iboss®

FEATURE BENEFIT SHEET

Network DLP for Microsoft Purview Labeled Documents

Extend Microsoft Purview Data Labeling to the Network: Real-Time File Upload Blocking with MIP-Driven DLP

The Challenge

Organizations rely on Microsoft Purview, formerly Microsoft Information Protection (MIP), Data Labels to classify and protect sensitive data, but preventing labeled data from leaking outside Microsoft environments via the network remains a challenge. Sensitive files can still be transferred to unauthorized destinations like personal cloud storage, unapproved SaaS apps, or external devices. A 2024 IBM report found that 40% of data breaches involved data stored across multiple environments and more than one-third of breaches involved shadow data. The need for extending Purview labels beyond Microsoft environments is critical for reducing risk and ensuring compliance. Security teams need real-time enforcement of Purview labels to block unauthorized data movement and ensure compliance. Without automated label synchronization across security platforms, organizations face complex policy management, increased risk, and gaps in their Zero Trust strategy.

The Solution

The iboss **Network DLP for Microsoft Purview Labeled Documents** solution extends Microsoft Purview Data Labels by enforcing real-time inline DLP policies across web, cloud, and network traffic. Unlike out-of-band DLP, iboss automatically synchronizes Purview labels and applies them to inline policies to block unauthorized data transfers. This ensures that labeled files cannot be uploaded to Shadow IT, personal SaaS apps, or external storage. Dynamic Zero Trust access policies control file movement based on users, groups, destinations, and labels. By integrating seamlessly with Microsoft Purview, iboss reduces complexity, enhances compliance, and prevents breaches. Organizations gain proactive security, automated protection, and greater control over their sensitive data. By leveraging Microsoft Purview's existing label structures, iboss enables organizations to reduce complexity, ensure compliance, and prevent costly data breaches.

$5M

The average cost of a data breach reached nearly **$5 million** in 2024, a 10% increase from 2023

40%

40% of breaches involved data stored across multiple environments

33%

One in three data breaches involved unmonitored shadow data

Why iboss?

Real-Time Inline Data Protection:
Extend Microsoft Purview label enforcement beyond email and limited SaaS apps to secure all network data transfers, including unmanaged destinations.

Seamless Microsoft Integration:
Automatically synchronize Purview labels with iboss, extending Microsoft DLP policies for enhanced Zero Trust enforcement.

Block Unauthorized Data Transfers:
Stop labeled documents from being uploaded to unapproved cloud storage, personal SaaS apps, or external devices.

Fully Unified + Fully Distributed

Unified Controls:
Enforce real-time policies based on Microsoft Purview Data Labels, preventing unauthorized data transfers across any device and location.

Unified Protection:
Automatically classify, detect, and block the movement of labeled sensitive data to unapproved destinations, reducing data loss risks.

Unified Visibility:
Provide real-time alerts and audit logs for security teams, ensuring continuous monitoring of sensitive data movement and enforcement.

FEATURE BENEFIT SHEET

Network DLP for Microsoft Purview Labeled Documents

Extend Microsoft Purview Data Labeling to the Network: Real-Time File Upload Blocking with MIP-Driven DLP

Feature Capability

Inline DLP Enforcement Using Data Labels

- Prevent unauthorized data transfers by enforcing Microsoft Purview labels within real-time, inline security policies.

Automatic Purview Label Synchronization

- Seamlessly synchronize Microsoft Purview Data Labels with iboss, ensuring continuous enforcement of data security policies.

Real-Time Data Loss Prevention

- Detect and block attempts to move labeled sensitive data to unapproved destinations before breaches occur.

Shadow IT Protection

- Prevent the transfer of classified documents to unauthorized cloud storage services and personal SaaS applications.

Zero Trust-Based Label Policies

- Dynamically apply data transfer policies based on users, groups, destinations, and document classification labels.

Seamless Microsoft Integration

- Extend Microsoft Purview security beyond Microsoft environments by integrating Purview labels with iboss Zero Trust policies.

Real-Time Alerts

- Send immediate alerts to designated staff with contextual details on detected risks.

Compliance & Audit Readiness

- Comprehensive visibility into data movements and ensures regulatory compliance across security frameworks.

Feature Benefit

Prevent Unauthorized Data Transfers

- Ensure that sensitive labeled documents cannot be sent to unauthorized destinations.

Streamlined Policy Management

- Labels created in Microsoft Purview are automatically applied within iboss policies, eliminating manual configuration.

Immediate Risk Reduction

- Stop data loss at the source by applying security controls as files move across networks.

Prevent Unapproved Cloud Storage

- Block attempts to transfer sensitive labeled files to unauthorized SaaS applications like personal Dropbox or Google Drive.

Adaptive Access Control

- Dynamically adjust access and transfer permissions based on user, role, and document classification.

Extends Microsoft Purview Security

- Enhance out-of-band Purview protections with real-time inline enforcement.

Instant Risk Notifications

- Facilitate quick decision-making and rapid response to potential threats.

Ensures Regulatory Compliance

- Meet regulatory requirements such as GDPR and HIPAA by preventing unauthorized data transfers.

Conclusions

Microsoft Purview Labels Alone Are Not Enough

While Purview classifies sensitive data, it lacks real-time enforcement across cloud and web, leaving data vulnerable to potential exfiltration.

Inline, Real-Time Protection Is Critical

Blocking unauthorized data transfers as they happen ensures sensitive information remains secure and prevents compliance violations.

Seamless Integration Maximizes Security & Efficiency

Automatically synchronizing Purview labels with iboss enforces Zero Trust policies without adding complexity, manual overhead, or disrupting existing workflows.

Contact Us

Additional Resources

Security Insights & Incident Management
GenAI Risk Module

Contact Us

The iboss Zero Trust SASE platform delivers comprehensive security and compliance from a single, centralized console. With built-in encryption, seamless policy enforcement, and full visibility across your Users & Applications real-estate, the platform simplifies management while protecting sensitive data across all devices and locations.

Request a Demo Today