Making **IRM** Work for You

Yuval Eldar, CTO

September 2014

secure islands

Why 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 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.

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 tech and attractive business models – but can you be sure they'll be around tomorrow? In truth, there's 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.

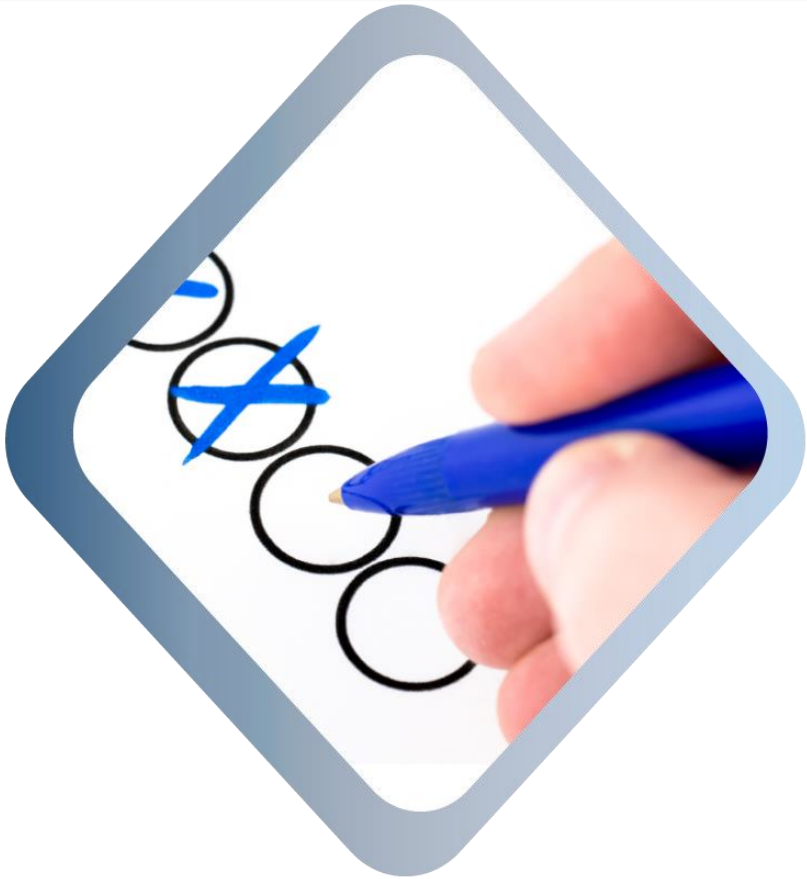
To this end, choose a classification-based IRM Enabler Solution. Classification should be intelligent, and flexible enough to deliver the full scope of classification options - from automatic classification which can identify data seamlessly through content and context attributes, via system recommendations,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

secure islands

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 classification and policy standards - current and future.



Tip 4: Maximize Your Coverage

There is life beyond MS 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 MS 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 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?

secure islands

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 scale with any existing and future enterprise systems. Sensitive information can originate in hundreds or even thousands of applications – from ERP systems like SAP, through CRMs like Salesforce.com, to 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.

secure islands

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 impacting workflow.

secure islands

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 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 which are used in the application/share/document library (or other entitlement sources) will propagate also to IRM-protected data assets - without replicating permission models.

secure islands

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.

secure islands

Tip 9: Don’t Hinder ECM & 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 MS SharePoint, OpenText, Documentum, and more. This is especially clear in light of recent authorized super-user breaches like that of NSA sub-contractor Edward Snowden. However, to maintain peak productivity, make sure your IRM-protected content can be seamlessly indexed, searched and accessed via these systems.

secure islands

Tip 10: Is Protection Dynamic?

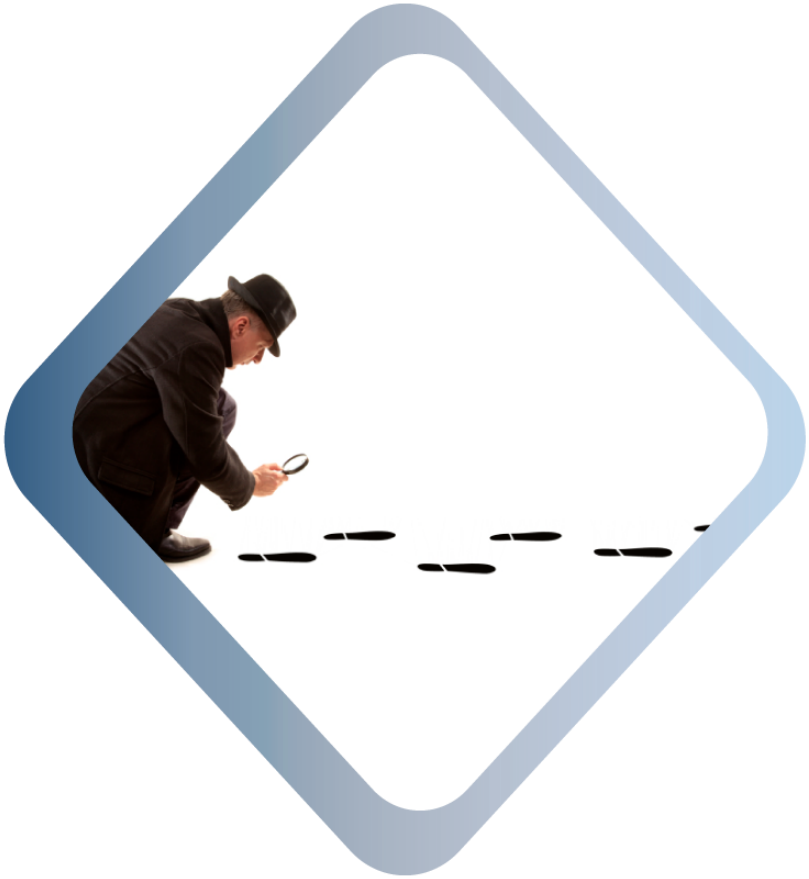
As context changes, the sensitivity of information changes.

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 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 security of newly-generated items.



secure islands

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 security policy 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.

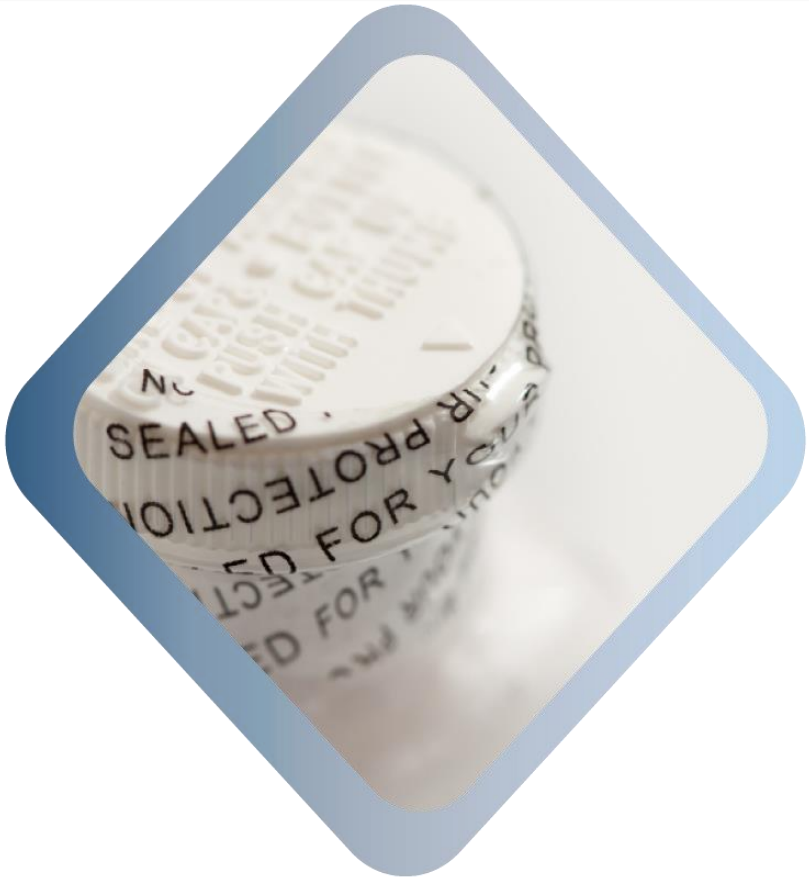
To avoid multiple points of control for key security systems, you have probably invested in a SIEM or SOC solution. Treat your IRM Enabler Solution just like any other mission-critical security system, and make sure it integrates seamlessly with your SIEM\SOC of choice.

secure islands

Tip 14: Anti-Tampering

Any security solution needs to be secure itself.

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



secure islands

Tip 15: Continuous Health Monitoring

Policy-derived security has to run 24/7/365.

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.

secure islands

Tip 16: Anti-Virus and Anti-Malware

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 security utilities like anti-virus and anti-malware.

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, AirWatch, MobileIron, and others.

secure islands

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, it should be organically compatible with the whole of your perimeter-free security environment.

secure islands

Conclusion

IRM has the potential to enable a new level of information security for your enterprise. However, mainstream IRM Engines are not sufficiently featured to smoothly integrate into existing business processes.

When choosing an **IRM Enabler Solution**, both security and productivity should be considered. An enduser-facing security solution is only as effective as its weakest link: the enduser. And today's endusers present a world of previously-unthinkable demands. They need to work from their device of choice, on their productivity tools of choice – and, for them, security considerations are secondary, at best. By choosing an IRM Enabler Solution that smoothly integrates into existing workflow and delivers the cutting-edge information security that your enterprise needs, you can enjoy the best of both worlds.

About Secure Islands

Secure Islands develops and markets advanced Information Protection and Control (IPC) solutions for the borderless enterprise. Offering policy-driven classification and protection for unstructured data, Secure Islands lays the foundation for sensitive information security in enterprises as they shift from perimeter defense to persistent protection. Secure Islands' holistic approach literally redefines information security and assists the enterprise in regaining control by identifying, classifying and protecting sensitive information throughout its lifecycle. Founded in 2006 and headquartered in Israel, the company's solutions are deployed in top-tier Fortune 500 firms and government agencies worldwide. For more information, please visit www.secureislands.com.

secure islands