

Forcepoint Data Loss Prevention and Microsoft Information Protection

Automate detection, validation & application of classification labels

Forcepoint



Forcepoint and Microsoft Partnership



- Increasing number of enterprises moving to O365



- 67% of enterprises running Microsoft Azure
- Customers trust the Microsoft ecosystem



- Most customers have on-premises environments

Integration Capabilities

- Label schema import from O365 Security & Compliance Center
- Data discovery on the endpoint to locate & identify sensitive data
- Automated application of classification labels
- Automated application of Rights Management templates
- Reporting and visibility via Forcepoint DLP and Azure consoles

Automate detection, validation & application of classification labels

Leveraging Microsoft Information Protection SDK

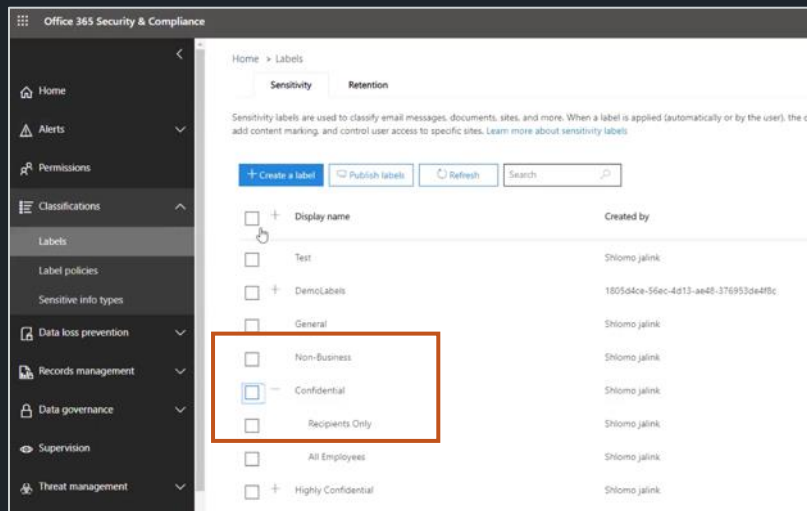
- Integration with Microsoft Information Protection SDK version 1.1.217
- Requirements & Prerequisites
 - Supports Windows 7, 8 and 10
 - Forcepoint: DLP v8.7 (available now)
 - Microsoft: E3 license
- Microsoft Information Protection SDK is packaged with and deployed by the DLP agent



The Microsoft Information Protection SDK brings the classification, labeling, and protection capabilities of Microsoft Information Protection into a simple, lightweight, cross-platform software development kit that enables any application to label and protect information.

Label Schema Import from Microsoft Information Protection

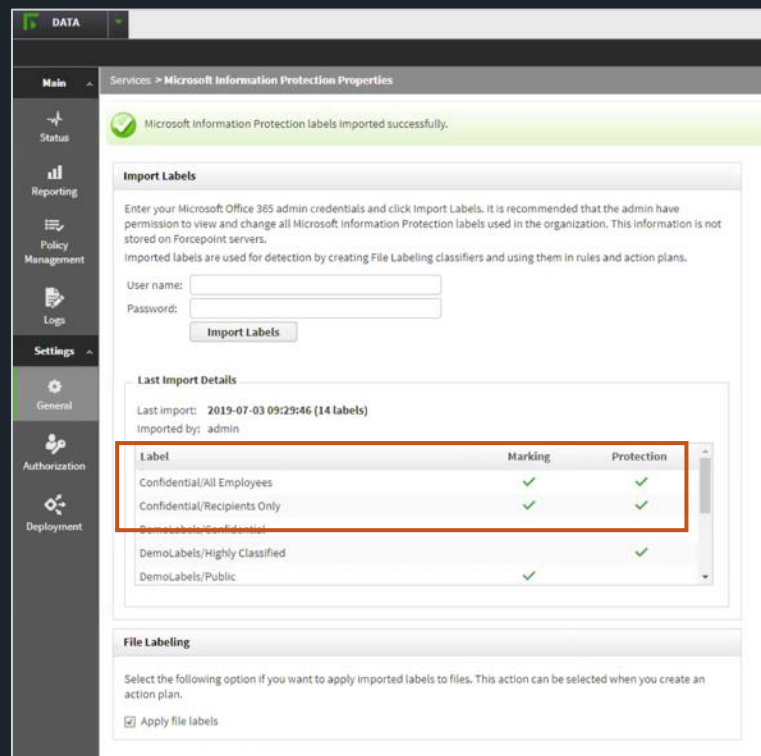
- Enabled for Microsoft 365 Security & Compliance Center
- Supported for Azure Information Protection*



Office 365 Security & Compliance



Forcepoint Security Manager (FSM)



Automate Detection and Application of Labels

- Configure endpoint discovery
- Policy applies Microsoft Information Protection labels
- If RMS is associated with a label, the file is automatically protected.

The screenshot displays the Forcepoint Data console interface. On the left, a sidebar contains navigation icons for Main, Status, Reporting, Policy Management, Logs, Settings, General, and Users. The main area is titled 'Manage Discovery Policies' and shows a list of policies. One policy, 'US PII: Credit Card Number and Social Security Number', is highlighted. To the right, a detailed view of this policy is shown, including its name, severity, action plan, and description. A red box highlights the policy name in the list and the policy details section. Below the policy details, a table shows the condition for the policy: '<US PII: Credit Card Number and Social Security Number (predefined)>'. On the right side of the console, a 'Policy version: 5' label is visible. A red box highlights the 'Policy version: 5' label.

Policy Details:

- Rule:** US PII: Credit Card Number and Social Security Number
- Policy:** US PII for Discovery
- Severity & Action:** When matched - severity: Medium, action plan: Audit Only; At least 3 matches - severity: High, action plan: Audit Only
- Description:** Matches are calculated as the sum of all matched conditions. Rule for detecting a valid credit card number in proximity to valid social security numbers (SSN) issued by the US Social Security Administration, taking into account SSN randomization, employing context sensitive lexical analysis, statistical analysis of patterns and custom dictionaries.
- Condition:** <US PII: Credit Card Number and Social Security Number (predefined)>

Azure Information Protection Label Priorities are Respected

- When a document already has a label such (ie. *Confidential*) DLP can elevate the label to a higher sensitivity (ie. *Top Secret*)
- If a higher priority label is already applied to the document, then DLP won't override but will report it.

The screenshot displays the Azure Information Protection (AIP) interface, showing the 'Properties' tab for a file. The file is named 'FPIL1\qa2' and was last modified on 10 Jul. 2019, 03:17:52 PM GMT+0000. The file's checksum is 009327cacc1a247e6792b72905e88d47. The file permissions are listed as [RW] for LOCAL_SYSTEM, FPIL1\qa2, and BUILTIN\Administrators. The incident details section shows a severity of High and a status of 'Marked by Microsoft Information Protection'. The 'Applied a file label' section is highlighted with a red box, showing 'File was not labeled' and a tooltip that reads: 'File was not labeled. PastaLabel - a higher-priority label was found on the file. The file was not labeled.'

Properties	
Date Modified:	10 Jul. 2019, 03:17:52 PM GMT+0000
Date Accessed:	10 Jul. 2019, 03:17:52 PM GMT+0000
Checksum:	009327cacc1a247e6792b72905e88d47
File owner:	FPIL1\qa2
File Permissions	
LOCAL_SYSTEM	[RW]
FPIL1\qa2	[RW]
BUILTIN\Administrators	[RW]
Incident Details	
Severity:	High
File properties:	Marked by Microsoft Information Protection
Action:	Applied a file label
File labeling status:	File was not labeled
Previous labels:	PizzaLabel
Current labels:	PizzaLabel
Status:	New
Channel:	Endpoint Discovery

DLP Incident Reporting

- Labeling columns are visible within the DLP incident record to indicate file labeling operations performed by the DLP system.

Show/Hide Columns		
<input type="checkbox"/>	IP Address	List the IP address of the host on which the violation was detected
<input type="checkbox"/>	Event time	The date the incident was detected
<input type="checkbox"/>	Endpoint Type	Indicates the type of Endpoint (PC, laptop, etc...)
<input type="checkbox"/>	Discovery Type	Indicates the type of resource (Network, SharePoint, Endpoint, etc...)
<input type="checkbox"/>	More Details1	More info about the incident
<input type="checkbox"/>	More Details2	More info about the incident
<input checked="" type="checkbox"/>	Action	The action that was taken on the discovered file
<input checked="" type="checkbox"/>	Previous Labels	Labels found on the file before DLP analysis
<input checked="" type="checkbox"/>	Current Labels	Labels found on the file after DLP analysis and action
<input checked="" type="checkbox"/>	Labeled by DLP	The status of the file labeling
<input checked="" type="checkbox"/>	File Properties	File properties such as label attributes
<input checked="" type="checkbox"/>	File Labeling Status	The status of the file labeling action

Maximum number of incidents in one page:

Incident Details	
Severity:	High
File properties:	Marked by Microsoft Information Protection
Action:	Applied a file label
File labeling status:	File was not labeled
Previous labels:	PizzaLabel
Current labels:	PizzaLabel

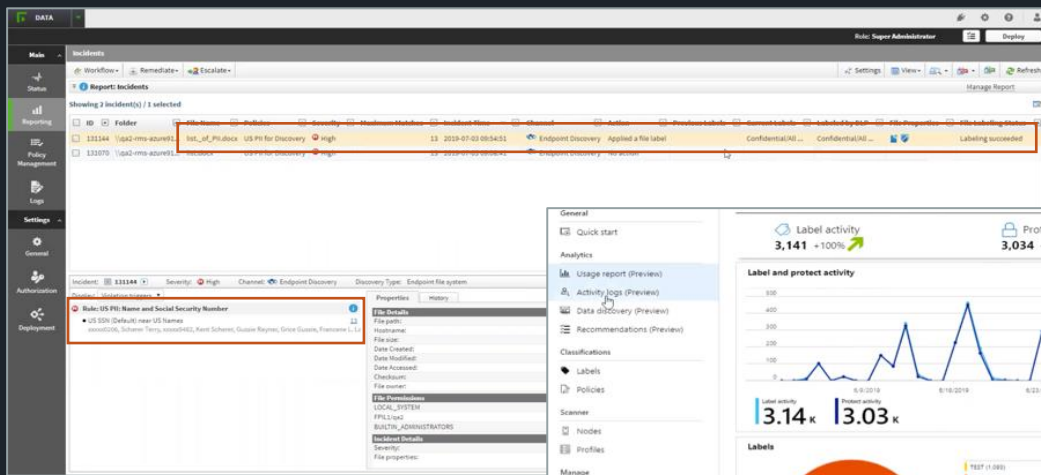
Action	Previous Labels	Current Labels	Labeled by DLP	File Properties	File Labeling Status
Applied a file label	PizzaLabel	PizzaLabel			File was not labeled
Applied a file label	PastaLabel	PizzaLabel	PizzaLabel		Labeling succeeded

Select the file properties to include in the report

- ☐ Marked by Microsoft Information Protection
- ☐ Protected by Microsoft Information Protection

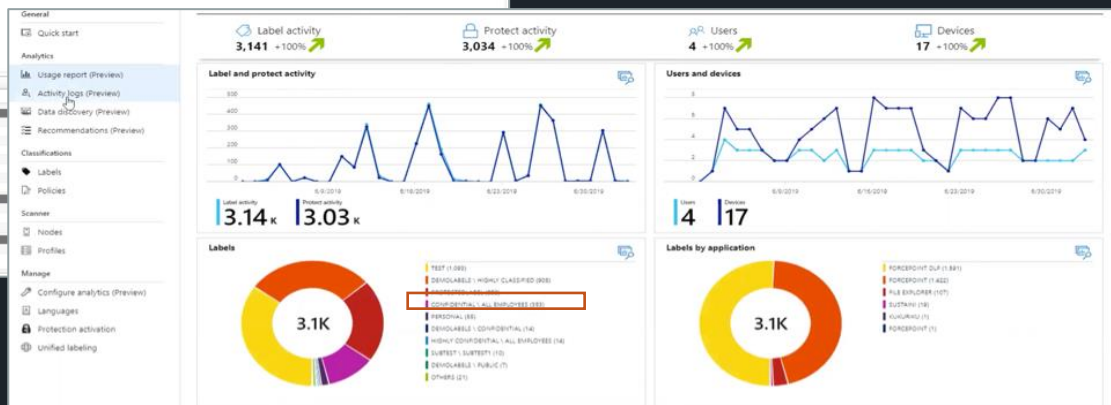
Reporting and Visibility

- Visibility to activity within both the **Forcepoint** and **Azure** consoles.

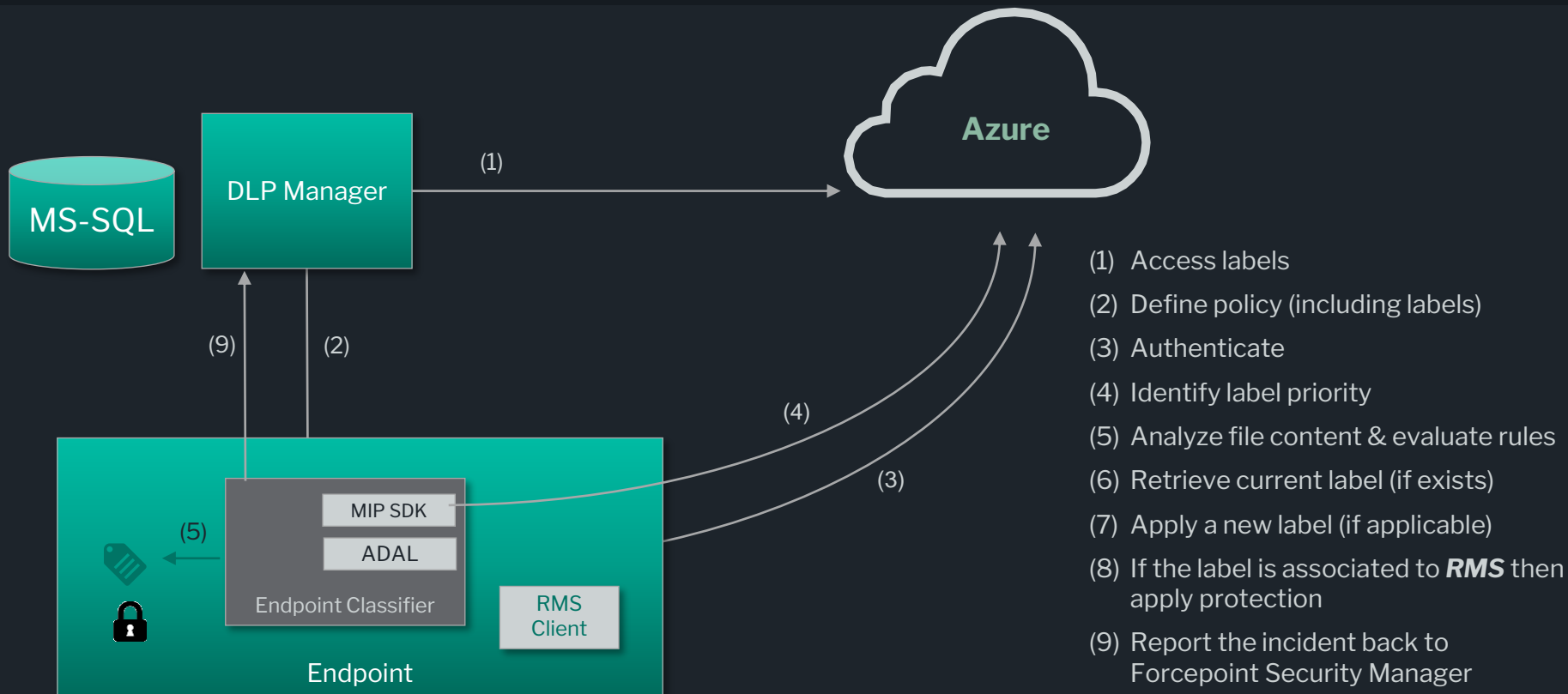


Forcepoint Security Manager (FSM)

Azure Information Protection Activity Log



How Does It Work?



Simplifying Data Classification & Labeling



Forcepoint DLP seamlessly integrates with **Microsoft Information protection** to import data classification labels

Leverage Microsoft Information Protection classification labels in Forcepoint DLP policies to protect sensitive business data



Enforce automatic labeling of sensitive documents at rest

Enable automated application of **Rights Management Templates**



Validate correct labels have been applied and **relabel** documents when required

Prevent accidental or deliberate distribution of documents labeled as sensitive



Thank you!