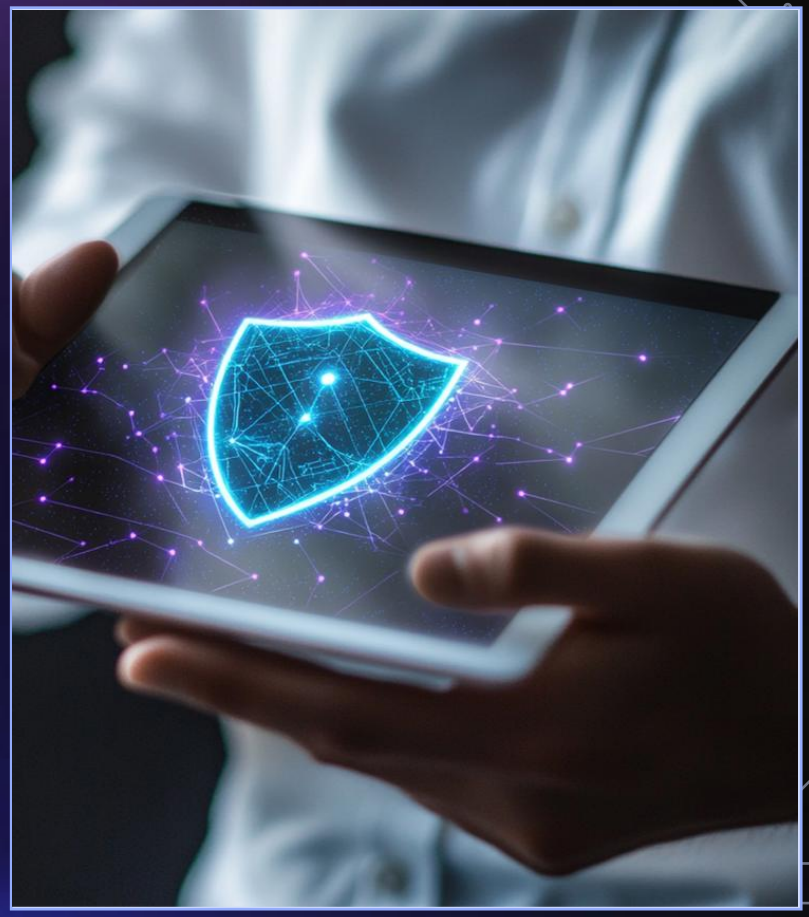
Microsoft Purview

Creating & Managing Sensitive Information Types

Contents

01

Overview of Sensitive Information Types



"Built-in vs Custom Sensitive Information Types

Built-in Sensitive Information Types

These are pre-configured types that Microsoft Purview offers, aimed at identifying common sensitive data such as credit card numbers and social security numbers.

Custom Sensitive Information Types

Custom types allow users to define their own parameters for identifying sensitive information specific to their organization's needs.

"Creating Custom Sensitive Information Types

Steps to Create

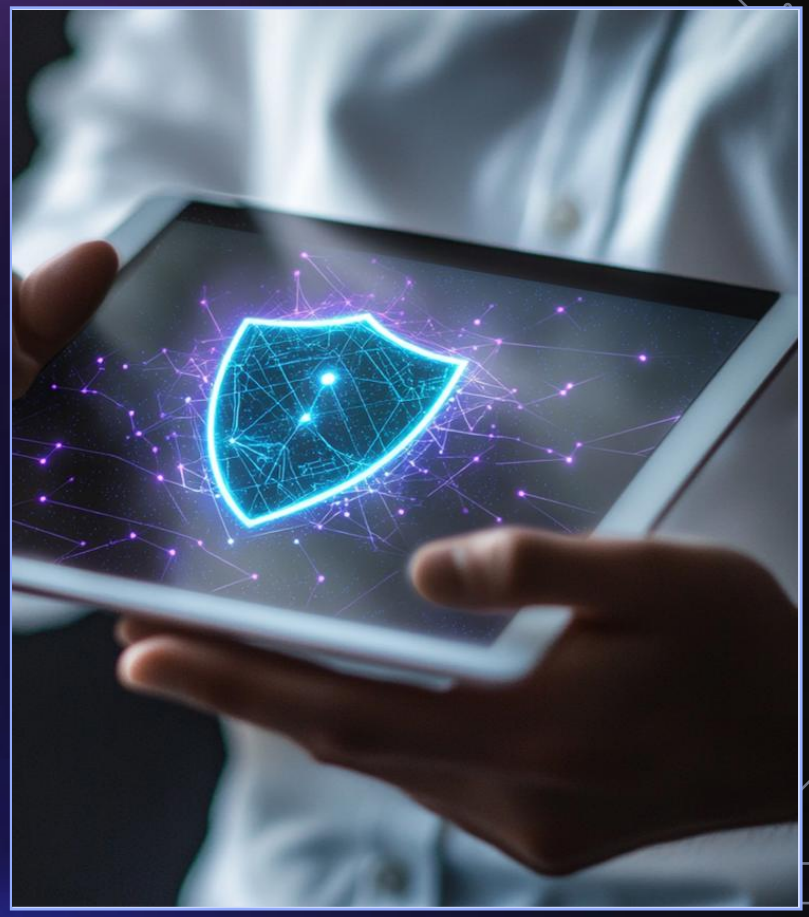
Follow detailed steps provided by Microsoft Purview to create and configure custom sensitive information types for your data protection strategy.

Example Scenarios

Examples include creating types for specific internal codes or data formats unique to your company's operations.

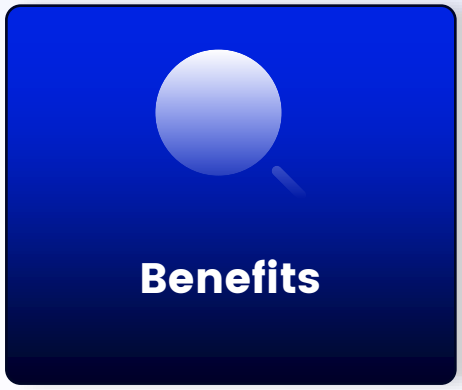
02

Document Fingerprinting



"Introduction to Document Fingerprinting

Document Fingerprinting is a method for creating a digital fingerprint of a standard document, which can then be used to identify sensitive information stored in similar formats.



Benefits include enhanced data protection by preventing unauthorized access to identifiable document types.

How to Implement Document Fingerprinting

Configuration Process

In one of the labs, we will see the step-by-step process used to configure document fingerprinting.

01

Real-World Applications

Leveraging sensitivity of a particular document template (like a standard HR form) to prevent leaking of the data contained therein. More about the “type” of document and less about a specific piece of data content.

02

03

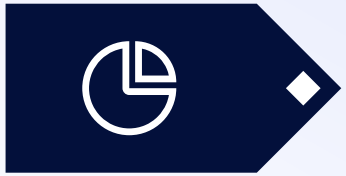
Named Entities

"Defining Named Entities

01

Understanding Named Entities

Named entities are predefined or unique information types recognizable by Microsoft Purview, such as IDs, names, or email addresses.



02

Predefined vs User-Defined

Important to differentiate between predefined named entities included in Microsoft Purview and those created by users to address specific data needs. NOTE: You cannot technically create a named entity like those provided by Microsoft, but you can satisfy the spirit of doing so by creating a custom SIT (and, optionally, creating a Trained Classifier to use Machine Learning for “fuzzier” matches).

"Utilizing Named Entities

Use Cases

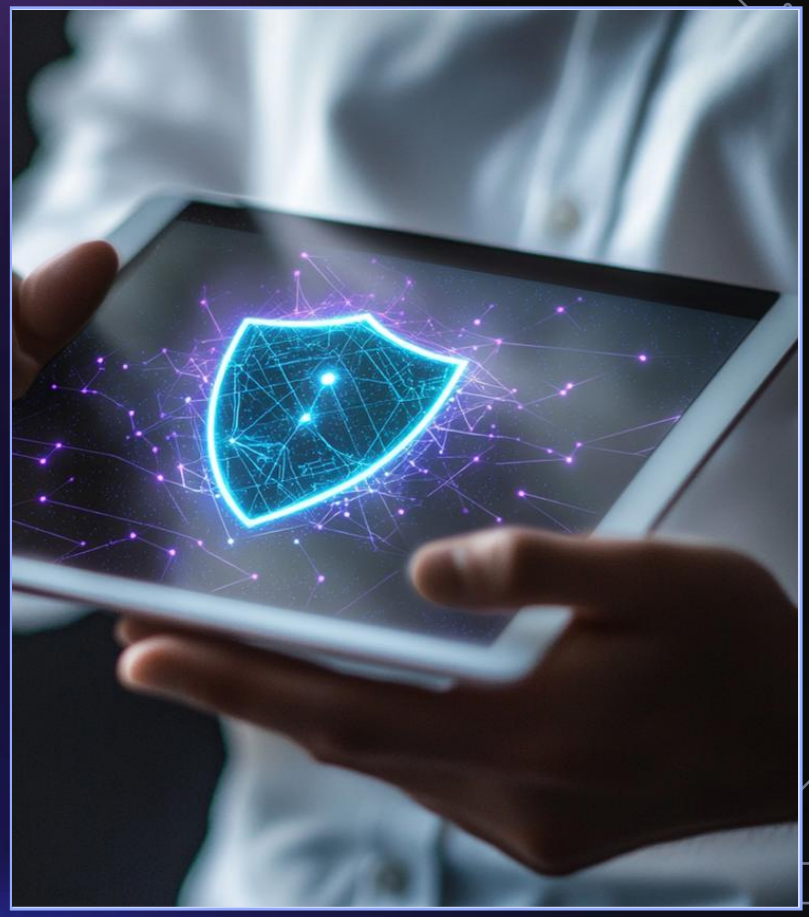
Provides another option for locating and identifying sensitive information by the type of data, especially for data types that are specific to an industry or an organization.

Best Practices

Leverage predefined types if possible (rather than reinventing the wheel). Use the customized use case for those types of data/information that are unique to your organization.

04

Sensitive Information Policies



"Creating Policies

Policy Framework

Purview offers a rich and intuitive framework for creating different policy types for different purposes. As previously discussed, those policies are mechanisms that can be used by Purview to automatically enforce compliance.

Policy Examples

Include DLP policies, retention policies, auto-labeling policies, etc. We'll see some of these in the labs.

"Managing Policies

01

Monitoring and Compliance

With policies defined and enforced, monitoring for policy adherence as a means of assessing your organization's compliance posture becomes critical. This monitoring (sometimes in the form of testing/simulation or through reports) provides visibility into what's working and where there might be compliance gaps.

02

Policy Updates

Long-term maintenance of policies is an important aspect of fully leveraging Purview. Policies are not just a "set and forget" vehicle. Monitoring and validation will help highlight areas requiring additional "care and feeding".

"Summary Reports

Generating Reports

Reports in Purview and explorers (like the Data explorer and Activity explorer) can provide invaluable visibility into how your configured policies and defined SITs are performing.

Report Features

These reports and explorers (with the right permissions configured) can allow an administrator to drill down into specific content that is triggering a policy or compliance action.

Thanks