FORCEPOINT

SECLORE

SOLUTION BRIEF

Seclore for Forcepoint DLP

HIGHLIGHTS

- ✓ Extend protection beyond the enterprise
- ✓ Secure email, cloud and other file sharing
- ✓ Reduce false positives
- ✓ Dynamically assign and revoke granular file permissions
- ✓ Gain comprehensive data reports for 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?

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 set classification labels and add the appropriate usage controls (rights) to documents and interactions with data.

Most organizations find it difficult to go beyond the discovery phase to the active data protection phase. Reviewing the tremendous amount of data collected by DLP logs is challenging enough and often impedes worker productivity. Seclore Data Classification and Rights Management solve this challenge, by adding user insights to the Classification label to reduce false positives and then automatically attaching usage control policies to the discovered 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 sensitive data is discovered by Forcepoint DLP, 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).

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

Forcepoint DLP

9x

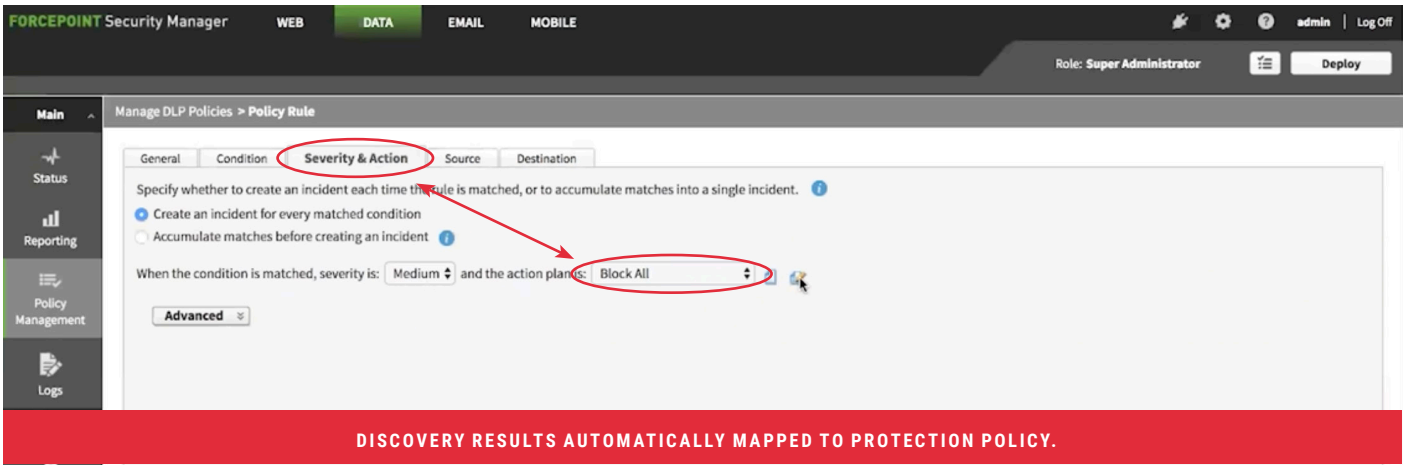
Gartner Magic Quadrant Leader

With Secore 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 controls, the scope of Forcepoint DLP can be extended to documents travelling 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.



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.

1 A user saves or copies a document containing sensitive data on their local computer.

2 Forcepoint DLP discovers sensitive data in a document on the endpoint – either during a scheduled or a real-time scan.

On policy violation, the relevant Seclore usage policy is applied.

3 Whenever the document is opened anywhere in the world, Seclore protection remains in effect.

All activities performed on the document are centrally logged in real time.

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

Seclore Rights Management and Forcepoint DLP Network

Forcepoint DLP Discover 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.

1 A user creates or copies a document containing sensitive data

2 ...and saves into a network share folder.

3 Forcepoint DLP discovers sensitive data in that document – either during a scheduled or a real-time scan.

On policy violation, the relevant Seclore usage policy is applied.

4 Whenever the document is opened anywhere in the world, Seclore protection remains in effect.

All activities performed on the document are centrally logged in real time.

Seclore Data Classification and Forcepoint DLP

Seclore Data Classification – powered by Boldon James – 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**.

With Seclore Data Classification, Forcepoint customers gain the worldwide market-leading classification solution, integrated with the most advanced Rights Management.

Seclore's global OEM partner for Data Classification, Boldon James:

- Best-of-breed technology
- Broadest feature set
- 30+ years of expertise

POWERED BY Boldon James
A QINETIQ company

SUPPORTED COMPONENTS

Forcepoint:

Forcepoint DLP 8.3 and above

Seclore:

Seclore Policy Server 3.3.0.0 (Seclore 3.6.0.0) or higher

Seclore Desktop Client 3.4.0.0 (Seclore 3.6.0.0) or higher

a. Seclore for Forcepoint DLP 1.0.0.0 or higher

b. Seclore customization module compatible with Seclore for Forcepoint DLP 1.0.0.0 or higher

Windows:

Windows® 7, 8, 8.1, or 10 for automatic protection with Forcepoint DLP Endpoint Discover

Windows Server® 2008, 2012, or 2016 for automatic protection with Forcepoint DLP Network Discover

Seclore Automatic Email Protection with Forcepoint Email Security

1 A user sends an email

2 Email travels through an Email Server or Cloud Service

3 Email content is inspected

4 Email gets automatically protected

5 External recipients get protected email

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 its 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 ten 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.

Key Business Benefits

- **Automated Data Protection:** DLP-Digital Rights 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 RM protection is completely transparent to the end user.
- **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 lifecycle 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 global human-centric cybersecurity company transforming the digital enterprise by continuously adapting security response to the dynamic risk posed by individual users and machines. The Forcepoint Human Point system delivers Risk-Adaptive Protection to continuously ensure trusted use of data and systems. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.

www.forcepoint.com

About Seclore

Seclore offers the market's first browser-based Data-Centric Security Platform, which gives organizations the agility to utilize best-of-breed solutions to discover, identify, protect, and audit the usage of data wherever it goes, both within and outside of the organization's boundaries. The ability to automate the data-centric security process enables organizations to fully protect information with minimal friction and cost. Over 2000 companies in 29 countries are using Seclore to achieve their data security, governance, and compliance objectives.

www.seclore.com

Global Headquarters
USA – West Coast
691 S. Milpitas Blvd
Suite 217
Milpitas, CA 95035
1-844-473-2567

USA – East Coast
Graybar Building
420 Lexington
Avenue
Suite 300
New York, NY 10170

Europe
Seclore GmbH
Marie-Curie-Straße 8
D-79539 Lörrach
Germany
+49 7621 5500 350

India
Excom House Second Floor
Plot No. 7 & 8,
Off. Saki Vihar Road
Sakinaka, Mumbai
400 072
+91 22 6130 4200
+91 22 6143 4800

Saudi Arabia
5th Floor, Altamyoz Tower
Olaya Street
P.O. Box. 8374
Riyadh 11482
+966-11-212-1346
+966-504-339-765

Singapore
Seclore Asia Pte. Ltd.
AXA Tower, 8 Shenton Way
Level 34-01
Singapore – 068811
+65 8292 1930
+65 9180 2700

UAE
Seclore Technologies FZ-LLC
Executive Office 14, DIC
Building 1 FirstSteps@DIC
Dubai Internet City
PO Box 73030
Dubai, UAE
+9714-440-1348
+97150-909-5650
+97155-792-3262

SECLORE