VERITAS

From Classification to Compliance

Microsoft Purview information protection labels enhanced by Veritas Data Insight.

Solution Brief | February 2024

Summary

In a time when data breaches are expensive and frequent, effective data management has become essential. This white paper outlines a comprehensive approach to data protection by combining the capabilities of Veritas Data Insight with the sensitivity labels of Microsoft Purview. This partnership offers businesses:

- A streamlined approach to accurate data classification and security compliance
- Enhanced data protection measures powered by a sophisticated, unified labeling mechanism

By harnessing Veritas Data Insight, organizations can amplify the effectiveness of Microsoft Purview's labeling, leading to improved data security and compliance management.

Importance of Data Classification and Labeling

Effective data management is anchored in the fundamental practice of classifying and labeling data appropriately. Microsoft Purview's sensitivity labels are essential tools that empower organizations to categorize their data, marking the information based on its level of sensitivity. These categorizations are critical; they dictate how data is handled, shared, and secured, ensuring that sensitive information receives the necessary safeguards.

Incorrect labeling or failure to label data can lead to serious compliance breaches or security oversights. An example of the risk posed by mislabeling or not labeling data is non-compliance with regulations such as GDPR or HIPAA. For instance, if personal data is not labeled as *Confidential*, it might not receive the required level of encryption or access control, leading to potential data breaches and heavy fines.

This approach is crucial to safeguard data and ensure compliance with strict data protection rules. It requires consistent attention from the moment data is created until it is securely disposed of.

Veritas Data Insight enhances this essential process through the Veritas Classification engine, elevating the precision of data categorization. The Classification engine provides an advanced mechanism to consistently assess and adjust data labels, ensuring ongoing accuracy as organizational needs and regulatory requirements evolve.

By integrating Veritas Data Insight with Microsoft Purview's labeling system, organizations are equipped to manage their data with greater efficacy, maintaining a strong stance on data security and regulatory compliance.

Empowering Label Management with Veritas Data Insight

Veritas Data Insight is at the cutting edge of improved data governance, with its sophisticated label management features that are tailored to address the detailed aspects and capabilities of Microsoft Purview Information Protection (MPIP) sensitivity labels.

Label Detection and Insights

Data Insight surveys the enterprise's data landscape, pinpointing and documenting existing MPIP labels. It guarantees thorough visibility across data repositories, recognizing the existence of sensitive documents and ensuring they are managed correctly.

Responsive Label Modification

Leveraging the Veritas Classification engine, Data Insight provides a responsive mechanism for modifying MPIP labels. This process is fine-tuned through policies that recognize and react to shifts in data classification, effectively recalibrating the associated labels to match the updated data sensitivity levels.

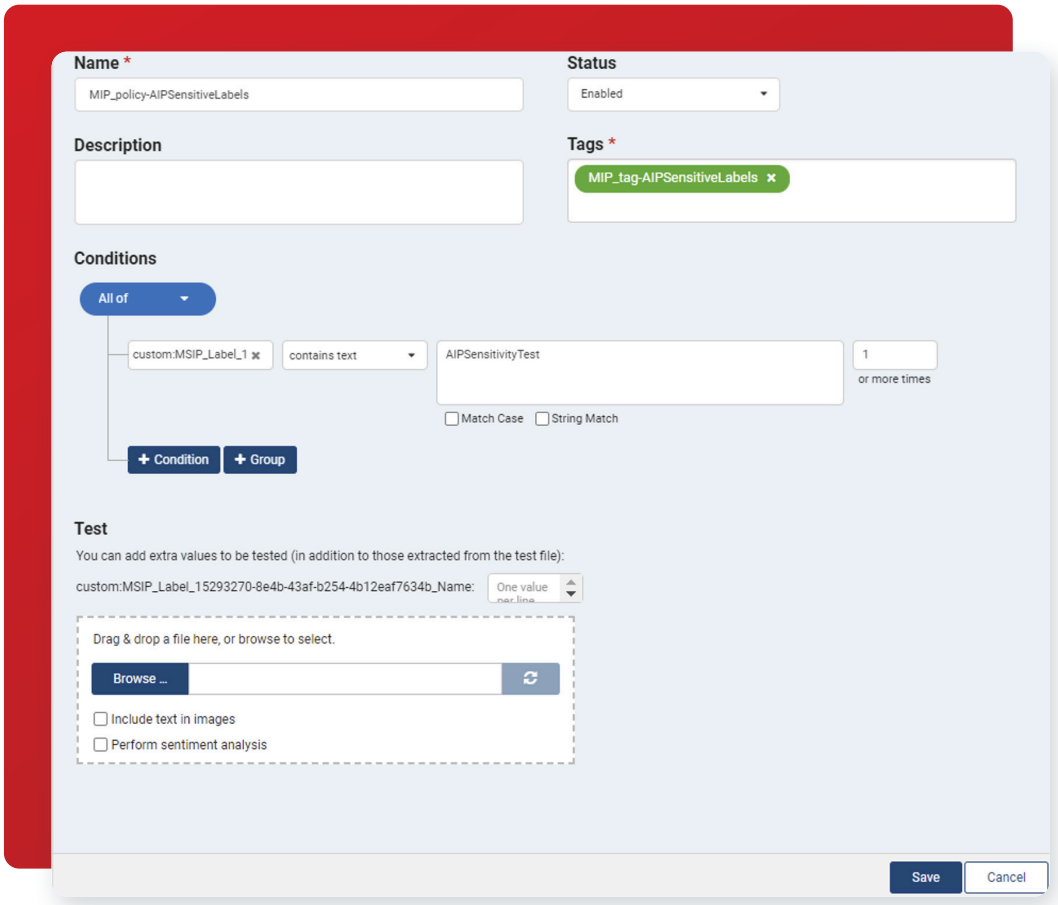

Figure 1. Configuring policies using Veritas Classification engine for MPIP labels

Strategic Label Application

Data Insight extends its capabilities to the proactive labeling of documents. It identifies files and their MPIP labels, enabling the labeling of unlabeled content and the correction of mislabeled data including those on CIFS devices. This action fortifies the organization's data security strategy, particularly for shared storage systems where sensitive data might otherwise remain unprotected.

Correcting labeling errors — including non-classification and misclassification — is paramount to uphold security standards and achieve regulatory compliance.

Automated Reclassification and Remediation

The true power of Data Insight lies in its automated reclassification capabilities. Users can easily set up rules within the system to auto-classify documents according to their content. With a simple setup process, sensitive files that are initially unclassified or misclassified can be detected and labeled correctly, without manual intervention.

To streamline the process of applying MPIP labels across your data estate, Veritas Data Insight offers a powerful feature: the Data Query Language (DQL) report for automation. Here's a step-by-step guide to create a DQL report that automates the application of MPIP labels to your sensitive files:

Step 1: Initiate DQL Report Creation

From the Veritas Data Insight dashboard, navigate to the *Custom Reports* section and select *DQL Report*. This area allows for the creation and management of custom reports based on specific criteria.

Step 2: Configure Report Parameters

Within the *Create DQL Report* interface, direct your attention to the *Query* tab. Here you can utilize templates for various data classification scenarios. For instance, select *Classification* from *Category,* and a template such as *[On-premise] Sensitive file unlabeled* to target sensitive documents that lack MPIP labels.

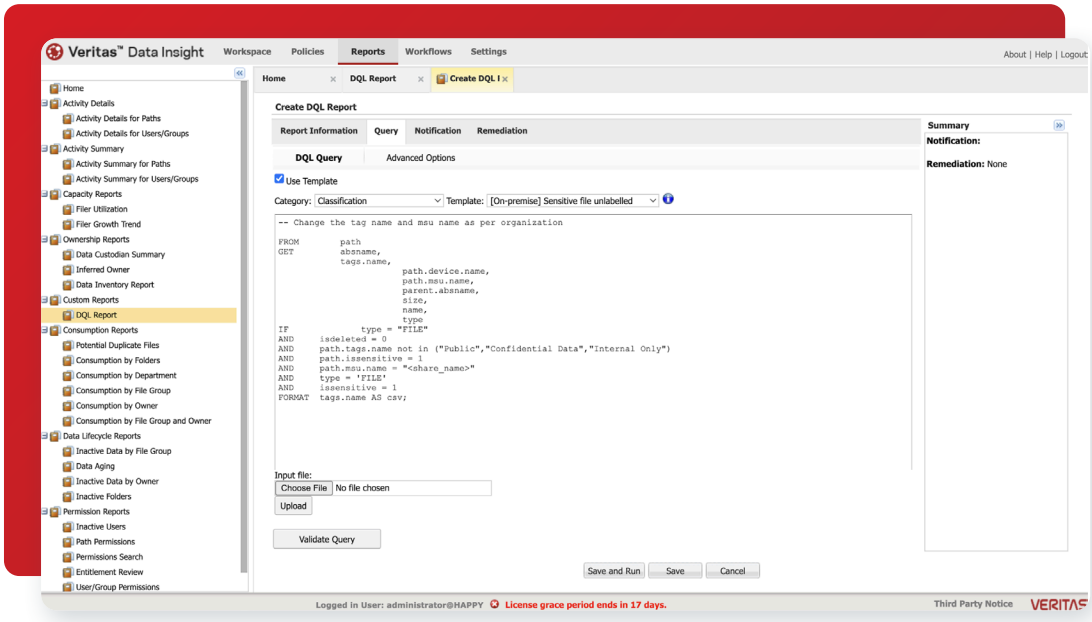

Figure 2. Creating a DQL report to automate MPIP labels application

Step 3: Customize Query for Your Environment

Modify the query parameters to suit your organization's unique environment. Adjust the *path.tags.name and path.msu.name* to match the specific labels and shares relevant to your data governance framework.

Step 4: Set Up Remediation Actions

Switch to the *Remediation* tab. Choose the *Set Microsoft Purview Information Protection (MPIP) Label* action. From the dropdown, select the appropriate label that aligns with the sensitivity of the content being targeted by the report.

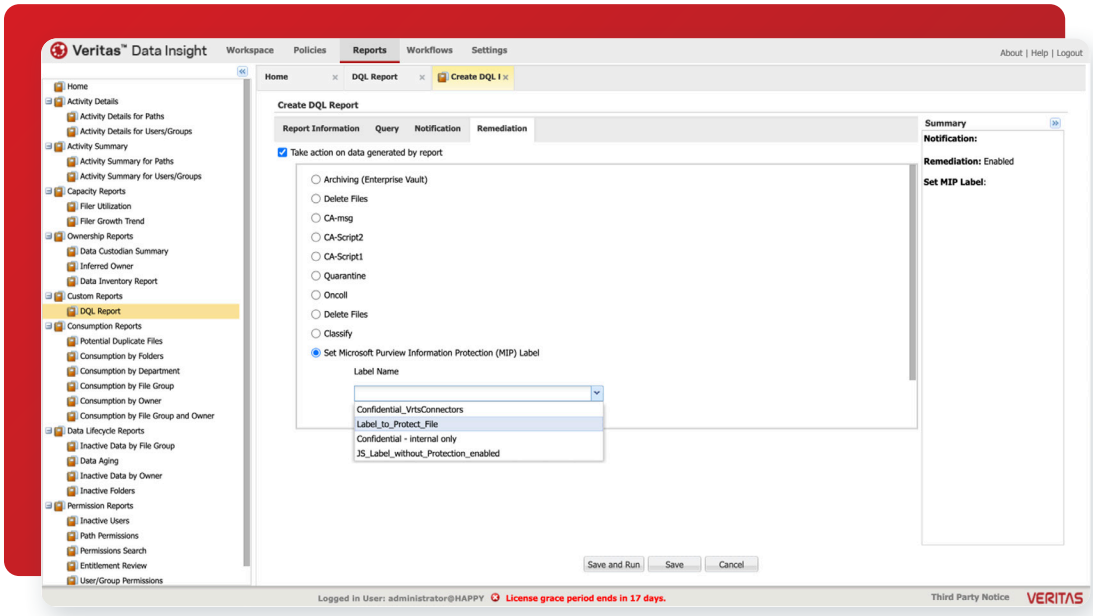

Figure 3. Creating a DQL report to automate MPIP labels application

Step 5: Justification and Execution

Before executing the report, provide a justification for the remediation action. This step is crucial for auditing and compliance purposes. Once complete, save your settings and run the report.

As the report executes, it will automatically apply the chosen MPIP label to all files that meet the criteria specified in the DQL query. This automated labeling ensures a consistent and compliant data protection stance across your organization's digital assets.

Data Insight supports applying MPIP labels to Microsoft Office documents and PDF files, syncing with the label configurations in a customer's Office 365 environment. While it primarily operates with real-time synchronization in environments with internet access, it also has the capability to handle labels in internet-isolated settings. In such cases, labels can be pre-fetched and used within Data Insight, ensuring data classification and protection continues effectively, regardless of the connectivity scenario. This flexibility makes Data Insight adaptable to various operational needs, emphasizing seamless integration with the Azure Compliance Center for up-to-date label management.

Automated Security Actions Through Label Management

The integration of Veritas Data Insight with MPIP labels is not just a matter of label management, it's about activating a security framework that responds to changes in data classification. This dynamic approach is pivotal to the Veritas remediation narrative, ensuring that as data is reclassified — whether due to policy updates or evolving content — security measures are immediately and automatically adjusted.

Proactive Protection Measures

In the realm of data security, proactive measures are essential to safeguard sensitive information. The collaboration between Veritas Data Insight and MPIP labels exemplifies this approach. Through this integration, when a document's MPIP label is updated to a higher sensitivity level, it signals a need for enhanced protection measures. This label change enables a series of preemptive actions to secure the document, such as adjusting access permissions and applying additional security protocols. These measures are tailored to align with the newly assigned level of sensitivity, ensuring that each piece of data receives the precise level of protection it requires. This fortifies data against potential threats and aligns with evolving compliance and regulatory requirements, thus maintaining a robust and adaptive security posture.

Encryption as a First Line of Defense

Veritas Data Insight is instrumental in the governance of document security labels. When a change in a document's sensitivity is indicated, an MPIP label can be updated through Data Insight. This action triggers Microsoft Purview's security measures, which may include encrypting the document. Such encryption ensures that the document can only be accessed with the appropriate decryption key, significantly enhancing the document's security against unauthorized viewing or access.

Watermarking for Traceability and Deterrence

Through the management of MPIP labels, Data Insight enforces the application of watermarks on sensitive documents. The updated labels prompt Microsoft Purview to implement watermarks, which serve as a measure to trace document origin and discourage unauthorized distribution.

Throughout this process, Veritas Data Insight provides a user-centric interface that allows for on-demand label remediation actions, all underpinned by role-based access control to maintain security and compliance integrity.

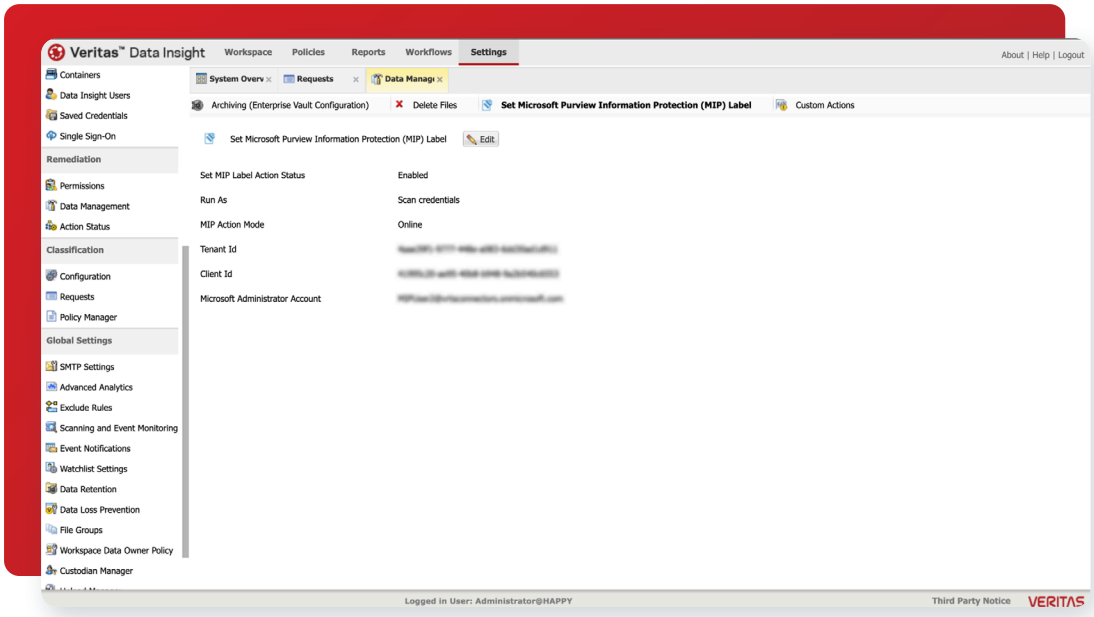

Figure 4. Setting an MPIP label in Veritas Data Insight

By integrating these actions into their data governance systems, Veritas Data Insight helps organizations quickly fix security weaknesses. This makes the process of correcting issues a key part of their overall approach to data security.

Conclusion

We have explored the transformative integration of Veritas Data Insight with MPIP labels, a synergy that redefines the landscape of data governance and security. The combination of Data Insight's sophisticated classification capabilities and MPIP's robust labeling framework provides a comprehensive solution that anticipates and meets the needs of modern data protection.

This integration enables organizations to automate the classification and protection of sensitive data, streamline compliance efforts, and fortify their security posture with a suite of proactive measures.

In conclusion, organizations looking to elevate their data governance strategies will find a powerful ally in the Veritas Data Insight and MPIP integration. It is an essential step toward a more secure, compliant, and resilient future for data management.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V2083 02/24