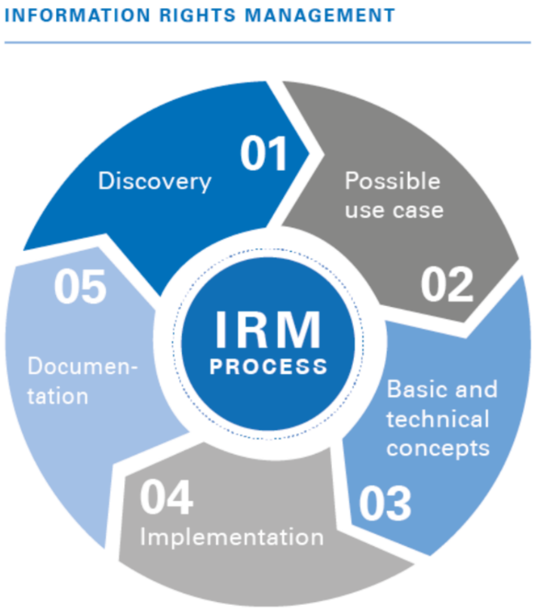
Using Check Point's Capsule Docs with Data Loss Prevention to achieve IRM

Jason Pena
Security Engineer
12-4-18

In today's digital world, protecting your company's assets is paramount. Hackers are always on the hunt for ways to exfiltrate your data and cause havoc on your network. Whether it is for monetary, political, or personal reasons, there is always a threat to your data. A systematic approach to protecting company data that is used by security-minded people is called Information Rights Management (IRM). With IRM companies practice imposing technological restrictions that governs what users can do with digital media. When a solution designed to prevent you from copying, printing, or even sharing a document you are being restricted using IRM. Finding the right security solution to protect your assets can seem challenging but with Check Point Software, leveraging data loss prevention (DLP) and document encryption (Capsule Docs) your company has the best of both worlds. Therefore, if a document becomes exposed you can rest assured that it will provide zero visibility into what a malicious hacker really wants to see.

What is Information Rights Management?

Information Rights Management, also known as 'IRM', is a term used in relation to Digital Rights Management (DRM) - technologies that protect sensitive information from unauthorized access. IRM focuses on business documents and emails sent across the wire and adding encryption to enhance security. Once encryption is set, an IRM user can add access permissions to a document (i.e. read/write, print, or copy/paste). In order to determine what assets a company wants to protect there are processes users can follow. A sample IRM process is illustrated as follows (Graph 1):



Graph 1 – IRM Process (TUV Rheinland)

How IRM is implemented using Check Point Software?

Check Point offers unique solutions that provide access control to data that sits at rest or is in transit using DLP controls. With Capsule Docs organizations can seamlessly protect documents, ensuring access for authorized users only. Business sensitive documents are encrypted to ensure the contents are protected wherever they go. Capsule Docs defines who can view the document and what they can do with it. Adding DLP to the mix allows the company to flag documents sent thru the organization and apply Capsule Docs file protections or add Watermarks for tracking.

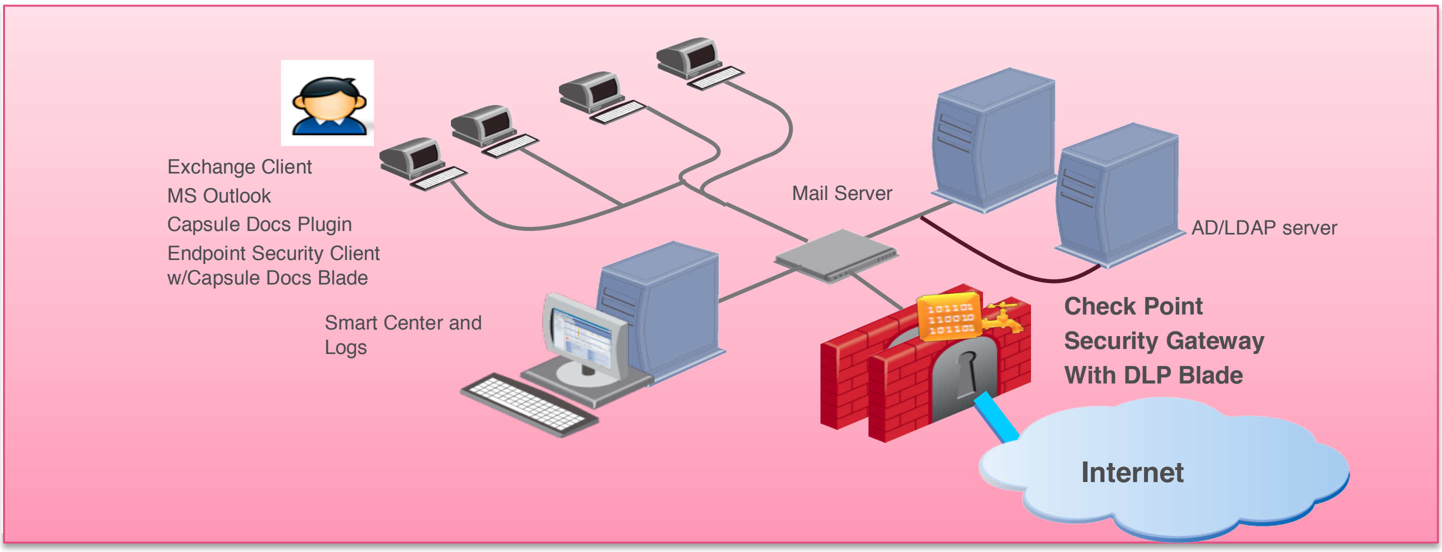
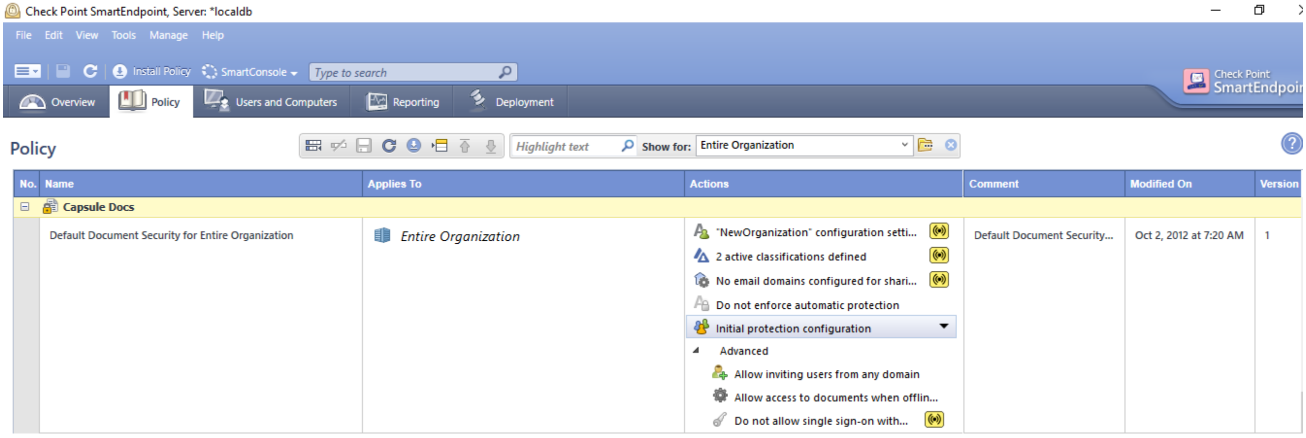


Figure 1. – Check Point Capsule Docs & DLP solution overview

The Check Point Solution

- **Capsule Docs**
  - Using the R80.20 SmartEndPoint Console navigate to Policy->Capsule Docs (Figure 2)



No.	Name	Applies To	Actions	Comment	Modified On	Version
	Capsule Docs					
	Default Document Security for Entire Organization	Entire Organization	"NewOrganization" configuration setti... 2 active classifications defined No email domains configured for shari... Do not enforce automatic protection Initial protection configuration Advanced Allow inviting users from any domain Allow access to documents when offlin... Do not allow single sign-on with...	Default Document Security...	Oct 2, 2012 at 7:20 AM	1

Figure 2. – Check Point SmartEndpoint Console Policy Configuration

  - Configure the Capsule Docs Policy to enforce the configuration established by your company's standards.
  - These settings will ensure that any document traversing in and out of your network will be encrypted and will carry the restrictions set forth by the administrator (Figure 3)

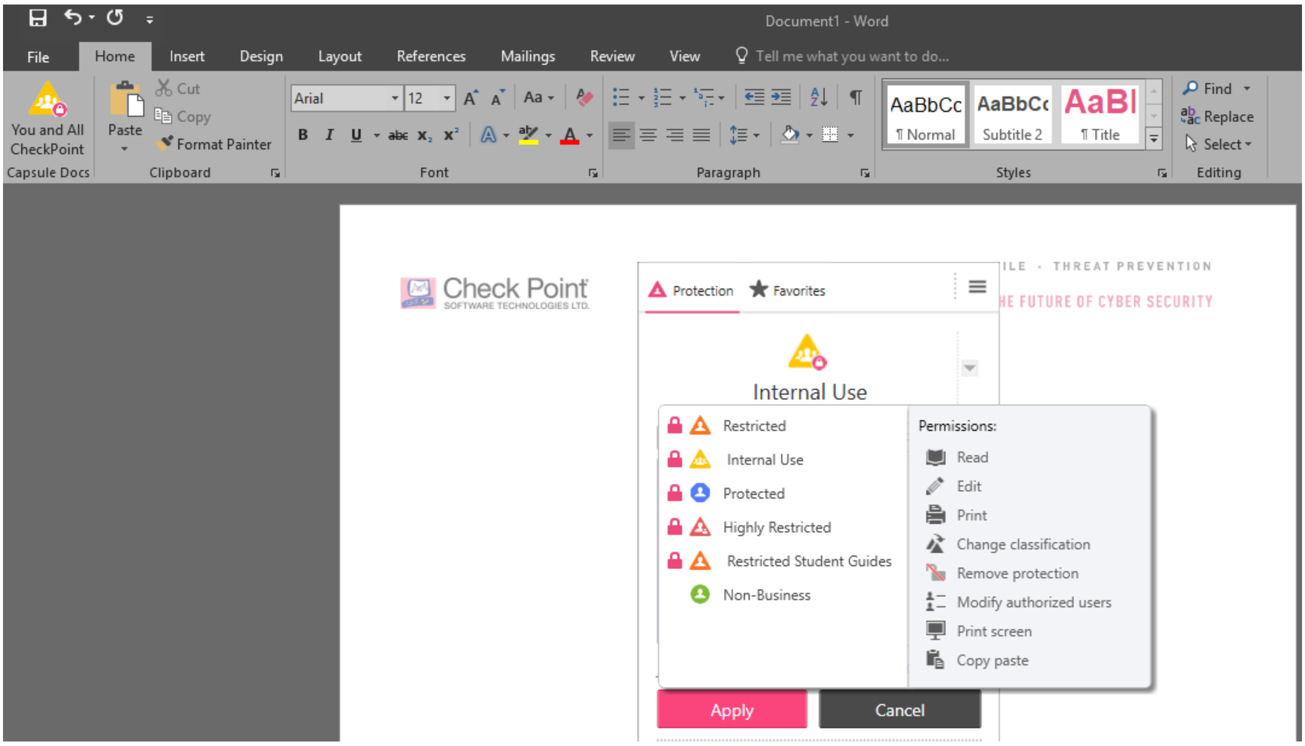
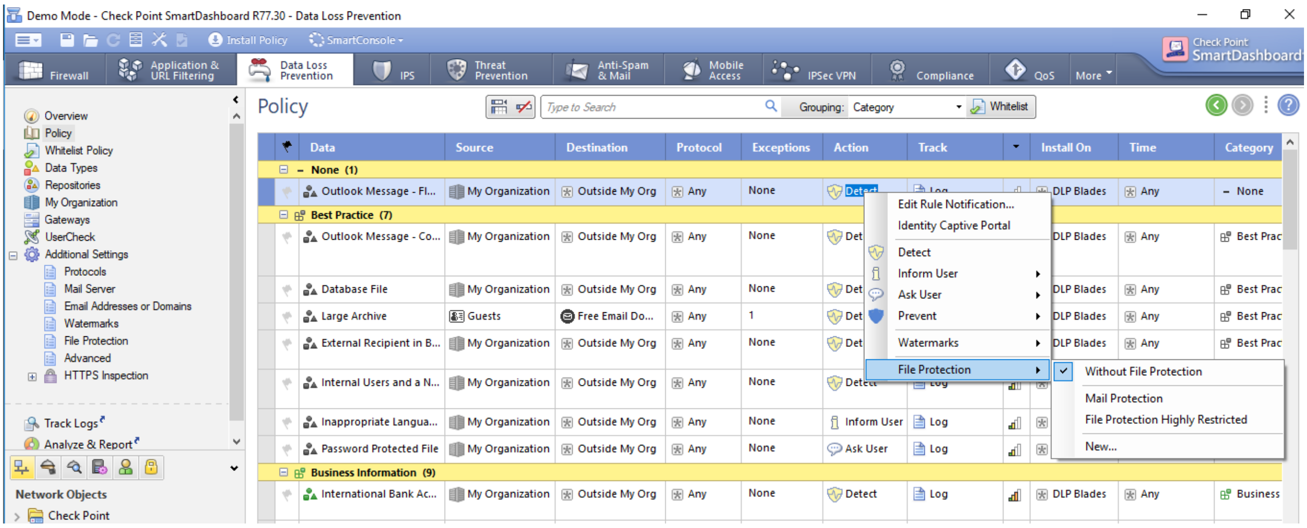


Figure 3. – Microsoft Word document with the Capsule Docs plugin installed

**Please Note that Capsule Docs is deployed as part of the Check Point Endpoint solution or as a standalone product. For more details please go to - https://www.checkpoint.com/products/capsule-docs/*

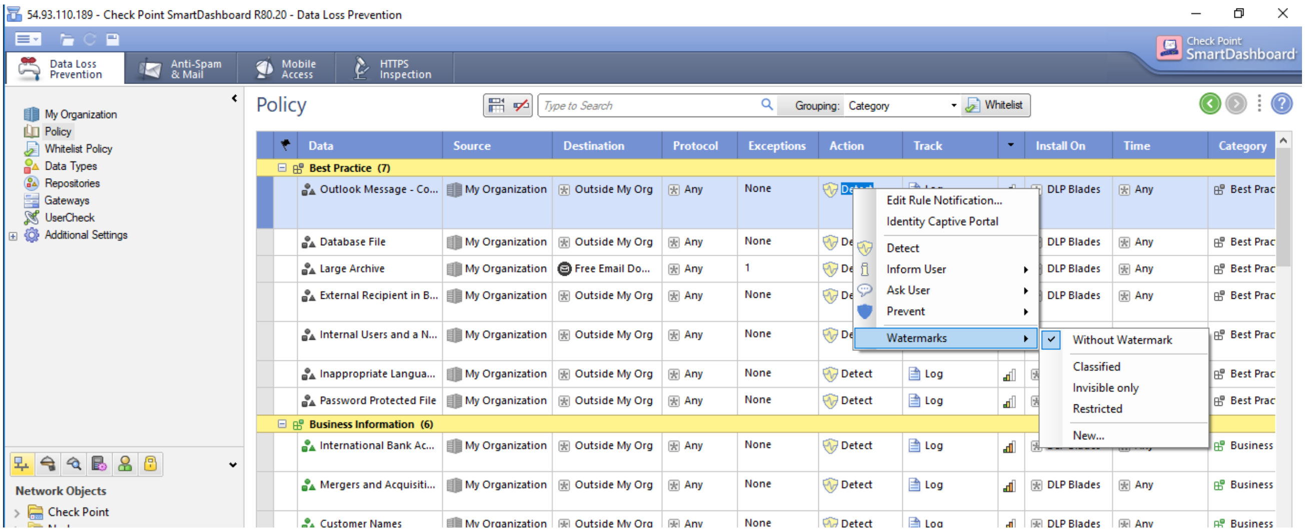
- **DLP Integration with Capsule Docs**
  - With Check Point's DLP solution, security administrators can add an extra layer of protection by analyzing data without encryption and adding Capsule Docs file protection(s) or by using Watermarks.
  - Using the R80.20 SmartConsole go to Manage & Settings -> Blades -> DLP->Policy
  - Create a new Data Type Rule and under Action select File Protection-> *Select the protection defined in Advanced Settings* (Figure 4)
  - You can customize the file protection to add specific classifications to documents to apply access restrictions post encryption.



Data	Source	Destination	Protocol	Exceptions	Action	Track	Install On	Time	Category
None (1)									
Outlook Message - Fl...	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	None
Best Practice (7)									
Outlook Message - Co...	My Organization	Outside My Org	Any	None	Det		DLP Blades	Any	Best Prac
Database File	My Organization	Outside My Org	Any	None	Det		DLP Blades	Any	Best Prac
Large Archive	Guests	Free Email Do...	Any	1	Det		DLP Blades	Any	Best Prac
External Recipient in B...	My Organization	Outside My Org	Any	None	Det		DLP Blades	Any	Best Prac
Internal Users and a N...	My Organization	Outside My Org	Any	None	Detect	Log			
Inappropriate Langua...	My Organization	Outside My Org	Any	None	Inform User	Log			
Password Protected File	My Organization	Outside My Org	Any	None	Ask User	Log			
Business Information (9)									
International Bank Ac...	My Organization	Outside My Org	Any	None	Detect	Log	DLP Blades	Any	Business

Figure 4. – SmartConsole DLP Policy. Configuring File Protection

  - To add Watermarks to a document change the action to Watermark and select one of the following (Figure 5):
    - **Classified** – Tags a document with the word Classified
    - **Invisible Only** – Adds an hidden (encrypted) watermark for forensics and tracking
    - **Restricted** – Adds the word Restricted to the document and allows for additional data fields – i.e. sender, recipient, and date



Data	Source	Destination	Protocol	Exceptions	Action	Track		Install On	Time	Category
Best Practice (7)										
Outlook Message - Co...	My Organization	Outside My Org	Any	None	Det			DLP Blades	Any	Best Prac
Database File	My Organization	Outside My Org	Any	None	De			DLP Blades	Any	Best Prac
Large Archive	My Organization	Free Email Do...	Any	1	De			DLP Blades	Any	Best Prac
External Recipient in B...	My Organization	Outside My Org	Any	None	De			DLP Blades	Any	Best Prac
Internal Users and a N...	My Organization	Outside My Org	Any	None	De					Best Prac
Inappropriate Langua...	My Organization	Outside My Org	Any	None	Detect	Log				Best Prac
Password Protected File	My Organization	Outside My Org	Any	None	Detect	Log				Best Prac
Business Information (6)										
International Bank Ac...	My Organization	Outside My Org	Any	None	Detect	Log				Business
Mergers and Acquisiti...	My Organization	Outside My Org	Any	None	Detect	Log		DLP Blades	Any	Business
Customer Names	My Organization	Outside My Org	Any	None	Detect	Log		DLP Blades	Any	Business

Figure 5. – SmartConsole DLP Policy. Adding the Watermark action to a DLP rule

Conclusion

Realizing Information Rights Management takes diligence and a solution that covers all bases. When it comes to your most sensitive business data, device-level security may not provide enough protection. With Check Point Capsule Docs and DLP, companies use a secure mobile document management system that lets you secure the document itself, creating access and usage controls that follow the document wherever it goes, for the entirety of its lifecycle. Providing hackers no visibility into the data they want to leak.

References

- *https://www.defectivebydesign.org/what_is_drm_digital_restrictions_management*
- *https://www.checkpoint.com/downloads/products/capsule-docs-datasheet.pdf*
- *Check Point Wiki – Capsule Docs Technical FAQ*
- *Check Point R80.20 SmartConsole*
- *Check Point R77.30.03 SmartEndpoint Console*
- *sk103706*
- *https://www.tuv.com/slovakia/en/information-rights-management.html*
- *https://en.wikipedia.org/wiki/Information_rights_management*