Forcepoint | SECLORE

Solution Brief

Seclore for Forcepoint DLP

Challenge

- DLP can either block sensitive data from leaving the enterprise or monitor it after leaving the organization. When blocking data on egress, productivity workflows break, while monitoring data allows it to be sent unprotected and left to defend itself.

Solution

- Automatically add persistent, granular usage controls to discovered data
- Dynamically assign and revoke file permissions instantly
- Map security permissions to DLP business rules
- Secure data at endpoints, on the network, or within the email
- Gather forensic detail on data usage

Outcome

- Expedite DLP deployments to reduce costs and increase 'time to value'
- Drastically reduce false positives to reduce administrative overhead
- Allow uninterrupted internal and external collaboration
- Maintain control and track sensitive data when it leaves the organization
- Meet audit and regulatory compliance

Data Loss Prevention (DLP) discovers sensitive data and prevents it from leaking outside your network. However, what happens after data discovery? What do you do with all those incidents? How do you keep collaboration with external, third-party business partners secure, when emails get blocked at the endpoint or are sent out unprotected? How do you protect files shared via the cloud, or viewed by outside contractors on mobile devices? How do you get sensitive data back when it gets into the wrong hands?

Seclore Rights Management and Forcepoint DLP

DLP can inspect content in documents and discover sensitive data. By detecting sensitive data, you can, in turn, automatically add the appropriate usage controls (rights) to documents and interaction with data. With Seclore Rights Management Integration, you have complete control over your information - up to and including the power to revoke access entirely - even beyond your enterprise boundaries. As soon as Forcepoint DLP discovers sensitive data, Seclore can instantly protect it with the appropriate usage policies. Seclore's persistent. Granular data usage controls stay with the file, wherever the file goes, inside or outside the enterprise, and protects data while in use (files being worked on), in transit (sent via email), and at rest (any file format, any device, any operating system).

The Power of Two

Seclore Rights Management helps you change your security posture from "reactive" to "proactive" when using Forcepoint DLP. Traditionally, DLP is configured in "monitor" mode, providing dashboards, reports, and alerts, which tracks information that leaves the enterprise. Monitoring mode is a standard application of DLP; however, the security concern is that sensitive data is leaving the enterprise. If your sensitive data falls into the hands of a bad actor or you need to retrieve it from a third party, you must chase your sensitive data to get it back. With Seclore, you are always in the driver's seat.

Seclore Rights Management also significantly expedites the deployment of Forcepoint DLP. If you are unsure of a business rule to apply to discovered information: block, quarantine, allow, etc., automatically protecting the information with Seclore can become the default action. Also, it eliminates ongoing configuration.

DLP Discovers

- Scans Content
  - Keywords
  - Patterns
  - Digital Fingerprints
  - Optical Character Recognition (OCR)
- Prevents sensitive information from leaving enterprise perimeter
- Logs incidents within the enterprise

Rights Management Protects

- Secures Content
  - Granular usage controls
  - Specify who can access what, where, when and how
  - Restrict and revoke access
  - Data in use, in transit and at rest
- Allows authorized external users to access sensitive information
- Tracks and audits data within and beyond the enterprise

With Seclore RM and Forcepoint DLP combined, you can control who can access the document, what they can do with it, when, and from which computer or device. By adding persistent, data-centric usage controls, the scope of Forcepoint DLP can be extended to documents traveling through public and partner networks, stored on the cloud or file-sharing services, or accessed on mobile devices.

Instant Protection:At Endpoints, on the Network or in the Cloud

Sensitive data discovered during Forcepoint DLP discovery scans - at endpoints, on the network, or in the cloud - can be instantly protected by Seclore Rights Management. For example, Seclore protection policies can be mapped to the discovery of sensitive keywords or regular expressions (e.g., credit card numbers). The usage controls will ensure that no user outside the responsible department (let alone outside the organization) can utilize that document - even if it is sent to them. With Forcepoint DLP, protection is extended further by leveraging precise ID fingerprinting to recognize sensitive data residing anywhere, such as on file servers, or when this sensitive data is being distributed by users, helping administrators to focus their attention on the riskiest users and behavior.

Moreover, this protection is almost immediate and completely automatic. The automated application of usage controls based on the DLP discovery policies results in no additional steps for employees, less training cost, and reduced change management efforts.

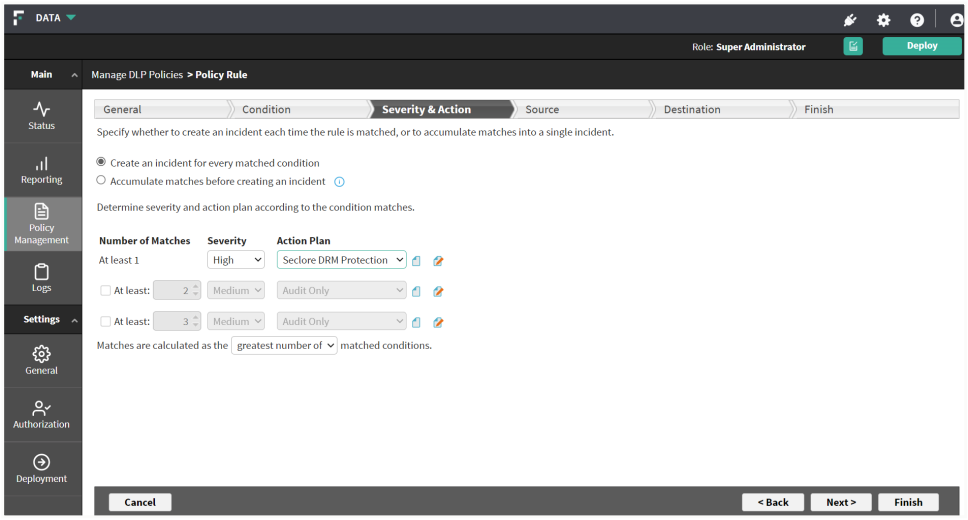

Figure 1: Discovery results automatically mapped to protection policy.

Seclore Rights Management and Forcepoint DLP Endpoint

Forcepoint DLP can scan documents and discover confidential data lying on network endpoints. Forcepoint DLP can match keywords (e.g., revenue projections), patterns, and regular expressions (e.g., credit card numbers) and can also look into specific folders or search for documents of specific formats. After discovery, Seclore secures this sensitive information, applying the relevant Seclore policy to prevent its leakage or misuse, based on policy definitions set by the organization's administrator. With Forcepoint DLP you can extend on-network policies to off-network devices and apply policies at the individual endpoint level so data is protected even when users are remote.

Advantages

- → Automated protection for sensitive information, on or off the network
- → Reduced dependency on users to protect sensitive data
- → Protection that stays with the file - in storage, in transit and while in use

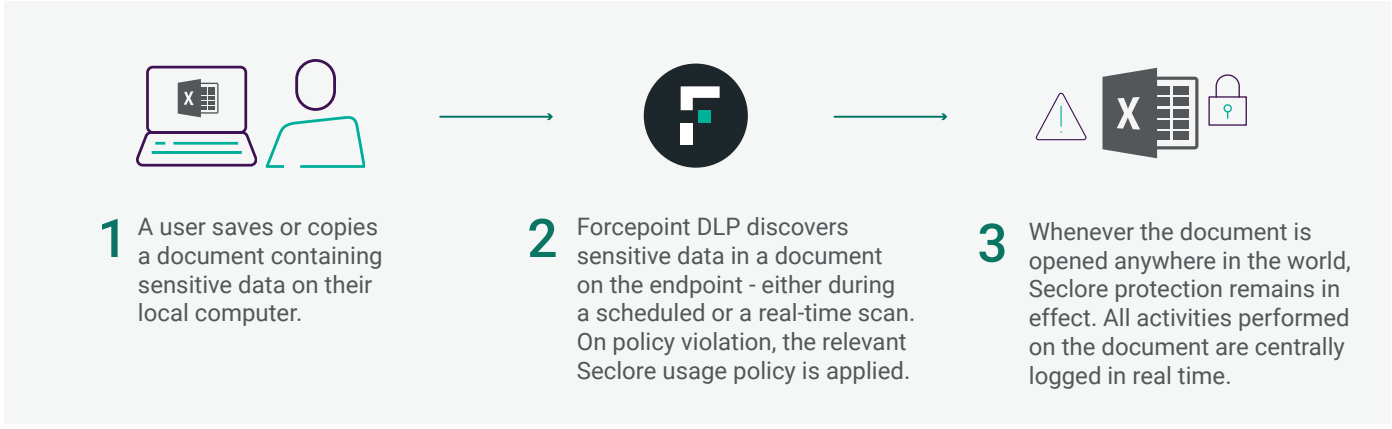

Figure 2: Endpoint Discovery

Seclore Rights Management and Forcepoint DLP Network

Forcepoint DLP scans sensitive documents residing in file servers. Protecting data being moved throughout and beyond the enterprise is key. With DLP Network, secure data in use by monitoring data flows via communication channels such as email and web. Seclore extends protection by securing sensitive information to prevent its leakage or misuse.

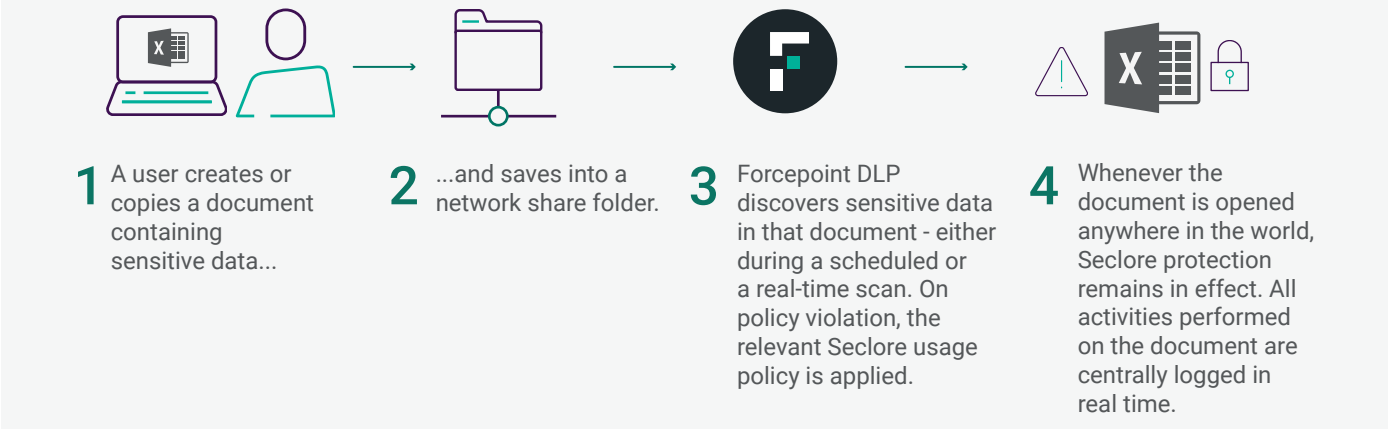

Figure 3: Network Discovery

Seclore Data Classification and Forcepoint DLP

Seclore Data Classification works with Forcepoint DLP to reduce false positives during data discovery.

- **A user classifies** an Office document, for example, by simply clicking on a classification label in the Office ribbon.
- **Forcepoint DLP tags** the document based on the chosen classification.
- **Seclore Rights Management protects** the document with the appropriate usage policy. Whenever the document is opened anywhere in the world, Seclore protection remains in effect.
- **Forcepoint fingerprinting** makes it possible to discover when partial pieces of the document are being copied, pasted, or edited, so data exfiltration can be detected and prevented.
- All activities performed on the document are centrally logged in real time. Since the classification of the document is selected by the user, the **chances of false positives are virtually eliminated.**

Seclore Automatic Email Protection with Forcepoint Email Security

DLP Email Security is most often run in discovery mode, due to the risk of false positives. Any discovery of anomalous user behavior occurs only after the fact. For data that needs to go out of the network for business purposes, there is no choice but to allow the emails to go completely unprotected.

Seclore offers an easy, streamlined solution to these problems. Once emails are processed by the DLP Email Gateway, Seclore Rights Management's automated protection capability secures the email and it's attachments with the appropriate usage policy. This ensures that recipients cannot misuse or leak the email after they receive and read it. Thus, an "allow" policy with DLP becomes a "for next 10 days" policy with Seclore.

With Seclore Rights Management's automated email protection, email security doesn't halt critical email collaboration. Data sharing can continue, with security and compliance still being maintained. And all of this is completely transparent to the email sender and recipient.

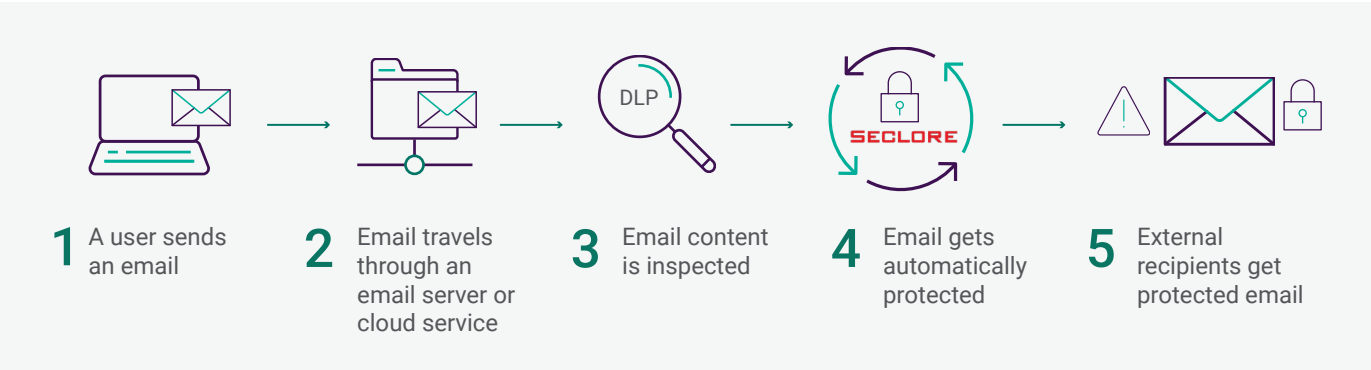

Figure 4: Seclore and Forcepoint DLP

Secure Email Decryption for Forcepoint DLP Content Discovery

A challenge DLP systems face is discovering sensitive content in encrypted emails and attachments to decide whether an email should be shared or blocked. Seclore Decrypter for Email solves this challenge by enabling secure access to Seclore encrypted emails and attachments. When the protected email is decrypted, Forcepoint DLP can look for sensitive content and patterns and take appropriate decisions (allow/block/protect). The Seclore Decryption for Email works in conjunction with Seclore's Email Auto-Protector to automate the protection of emails before sending them outside the organization.

Organizations using Seclore Rights Management and Forcepoint DLP can now claim compliance to regulations as Forcepoint DLP can discover, track, and audit all files - both unprotected and protected.

Key Business Benefits

Automated Data Protection
DLP-Digital Right Management (DRM) integration automates the entire process of classifying, protecting, controlling usage, and auditing. The handover from detection to protection is seamless. The process of DRM protection is completely transparent to the end user.

Faster DLP Deployments
DRM can be set up as DLP's "default" business rule to gain immediate benefits from DLP upon deployment.

Security and Compliance Beyond the Firewall
DLP-DRM integration secures and audits data everywhere it goes; to vendor and partner networks, to public networks, to the cloud or to mobile devices.

Reduced Incident Lists
DLP can be configured to treat DRM - protected files as safe - and not generate alerts for such files. This leads to significantly reduced incident logging.

Minimal Training Overhead
There is almost zero training required for end users, since protection is automatic, and a protected document opens in the native application just like any other document.

Increased Business Agility
The ability to secure information that travels beyond corporate borders solves a thorny compliance challenge, significantly reduces security risks, and enables the safe and secure adoption of file-sharing services, BYOD and cloud computing.

End-To-End Auditing and Regulatory Compliance
DLP-DRM integration enables compliance with regulatory obligations for the entire life-cycle of unstructured data - both within and outside the enterprise network.

Enforcing IT Policies on Third Parties
DLP-DRM integration helps enforce your data governance and corporate IT policies on contractors, vendors, partners and other third parties.

About Forcepoint

Forcepoint is the leading user and data security cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Our solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value.

forcepoint.com

About Seclore

Our mission is to safeguard sensitive information worldwide, regardless of its location. Seclore offers persistent protection and visibility for digital assets to help organizations remain secure and compliant. Our data-centric security approach ensures that only authorized individuals can access protected digital assets. With Seclore, organizations can specify who can access their data, what actions are permitted, and how long that access lasts. Join industry leaders like American Express in choosing Seclore for superior digital asset protection without sacrificing seamless collaboration and sharing.

seclore.com