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

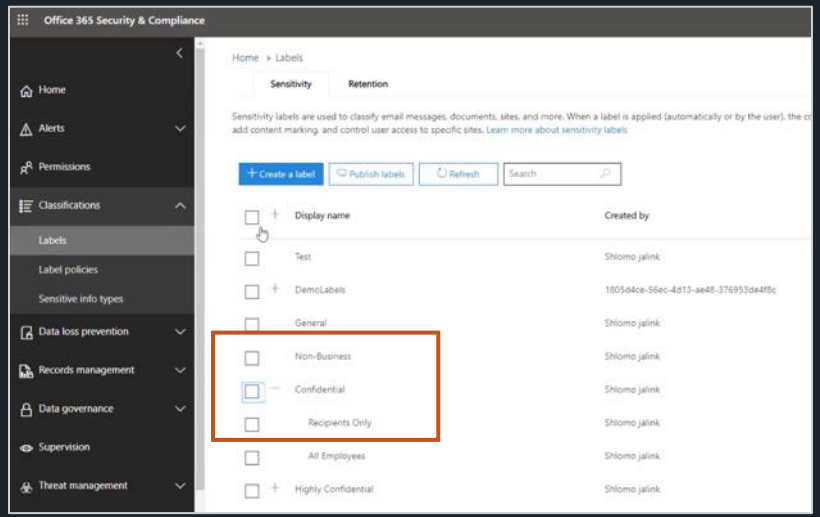
Automate detection, validation & application of classification labels

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

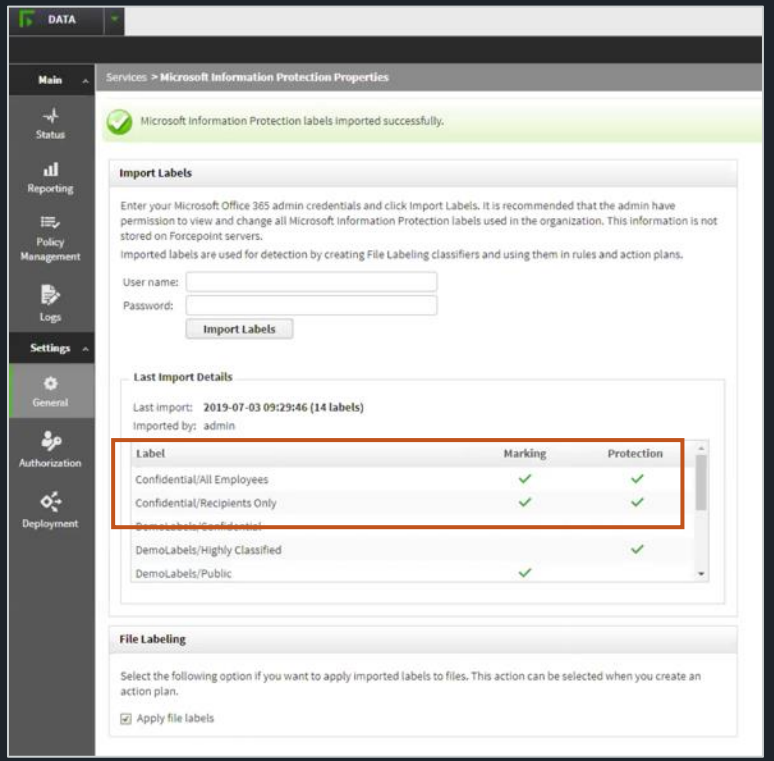
Label Schema Import from Microsoft Information Protection

- Enabled for Microsoft 0365 Security & Compliance Center
- Supported for Azure Information Protection*



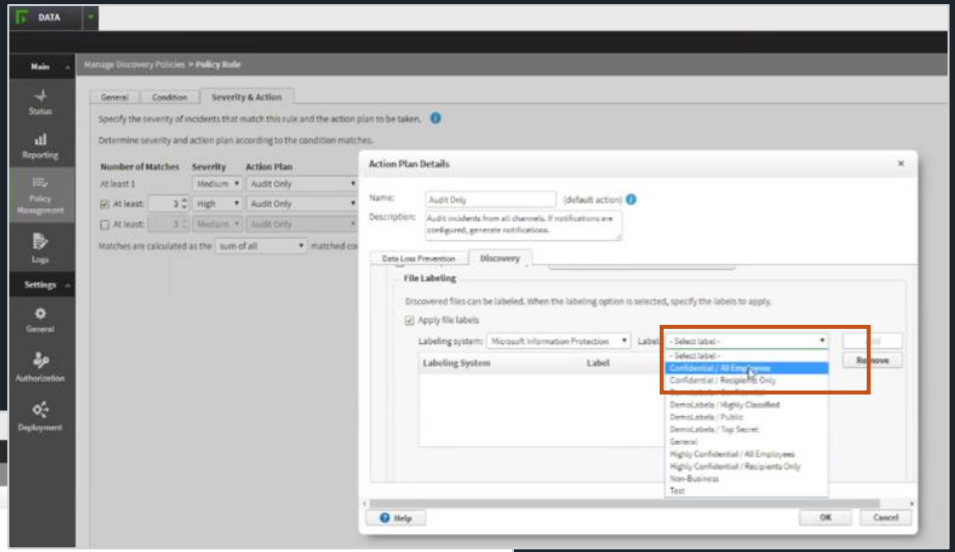
Office 365 Security & Compliance

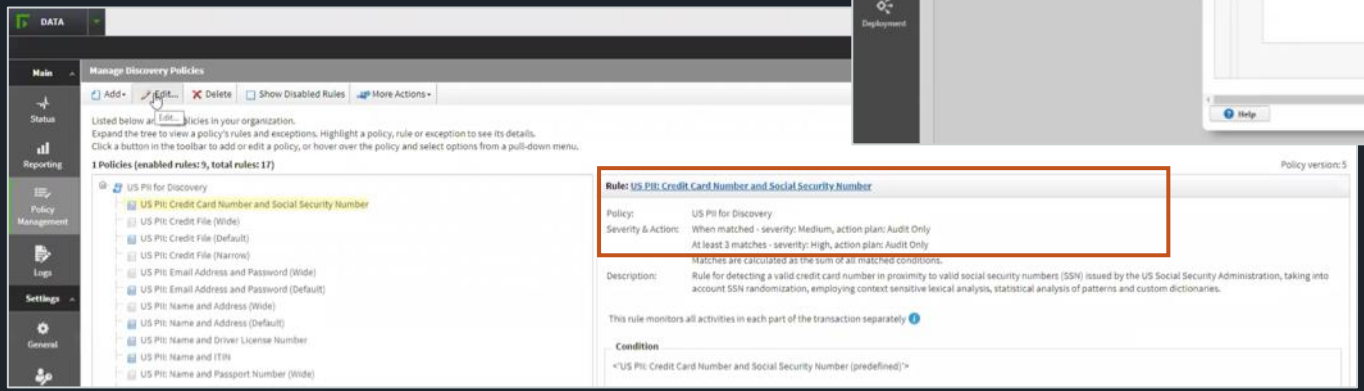
Forcepoint Security Manager (FSM)



Automate Detection and Application of Labels

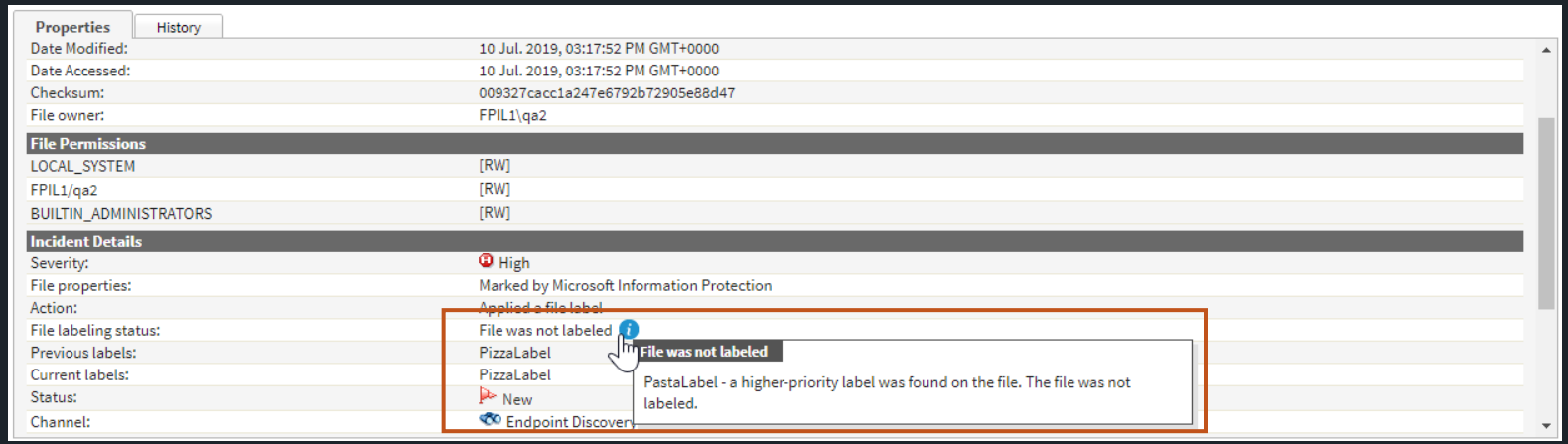
- Configure endpoint discovery
- Policy applies Microsoft Information Protection labels
- If RMS is associated with a label, the file is automatically protected.





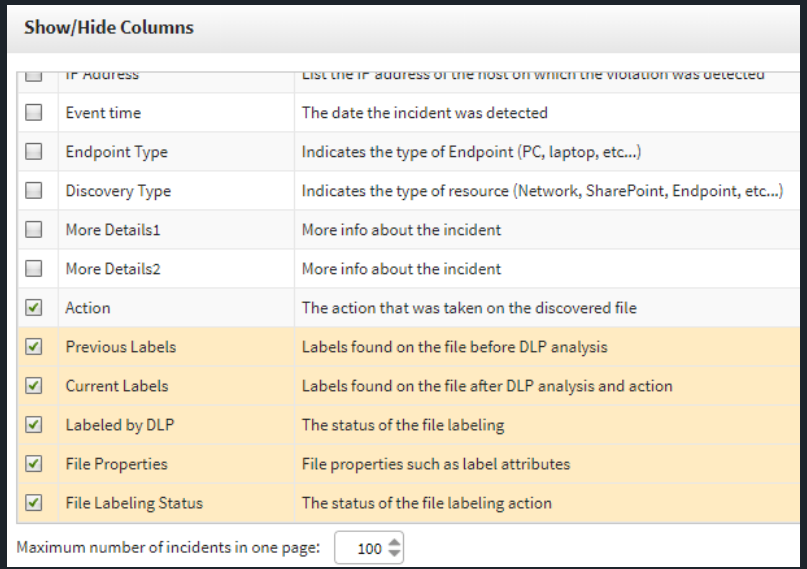
Azure Information Protection Label Priorities are Respected

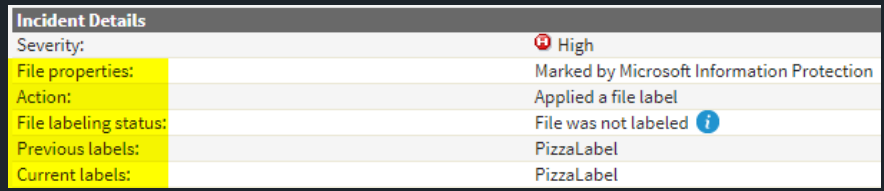
- When a document already has a label such (ie. *Confidential)* DLP can elevate the label to a higher sensitivity (ie. *Top Secret*)
- If a higher priority label is already applied to the document, then DLP won't override but will report it.



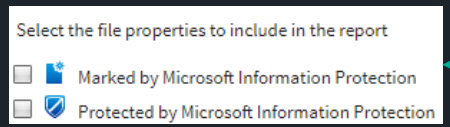
DLP Incident Reporting

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



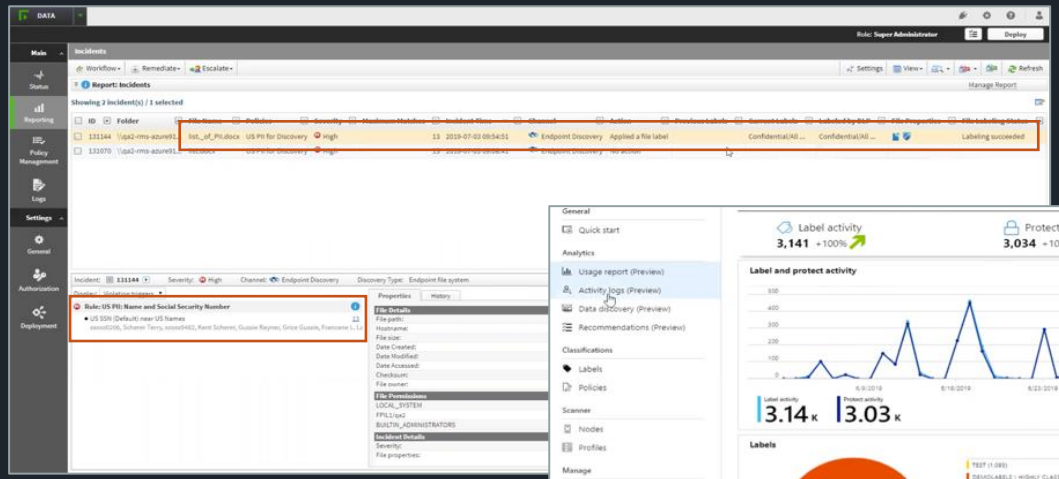


Action	Previous Labels	Current Labels	Labeled by DLP	File Properties	File Labeling Status
Applied a file label	PizzaLabel	PizzaLabel			File was not labeled
Applied a file label	PastaLabel	PizzaLabel	PizzaLabel		Labeling succeeded

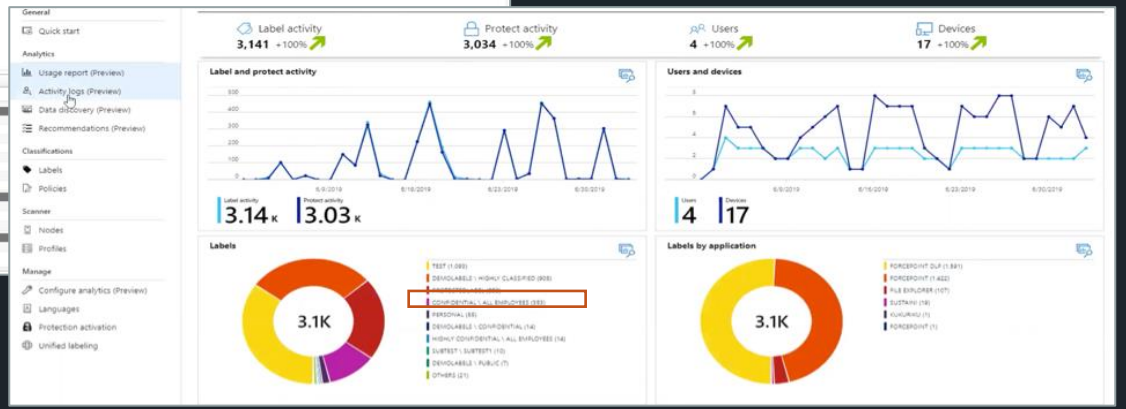


Reporting and Visibility

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

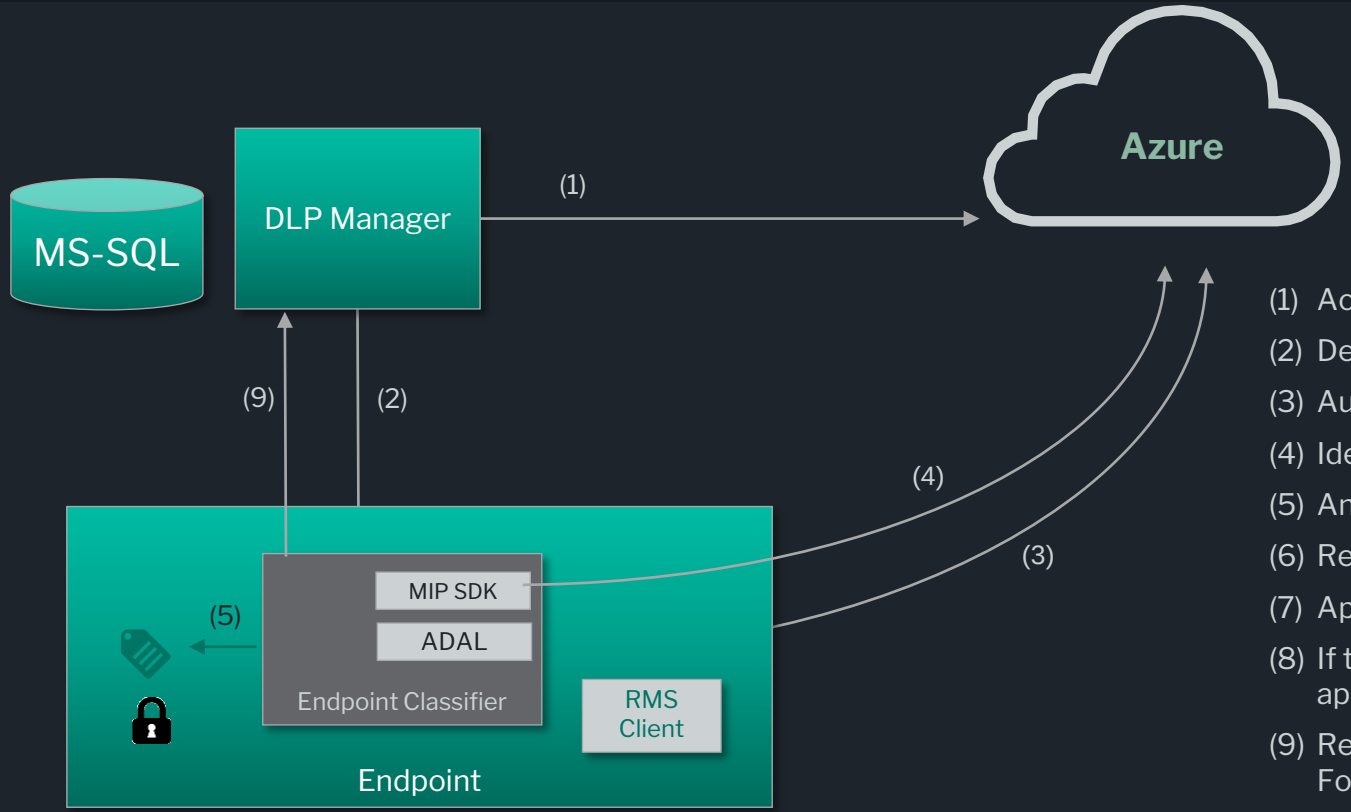


Forcepoint Security Manager (FSM)



Azure Information Protection Activity Log

How Does It Work?



(1) Access labels
(2) Define policy (including labels)
(3) Authenticate
(4) Identify label priority
(5) Analyze file content & evaluate rules
(6) Retrieve current label (if exists)
(7) Apply a new label (if applicable)
(8) If the label is associated to ***RMS*** then apply protection
(9) Report the incident back to Forcepoint Security Manager

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!

Forcepoint