Forcepoint ONE

Integrated DLP

Forcepoint ONE Integrated Data Loss Prevention (DLP) is a platform-wide capability of the Forcepoint ONE all-in-one cloud platform. It is the engine that detects sensitive data, and it is also the launching mechanism for invoking malware scanning using CrowdStrike or Bitdefender.

Key Benefits

- Define a data pattern once and apply it in multiple DLP policies for web, SaaS, and web-based private apps.
- Auto-scaling architecture on AWS lets you scan large volumes of data at rest in cloud storage in hours versus days.
- Over 100 predefined data patterns facilitate out-of-box enforcement of regional and industry standards regarding DLP for PII, PHI, and personal financial data.
- Control of any element in any web page using Field Programmable SASE Logic (FPSL).
- Minimize false positives by ensuring a pattern is matched multiple times using the Count and UniqueCount functions.
- Automatically assign a user to a risky user group when the user attempts to violate an upload or download DLP policy, thus minimizing insider threat.
- Easily detect forms data with the file fingerprinting function.
- Match text against records in a database, without uploading that database in the clear to Forcepoint ONE, using exact match data patterns and the data hasher tool.

Data patterns: the building blocks of Integrated DLP

Forcepoint ONE Integrated DLP relies on the use of predefined and custom data patterns. These data patterns are referenced in four types of Forcepoint ONE policies.

- → Proxy policies for data to and from managed SaaS applications (used by the CASB in reverse proxy and forward proxy modes).
- → Proxy policies for data to and from private web applications (used by the ZTNA gateway).
- → SWG content policies for data to and from any public web application (used by the SWG).
- → API policies for data at rest in selected SaaS and IaaS storage (used by the CASB in API mode).

Forcepoint ONE predefined and custom data patterns

Predefined Data Patterns

Forcepoint ONE Integrated DLP contains over 100 predefined data patterns that help you enforce regional and industry standards regarding DLP for PII, PHI, and personal financial data. Examples include data patterns for government tax ID numbers, passport numbers, driver's license numbers, credit card numbers, and ABA routing numbers. Other predefined patterns include hate speech, terrorism, hazardous materials, and weather and emergency.

There are also four reserved data patterns: two for invoking malware scanning using CrowdStrike or Bitdefender, a "match any" pattern, and a pattern for detecting if a file is encrypted.

Simple Data Patterns

Simple data patterns let you match text against a list of keywords, followed by a list of regular expressions, with a parameter for specifying character count proximity between the keyword and the evaluated regular expression. This is done through the Match Criteria tab as shown in the figure below.

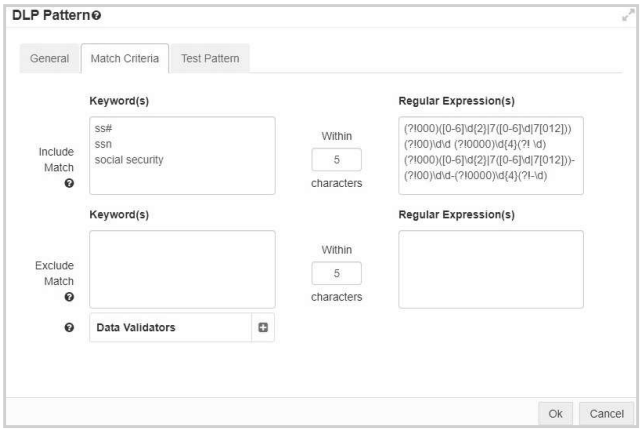

Figure 1: Match Criteria tab for a simple data pattern showing keywords, proximity, and regular expressions.

From the General tab of the simple data pattern, you can specify inclusion of text within 20 characters of the matched pattern in the event log for the match.

Figure 2: General tab for a simple data pattern showing the ability to capture contextual data.

From the Test Pattern tab of any data pattern, the administrator can test the data pattern against a text string or a file from the Test Pattern tab. Simply select either the Test Content or FIle radio button, select the file or enter the text, as appropriate, and click the Test button. In the example below, a data pattern for matching US social security numbers is tested against a matching text string.

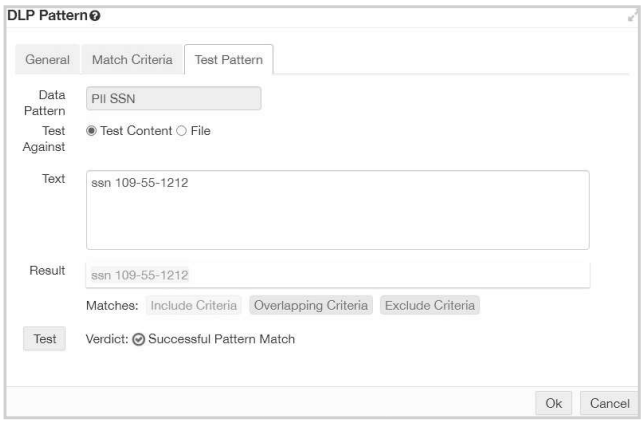

Figure 3: Test Pattern tab for a simple data pattern showing the result of a text entry test.

Advanced Data Patterns

Advanced data patterns let you logically combine the results of simple data patterns and other advanced data patterns into a single data pattern. Primitives that may be used in expressions are:

- → **Pattern counting functions:** Count and UniqueCount
- → **Arithmetic operators:** +, -, *
- → **Relational operators:** ==, !=, <, >, <=, >=
- → **Logical operators:** and, or, not
- → **Conditional operators:** if, else
- → **Other functions:** max, min

Figure 4: Match Criteria tab for an advanced data pattern.

In the above example, the Count and UniqueCount functions help minimize false positive results.

Advanced data patterns support the use of three in-pattern actions: AssignToGroup, CreateCopy, and Justify.

- → AssignToGroup will assign the user that triggered the match to be added to the specified Forcepoint ONE user group when that data pattern is used in an upload or download DLP policy.
- → CreateCopy will create a copy of the file that triggered the match and upload it to the specified cloud storage provider, login email, and directory path when that data pattern is used in an upload or download DLP policy.
- → Justify causes a pop-up dialog box to appear when the pattern matches and is used in an upload DLP policy. The user would then have to add some text explaining the reason for the upload and click OK before the upload is allowed.

Finally, advanced data patterns also support the use of LUA scripting for Forcepoint ONE Field Programmable SASE Logic (FPSL). This lets you create a data pattern that matches text in any field of any HTTP/S request method for granular control of any element in any web page. See the Forcepoint ONE Top Unique Technologies brochure for more on FPSL.

Exact Match Data Patterns

Exact match data patterns let you match text against records in a database without storing the database contents unencrypted in Forcepoint ONE's infrastructure. Simply download the data hasher tool, run the tool against the csv file containing the database records, then upload that hashed version of the csv file to Forcepoint ONE. When an exact match pattern is applied in a DLP policy, Forcepoint ONE uses the same hash code used to create the hashed version of the csv file to create hashed versions of each text field being examined. Thus, Forcepoint ONE can detect if sensitive data from the database is being leaked without every seeing that data in the clear. This ensures data privacy for the Forcepoint ONE tenant.

The exact match data pattern lets the administrator specify whether is match is triggered by any "x" columns of a row matching the examined text, or a list of specific columns that must match, or any logical combination of the above.

Figure 5: Match Criteria tab for an exact match data pattern.

File Fingerprinting Data Patterns

File fingerprinting data patterns let you match text in a document that is "x" percent similar to a single target document or a group of target documents. Simply copy all of the target documents to a common folder on your PC, download the zip file containing the Windows and Linux file fingerprinting scripts, execute the appropriate script on your PC against the file folder of the target file or files, and finally, upload the resulting fingerprint signature file to Forcepoint ONE. When a file fingerprinting match pattern is applied in a DLP policy, Forcepoint ONE records a match if the scanned file is at least "x" percent similar to any of the target files.

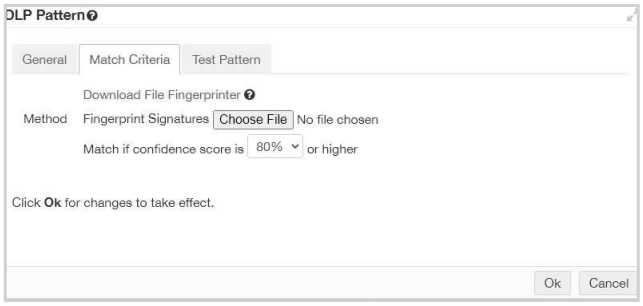

Figure 6: Match Criteria tab for a file fingerprinting data pattern.

File MIME Type Data Patterns

File MIME type data patterns let you match against the MIME type of a file. Forcepoint ONE can distinguish hundreds of MIME types, including text, Microsoft Office, Open/Libre Office, PDF, HTML, Zip, Gzip, and executables.

Figure 7: Match Criteria tab for a MIME type data pattern.

File Size Data Patterns

File size data patterns let you determine if a scanned file is greater than or equal to a specified size. These data patterns can only be used in CASB API policies.

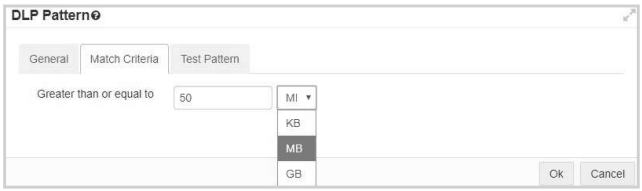

Figure 8: Match Criteria tab for a MIME type data pattern.

File Metadata Data Patterns

File metadata data patterns let you match against file metadata. This can be any file metadata including Azure Information Protection (AIP) sensitivity labels. As shown in figure 9, the file metadata data pattern Match Criteria tab lets you first upload a sample file to extract the names of all metadata tags in the document (callout 1).

Figure 9: Match Criteria tab for a file metadata data pattern.

From this information, you can click on a metadata tag name to have it automatically populate the property name field (callout 2). Then, simply add the text sting to match against in the property value field. A file metadata patch pattern can be used to match against the value of an AIP sensitivity label, as an example.

Conclusion

Forcepoint ONE Integrated DLP provides a library of many predefined match patterns for common use cases and allows creation of several types of custom data patterns for various needs, all while allowing these data patterns to be applied to data at rest in the cloud, data in motion between users and managed SaaS applications, and data in motion between users and any website.

Forcepoint ONE Integrated DLP Features and Benefits

FEATURE	BENEFIT
Platform-wide data patterns for DLP.	→ Define a data pattern once and apply it in multiple DLP policies for web, SaaS, and web-based private apps.
Over 100 predefined data patterns.	→ Facilitates out-of-box enforcement of regional and industry standards regarding DLP for PII, PHI, and personal financial data.
Field Programmable SASE Logic. Monitors, logs, and optionally blocks any HTTP/S request method based on any portion of the request method.	→ Fine-grained control of any element in any web page.
Advanced data patterns with Count and UniqueCount functions.	→ Lets you assign a user to a risky user group when the user attempts to violate an upload or download DLP policy, thus minimizing insider threat.
Exact match data patterns with data hasher tool.	→ Lets you match text against records in a database without uploading that data in the clear to Forcepoint ONE, thus ensuring data privacy and data sovereignty.
File fingerprinting data patterns.	→ Lets you match text in a document that is "x" percent similar to a single target document or a group of target documents, thus letting you detect form documents.
File MIME type data patterns.	→ Lets you identify very large files in your cloud storage and take appropriate actions.
File metadata data patterns.	→ Lets you match against any file metadata, including AIP sensitivity labels, thus providing an extra layer of DLP.
Distributed, auto-scaling architecture on AWS.	→ Allows large volumes of data at rest in cloud storage to be scanned in hours versus days.

[FP-FP ONE Integrated DLP-Datasheet-US-EN] 28Feb2022