitive data from leaving the organization. When information is protected at creation, it reaches the end user already protected without any chance of tampering with the data. You can gain the benefit of sensitive data internal compartmentalization as a complementary tool for continuous data classification and encryption.
The HP Atalla Information Protection and Control

HP Atalla Information Protection and Control solutions provide the enterprise with:

- **File and mail classification:** Classify file and email data items either automatically or manually based on the Atalla IPC information classification prism for data originating from any source (user, applications, cloud services, and more) according to corporate policy. Classification also allows adding visual classification to Microsoft Office and emails in order to raise users’ awareness on data sensitivity.

  The classification policy can be configured to require user input to raise the automatically assigned security level manually, where the data type, content, and context are insufficient parameters for a meaningful classification.

- **File and mail automatic protection:** IQProtector applies Microsoft AD RMS protection to files and mails based on the data item classification and according to the corporate security policy. Protection is applied automatically and transparently, with no operational disruption.

  The AD RMS protection includes encryption and a security policy of permissions (such as view, edit, print, extract), per user or user group, according to the organizational policy for the specific data type. However, unlike traditional access control lists (ACLs), which are location-specific, AD RMS is embedded in the data itself and goes with the data. The permissions policy may be subsequently changed by IQProtector itself in accordance with the organizational policy and the business process.
• **Secured mail collaboration:** IQProtector collaboration rules are classification- and protection-aware allowing the corporate to help ensure that only authorized users collaborate authorized data to authorized recipients inside and outside the corporate. Such collaboration rules may adapt the classification and protection of data items, block specific items from being sent or accessed, or strip data item from its protection based on the corporate security policy and business needs.

• **Application protection:** IQProtector classifies and protects unstructured data in Web applications applying AD RMS rights within the Web application page (copy, print, etc.). IQProtector intercepts documents and reports generated and downloaded from any Web- or client-based applications without any need for integration allowing continuous protection for data beyond application boundaries.

• **Mobile support for AD RMS:** Enables secure collaboration on RMS-protected emails and attachments on all major mobile devices and operating systems (iOS, BlackBerry, and Android).

• **Non-intrusive data discovery:** IQProtector tracking and logging capabilities can be used to discover where the organization sensitive data is located. No data center deployment or intrusive scanning is needed. Instead, IQProtector monitors data usage and locates the data sources. The discovery results enable designing an effective and non-interruptive IQProtector security policy.

• **Data usage discovery for granular policy design:** IQProtector tracking and logging capabilities can be used to discover how data is used in the organization: who is using which data, to whom are they sending it, and where are they saving it. Differentiating between legitimate business practices and usage, which should be prevented, enables organizational security officers to formulate a granular policy meaningfully, defining who should be allowed access and to what information.

• **Comprehensive data usage auditing:** The entire information lifecycle, from creation, through distribution and storage, is fully audited to supply security officers with comprehensive information about compliance to privacy, state, and industry regulations. Known security breaches can be tracked by identifying the usage of the leaked data.

• **Transparent assimilation in IT environment:** Trusted applications like data loss prevention (DLP), antivirus (A/V), or search engines can still access encrypted data seamlessly without integration efforts. IQProtector enables ECM, DLP, antivirus, and other enterprise IT systems to inspect, index, and classify encrypted content—preserving investment in existing systems.
**HP Atalla IPC key benefits**
Delivers data classification and automated data protection

- **Proven classification accuracy**
  - Powered by content and context analysis

- **Multi-disciplinary classification mechanisms**
  - User, system recommendation, automatic source-based between data source and destination

- **Optimized classification cycle**
  - Triggered by captured events (open, close, save, upload, download, copy, etc.)

- **Full analytics of data usage events**
  - For all classification attributes; for enforcement, reporting, and audit

- **Persistent protection wherever the data travels**
  - Protection injected at the point of creation and travels with the data throughout its lifecycle

**Learn more at**
hp.com/go/AtallaIPC

---

**Sign up for updates**
hp.com/go/getupdated

© Copyright 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft is a trademark of the Microsoft group of companies. Oracle is a registered trademark of Oracle and/or its affiliates. SAP is the trademark or registered trademark of SAP SE in Germany and in several other countries.

4AA5-7732ENW, April 2015