March 19, 2019

SECURE CONTENT MANAGEMENT & MONITORING

HP INC

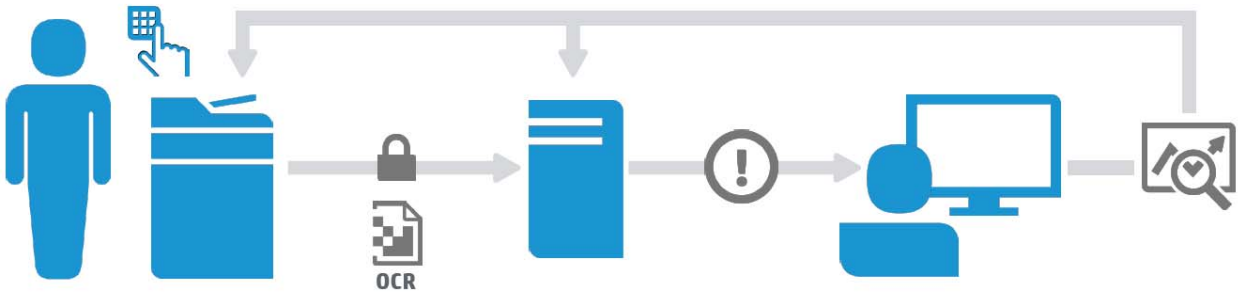
Secure Content Management & Monitoring

Abstract

The Secure Content Management & Monitoring solution is a robust and efficient information security software solution developed for document distribution oversight and governance. This solution is on the cutting edge of security monitoring technology in the information security industry by leveraging key innovation such Document Capture, Security, Big Data Analytics and customer DLP integration. It's the first product to provide capture, archive, and audit capabilities of device activities such as print, scan, fax, copy, and send jobs.

The Secure Content Management & Monitoring solution deters intentional or unintentional data leaks of important and valuable information processed through MFP or printing devices. If such data leakage does occur, crucial information such as who, what, when, and where this event occurred as well as key words within the data can be quickly retrieved and appropriate personnel notified.

Basic solution functionality:



Problem statement

Every time employees use a network device to print, scan, copy, or fax documents, organizations run the risk of a damaging security breach. Not to mention associated fines for noncompliance with industry and government regulations that can run into the millions of dollars. To ensure

complete control of all your organization's content, Security Administrators need a better way to identify, investigate, and halt document and information leaks before they hurt their organization—and their company's bottom line.

The area of Enterprise Secure Content Management & Monitoring is a new and emerging technology space that is impacting customers globally in government agencies, healthcare, financial services, and other regulated industries such as energy and professional services companies. This solution area requires technology vendors to create and deliver the capability to secure devices such as MFPs and Scanners with policies and tools to lock down vulnerabilities for potential breaches, audit all usage for authenticated users, and securely archive all the content generated by that user for forensic analysis by business and Security administrators.

When it comes to protecting sensitive information from insider threats, many organizations think first about securing their digital systems and channels—their networks, servers and web-based sources. But leaving the hardcopy portion of your data out of your security strategy can be a costly mistake.

The Secure Content Management & Monitoring solution can help fill in the gap of hardcopy security with technology that's discreet, automated and connected to your existing systems. We make the challenge of identifying and stopping paper and output-related threats effortless.

This solution helps ensure compliance for these organizations at risk and minimize or prevent fines and penalties in the millions of dollars depending on severity of the breach and jurisdiction. The need for protection of important information has risen from both compliance regulations and the increase in theft and misuse of closely held information. The Secure Content Management & Monitoring solution helps reduce the risks and liabilities associated with security breaches of physical documents. This single solution can simultaneously monitor and audit the information in millions of documents coming from all of your printers and multifunction devices--to improve the way your enterprise detects, investigates and deters security breaches.

Solution Overview

Knowing when and how sensitive data is printed, copied, scanned or faxed can be especially difficult. And while new tools and devices are improving productivity more than ever, those

improvements are also creating additional complexities that make it difficult to know exactly what information is being accessed and viewed from your devices.

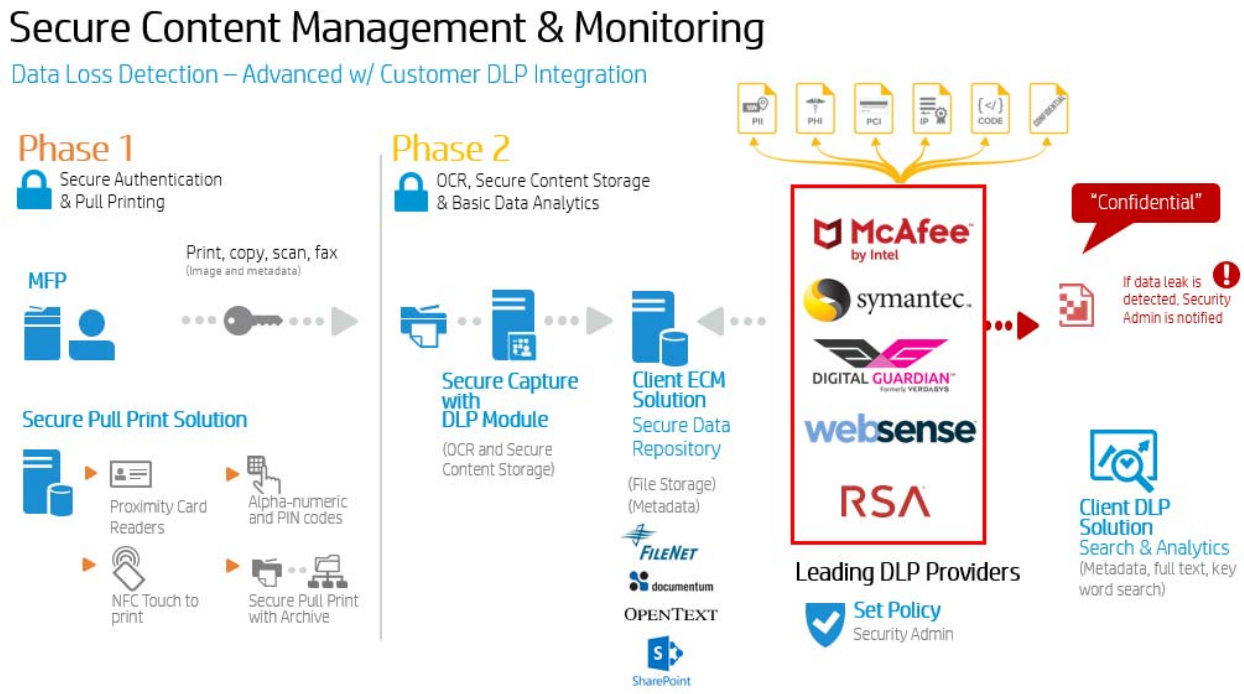
That's why the Secure Content Management & Monitoring solution resides on your MFPs and printers to monitor hardcopy documents directly from their point of origination. The technology automatically captures the content of every document that passes through a device, recognizes with its internal policies or routes it to a DLP provider for review. An IT administrator will everything they need to investigate potential threats, at their fingertips.

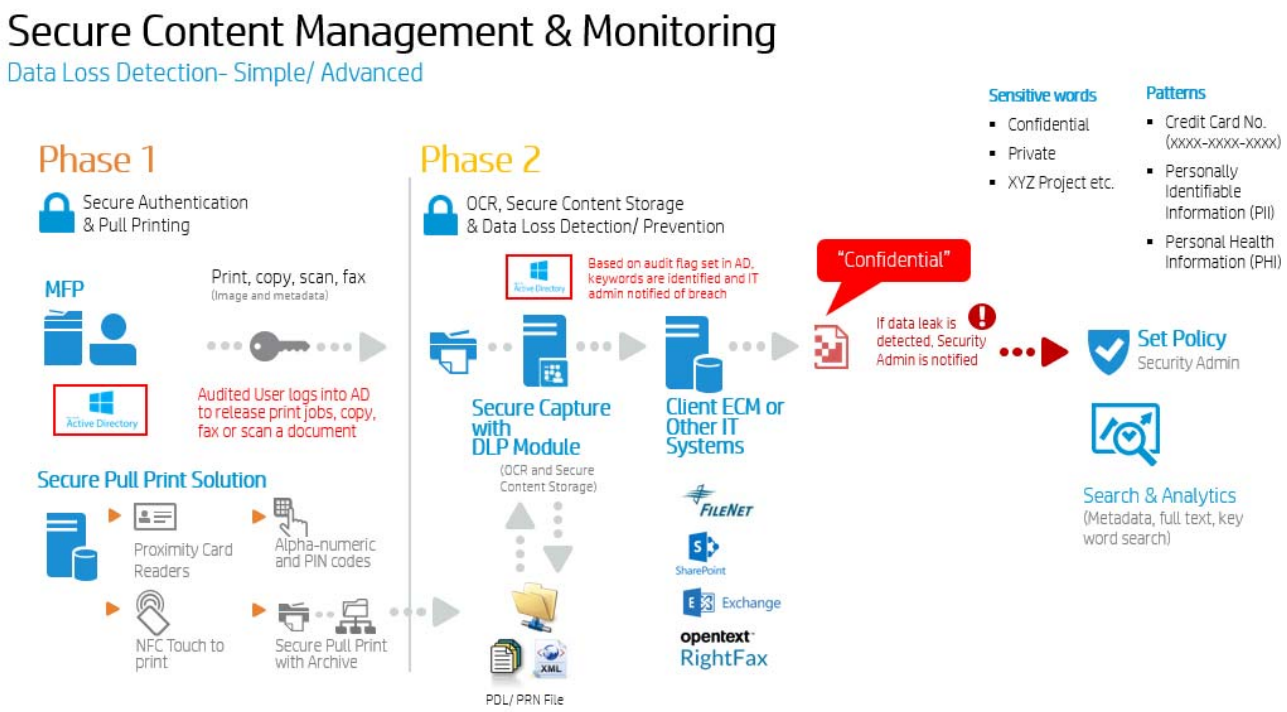
The Secure Content Management & Monitoring solution provides full-text and attribute search capabilities that are supported in multiple languages. This solution lets you see every document that's printed, copied, scanned or faxed through an output device. Plus, it lets you set up Discovery Alerts to continuously search all the content and it notifies authorized users when key words or phrases are found.

Secure Content Management & Monitoring:

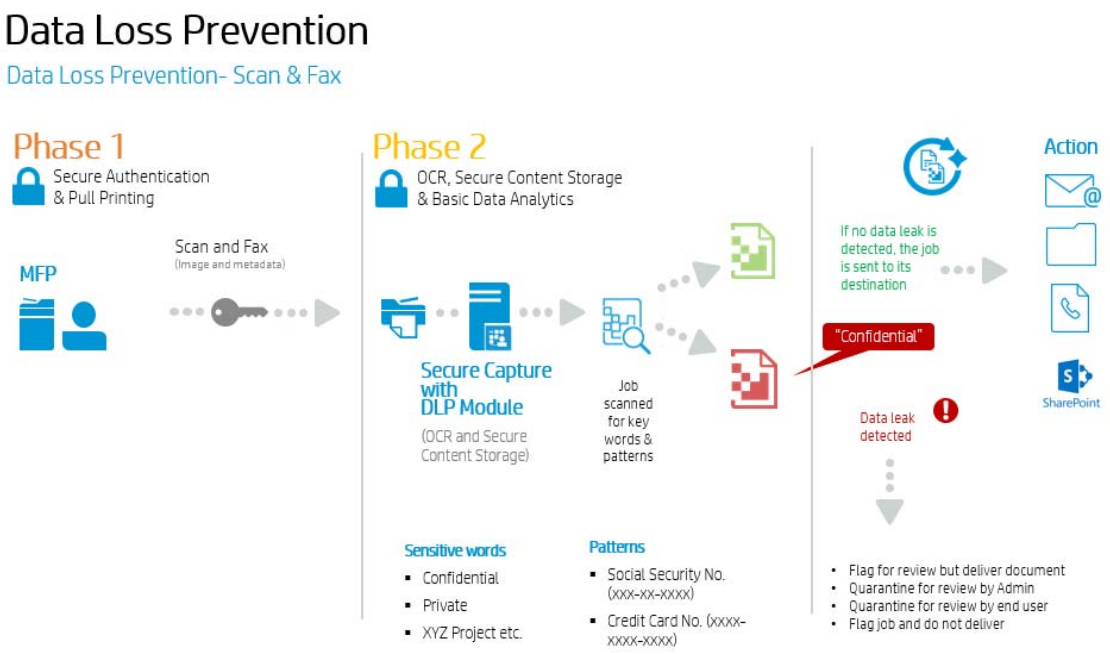
Present architecture/ use cases:


Data Loss Detection
Secure Content Management & Monitoring


Secure Content Management & Monitoring
Data Loss Detection – Advanced w/ Customer DLP Integration
Phase 1
Secure Authentication & Pull Printing
Print, copy, scan, fax
(Image and metadata)
MFP
Secure Pull Print Solution
Proximity Card Readers
Alpha-numeric and PIN codes
NFC Touch to print
Secure Pull Print with Archive
Phase 2
OCR, Secure Content Storage & Basic Data Analytics
Secure Capture with DLP Module
(OCR and Secure Content Storage)
Client ECM Solution
Secure Data Repository
(File Storage)
(Metadata)
FileNet
documentum
OpenText
SharePoint
PII
PHI
PCI
IP
CODE
McAfee by Intel
symantec.
DIGITAL GUARDIAN
websense
RSA
Leading DLP Providers
Set Policy
Security Admin
"Confidential"
If data leak is detected, Security Admin is notified
Client DLP Solution
Search & Analytics
(Metadata, full text, key word search)


Secure Content Management & Monitoring
Data Loss Detection- Simple/ Advanced
Phase 1
Secure Authentication & Pull Printing
MFP
Print, copy, scan, fax
(Image and metadata)
Active Directory
Audited User logs into AD to release print jobs, copy, fax or scan a document
Secure Pull Print Solution
Proximity Card Readers
Alpha-numeric and PIN codes
NFC Touch to print
Secure Pull Print with Archive
Phase 2
OCR, Secure Content Storage & Data Loss Detection/ Prevention
Active Directory
Based on audit flag set in AD, keywords are identified and IT admin notified of breach
Secure Capture with DLP Module
(OCR and Secure Content Storage)
PDL/ PRN File
Client ECM or Other IT Systems
FileNet
SharePoint
Exchange
opentext
RightFax
"Confidential"
If data leak is detected, Security Admin is notified
Sensitive words
Confidential
Private
XYZ Project etc.
Patterns
Credit Card No. (xxxx-xxxx-xxxx)
Personally Identifiable Information (PII)
Personal Health Information (PHI)
Set Policy
Security Admin
Search & Analytics
(Metadata, full text, key word search)


Prevention
Data Loss Prevention- Scan & Fax

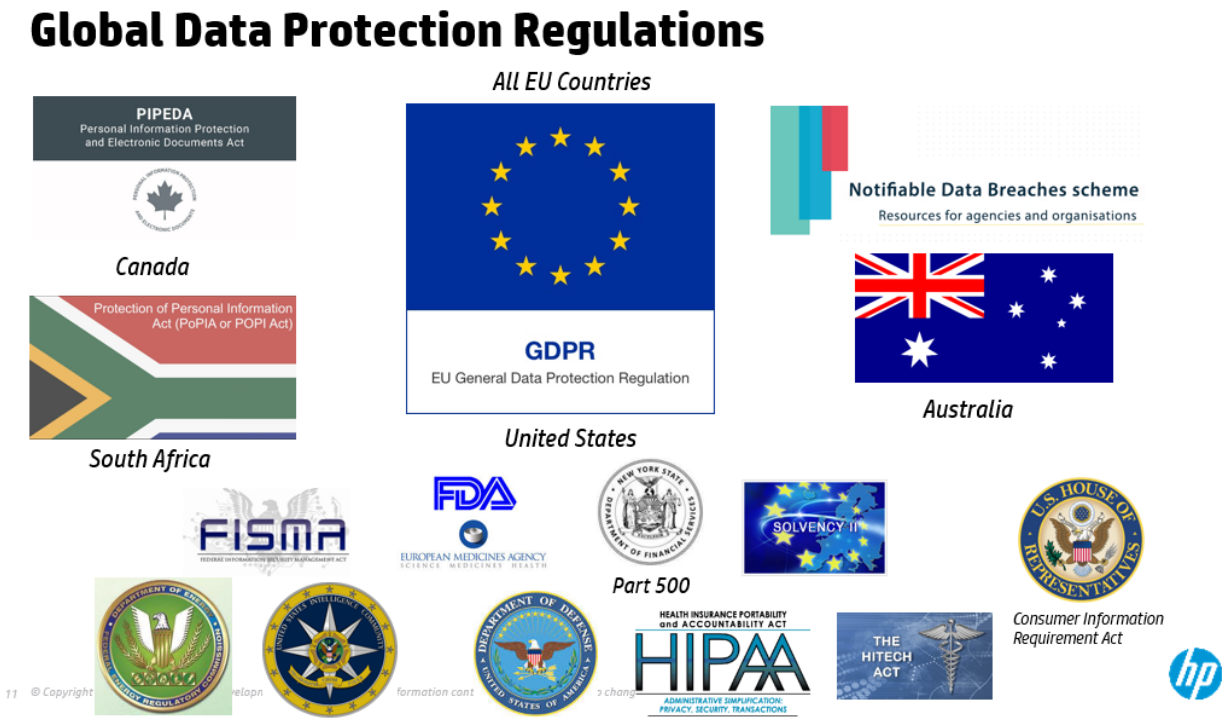


Global Compliance and Governance achieved with solution:

The solution offers a reduction of exposure to steep fines with a solution that's fully complaint with the latest industry and government regulations on document security, including HIPAA, HITECH, GDPR, SOX, FERC, NERC, and more. The solution helps cut costs by automating the process of tracking security leaks. Secure Content Management & Monitoring provides a full audit trail within minutes—not days or weeks.

As a result of John's efforts, the Data Loss Detection & Proactive Monitoring and Alerting solution is now enabled globally with applicability for security information governance for the following countries:

- United States- DoD, US Intelligence Agencies, FISMA, NERC, FERC, HIPAA, Hitech, FDA- European Medicines Agency, NY DFS Part 500, & Solvency II, NY DFS Part 500
- EU GDPR- All 28 European Union Countries
- Canada- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Australian Government- Notifiable Data Breach Scheme
- South Africa- The Protection of Personal Information Act (called the POPI Act or POPIA)



Data Loss Detection use case example: Tracking document transactions

1. A user obtains a confidential document with or without authorization.
2. The user logs into the MFP with an employee badge or other form of authentication.
3. Using the e-Task touch screen, the user scans the document and makes a copy about “Project Titan”.
4. The Secure Document Monitor application automatically: Captures a digital image of the document and collects the user’s ID, date and time of the transaction and the device ID
5. The job is converted into a TIFF image or multiple TIFF images (if the document is more than one page) and sent to an OCR engine, which is either provided by Secure Content Monitor or the customer’s existing DLP.
6. Each document’s image, metadata and full-text results (extracted during OCR) are then pushed into a DLP server.
7. The content is submitted against the monitoring parameters set up in the DLP by the organization.

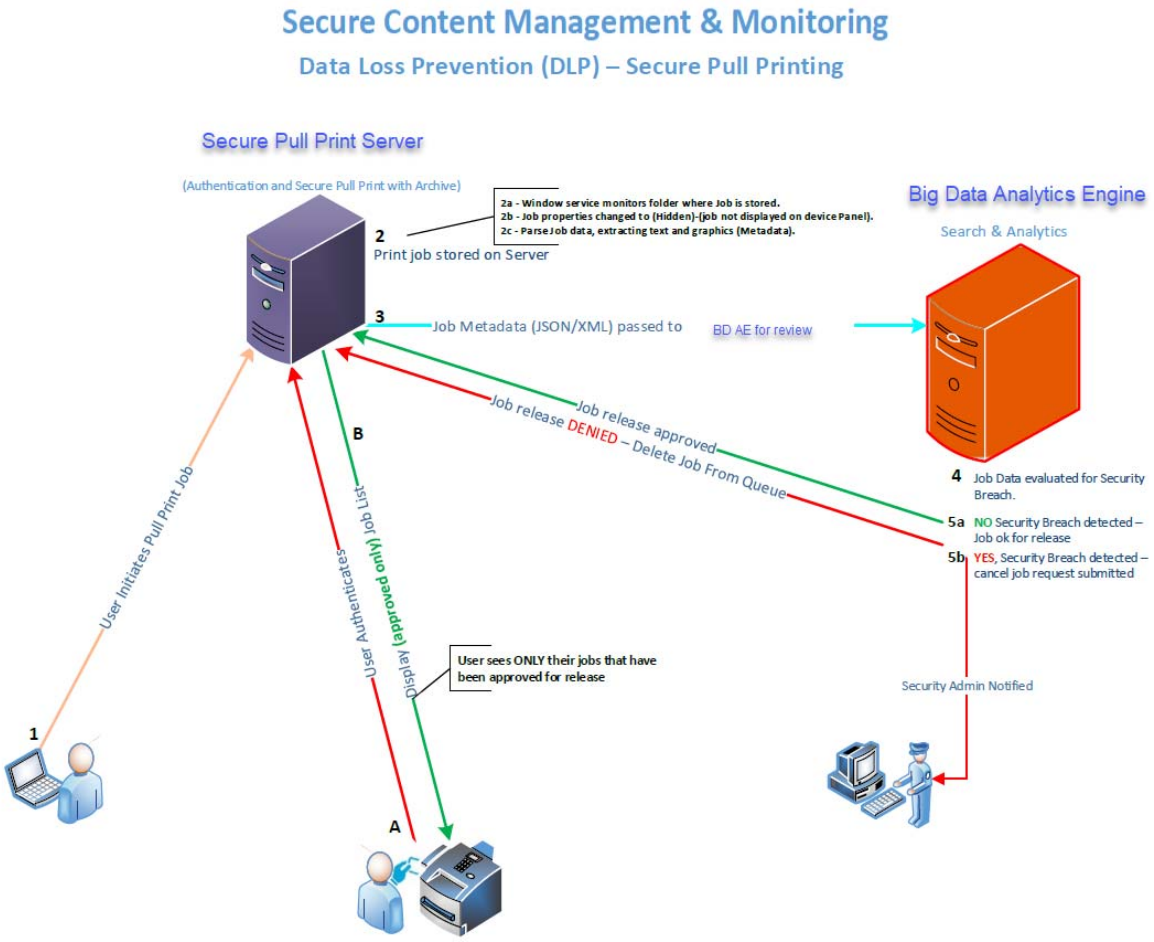
Within the customer’s DLP

8. The organization was worried about information leaking about Classified “Project Titan” and had set up an alert for any document containing that phrase.
9. The security officer receives a notification that a document was copied by an employee that contains phrase, “Project Titan”.
10. The security officer proceeds with an investigation, using the digital document images and specific transaction details as evidence.

The following table lists the metadata fields that are examples of the different types of metadata that can be associated with each document that is sent to the DLP.

User name who performed the operation
Time operation occurred
Device name where the operation occurred
Type of document (print, copy, fax, email, FTP)
Number of copies
Printed document file name
Computer name and user name that sent originating print job
Recipient fax, email or FTP address
Sender's fax number or email address
Email subject
Device location, device contact name, and device hostname as specified on embedded web page

Early work: 2014



Disclosed by John S. Steele, HP Inc.

Early work contiued: 2014