

Het beveiligen van ongestructureerde data: We zien door de bomen het bos niet meer.....

## DLP en IRM .. wat kan de combinatie doen?

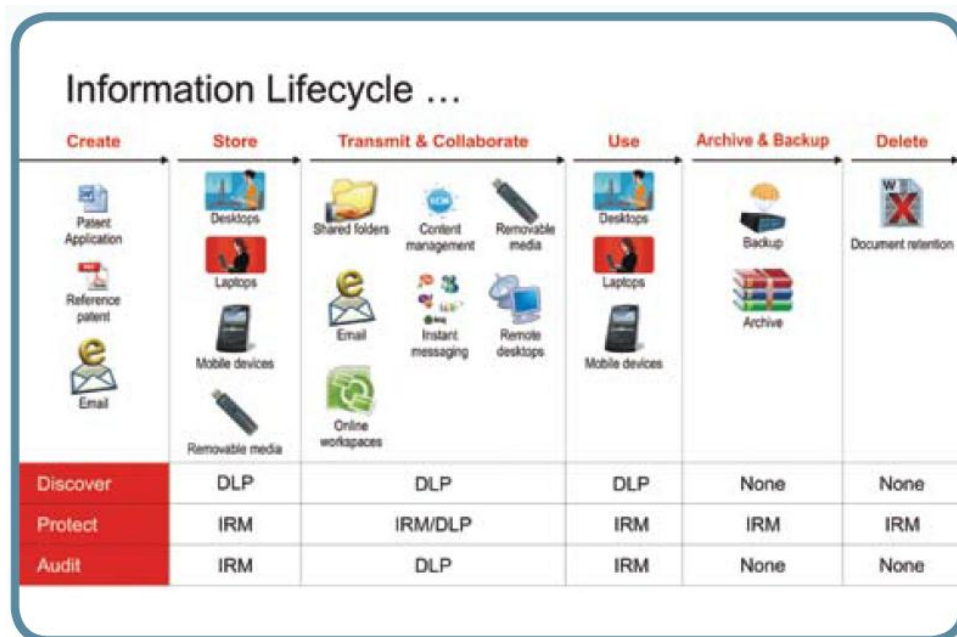
In het beveiligen van ongestructureerde gegevens is een hoop verwarring over welke technologie het beste kan worden toegepast in welke context. DLP en IRM oplossingen kunnen gecombineerd worden om organisaties zo het meeste rendement te geven op hun investeringen in de zin van betere, effectievere beveiliging tegen een lagere prijs.

-----

In de afgelopen paar jaar is een hoop marketingeuro's besteed aan verschillende oplossingen voor het beschermen van ongestructureerde informatie (e-mails, documenten, ontwerpen, tekeningen, ...) van de onderneming. Oplossingen variëren van basis poortblokkering technologieën die gebaseerd zijn op het beheersen van USB, DVD's en andere opslagmedia tot high-end Data Loss Prevention (DLP) en Information Rights Management (IRM) technologieën. Voor de leek is er veel verwarring over welke technologie past in welke zakelijke context en behoefte.

Wat is nu het probleem van het beveiligen van ongestructureerde informatie. Ongestructureerde informatie doorloopt een levenscyclus van creëren – opslaan – verzenden / samenwerken – gebruiken – archiveren – verwijderen. Binnen deze levenscyclus ontstaan er specifieke risico's, waardoor vertrouwelijke informatie gecompromitteerd kan worden. De behoefte aan informatiebeveiliging van een onderneming wordt bepaald door deze risico's en in welke mate men deze risico's wil wegnemen of de gevolgen van dit risico wil reduceren.

In de onderstaande figuur is de levenscyclus van informatie afgebeeld en hierbinnen worden de specifieke risico's benoemd met de mogelijke maatregelen.



Teneinde ongestructureerde informatie effectief te kunnen beschermen, dient de onderneming over de volgende mechanismes te beschikken:

- Men dient de mogelijkheid te hebben om in kaart te brengen waar de vertrouwelijke documenten zich bevinden (discover). Uit onderzoek is gebleken dat 85% van de ondernemingen geen of geen volledig beeld heeft waar de vertrouwelijke documenten zijn opgeslagen (mail, file-shares, lokale schijf, USB stick, Cloud etc);
- Men dient de mogelijkheid te hebben om deze informatie vervolgens te beveiligen op een zodanige wijze dat de beveiliging geen blokkering vormt voor informatie-uitwisseling binnen een geoorloofde samenwerkingsverband;
- Men dient de mogelijkheid te hebben om de activiteiten die plaatsvinden op de vertrouwelijke documenten vast te leggen in een audit trail.

Deze functionaliteit wordt geboden door een gecombineerde DLP-IRM oplossing. Allereerst wordt in het kort uitgelegd wat een DLP systeem doet. Vervolgens wordt beschreven wat een IRM systeem is. Tot slot wordt de kracht van de combinatie van beide technologieën toegelicht.

**Wat is een DLP-systeem:** Een content-aware DLP systeem brengt de documenten in kaart, die zich bevinden op verschillende locaties, zoals desktops, fileservers en databases. Het classificeert deze documenten in verschillende 'archieven' op basis van centraal vastgestelde inhoudspatronen. Het bewaakt en volgt deze informatiestroom op basis van centraal vastgesteld beleid. In het volgende voorbeeld wordt de werking van een DLP systeem uitgelegd aan de hand van een document met persoons- en creditcard gegevens. Een DLP systeem zal:

1. de aanwezigheid van dit document op de computer '**ontdekken**' en het document 'classificeren' als bestemd voor het 'Credit card gegevens' archief.
2. de stroom van dit document '**beschermen**'. Bijvoorbeeld met de regel 'Het mag niet per e-mail de organisatie uitgestuurd worden', 'mag niet worden geupload naar een website'.
3. de stroom van dit document 'auditen', bijvoorbeeld 'Het document werd verstuurd naar een collega', of 'Er is geprobeerd dit document te kopiëren naar een USB-stick'.

**Wat een DLP systeem niet doet:** DLP beleid is van toepassing op informatie, zolang deze zich binnen de onderneming bevindt. Zodra informatie uitgaat naar zakelijke partners dan is het DLP-beleid niet meer van toepassing. Het DLP systeem codeert geen informatie, dus in geval van diefstal het dataopslag apparaat, kan informatie worden gecompromitteerd.

**In welke context is DLP nuttig:** een DLP-systeem is nuttig in situaties waar gegevens zich in heterogene systemen bevinden en ondernemingen een methode moeten vinden om hun eigen documenten in kaart te brengen ( te 'ontdekken'). Deze 'ontdekking' leidt meestal tot het formuleren van regels en het beleid voor bescherming en controle op naleving van de wettelijke kaders, zoals ISO, SOX, GLBA, ...

**Wat een IRM-systeem doet:** Een IRM-systeem versleutelt de gegevens en koppelt een "gebruiksbeleid" aan elk stukje informatie. Het gebruiksbeleid beschrijft doorgaans WIE (gebruikers / groepen, binnen / buiten de onderneming) de informatie kan gebruiken, WAT (lezen, bewerken, doorsturen, afdrukken, ...) kan elke persoon doen, WANNEER (na een bepaalde datum, gedurende een bepaalde periode) kan dit gedaan worden en WAAR (bepaalde PC, alleen officiële zakelijke laptop) men dit kan doen. De versleuteling en het gebruiksbeleid is geassocieerd met de informatie gedurende haar gehele levenscyclus.

Een IRM-systeem:

1. **Definieert** een gebruiksbeleid waarbij een hoofdgebruiker het wie / wat / wanneer / waar kan definiëren voor de verschillende soorten informatie. Bijvoorbeeld 'communicatie van de Raad van Bestuur kan alleen worden geopend door interne en externe bestuurders en het secretariaat van de onderneming'.
2. Voert **Beleidscontroles** uit door ervoor te zorgen dat het gebruik van de informatie verloopt volgens het gedefinieerde beleid. Bijvoorbeeld 'de financiële vooruitzichten mogen niet verspreid worden voor dinsdagochtend'.
3. **Audit** het gebruik van informatie door centrale rapportage van WIE WAT WANNEER en WAAR heeft gedaan met de informatie.

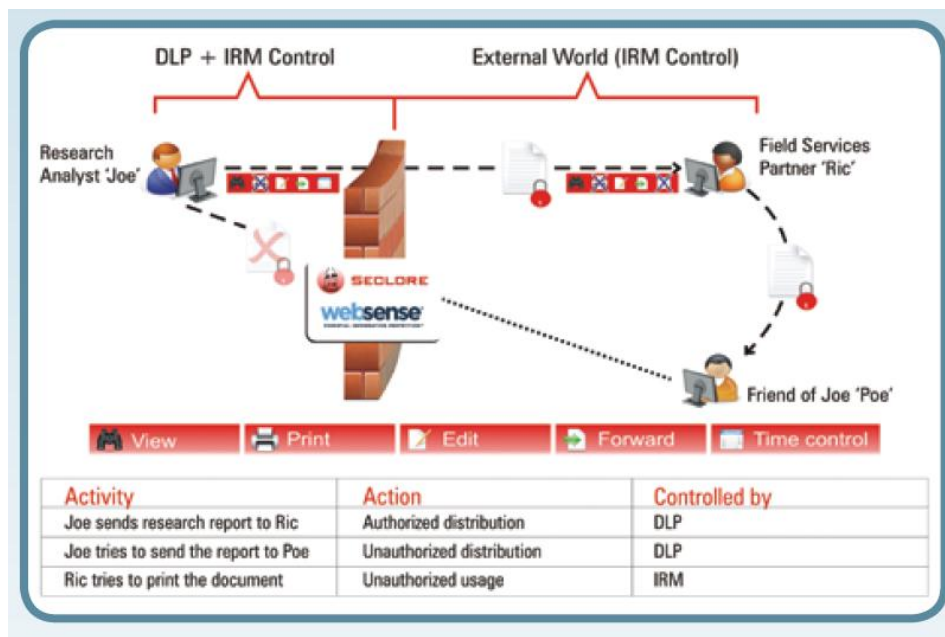
**Wat doet het niet:** een IRM systeem doet niet aan de beveiliging van de verplaatsing van informatie, zoals het blokkeren van e-mails en web-uploads. Controles worden uitgevoerd wanneer de informatie wordt **gebruikt**. Een IRM-systeem heeft geen mogelijkheid om informatie geautomatiseerd in kaart te brengen en deze informatie te classificeren. De beveiliging wordt toegevoegd wanneer bv: een document wordt aangemaakt, wordt bijgevoegd bij een e-mail, in een bepaalde folder wordt geplaatst of wordt geupload naar Sharepoint, etc.

**In welke context is IRM nuttig:** een IRM-systeem is nuttig wanneer men de controle wil behouden over de beveiliging van vertrouwelijke documenten en men toch deze documenten moet/wil uitwisselen interne en externe belanghebbenden. Het is ook nuttig in gevallen waar de beveiliging op het gebruik van informatie en controle hierop fijnmazig moet zijn om te voldoen aan wettelijke kaders (Need to know).

#### **Waarom zou u beide oplossingen nodig hebben?**

Een combinatie van IRM-en DLP-systemen helpt bij het in kaart brengen, beschermen en controleren van het gebruik van informatie binnen bedrijfsprocessen. De gecombineerde oplossing zorgt voor de inventarisatie en de classificatie van informatie, de fijnmazige bescherming op het gebruik van informatie en de controle op het daadwerkelijke gebruik van deze informatie en de pogingen tot misbruik. De content-aware DLP oplossing elimineert de noodzaak om handmatig bestanden te classificeren en te beveiligen, terwijl de IRM oplossing vervolgens de juiste beveiligingsmaatregelen op bestanden en e-mails plaatst en beheert. De integratie helpt organisaties hun investeringen in IRM en DLP te optimaliseren (het nadeel van de DLP oplossing wordt opgeheven door IRM en vice versa) en een betere, flexibele en meer effectieve beveiliging te bereiken tegen een lagere total cost of ownership.

In de onderstaande afbeelding is de gecombineerde DLP-IRM oplossing afgebeeld.



**Een gecombineerde DLP en IRM-oplossing maakt uitwisseling van vertrouwelijke informatie in de keten mogelijk, terwijl de gevoelige informatie beschermt blijft. De belangrijkste voordelen zijn:**

- Geautomatiseerd inventariseren vertrouwelijke documenten op netwerk;
- Bescherming van vertrouwelijke documenten ook buiten het eigen bedrijfsnetwerk, door het toevoegen van een IRM policy aan de bestaande DLP policies (dus in plaats van blokkeren documenten, de documenten versleutelen en beveiligen);
- Het faciliteren van compliance en auditing van 'ongestructureerde' data (bijvoorbeeld PDF's, MS Office-documenten, e-mail, webpagina's) binnen en buiten de organisatie;
- Integratie van DLP-IRM beveiligingstechnologie met Document Management systemen;
- Effectieve en efficiënte bescherming van uw kroonjuwelen tegen een lage cost of ownership.

De IRM oplossing van Seclore Filesecure combineert met diverse DLP producten in de markt, waaronder WEBSense en CTG.