Microsoft

CAPABILITY SOLUTION BRIEF

Inline Data Discovery for Microsoft Purview

Extend Microsoft Purview's reach to the network, preventing data loss and gaining visibility into all transfers.

Overview

The Problem

Microsoft Purview offers strong tools for classifying and protecting data within Microsoft environments. Yet, organizations also need protection for sensitive data when it moves beyond Microsoft's ecosystem over the network.

Unseen data transfers lead to security risks, compliance issues, and operational blind spots. For example, when a user transfers a labeled, sensitive document – say, to a personal Dropbox or Google Drive - this visibility is required to prevent data breaches and compliance violations. Leading to...

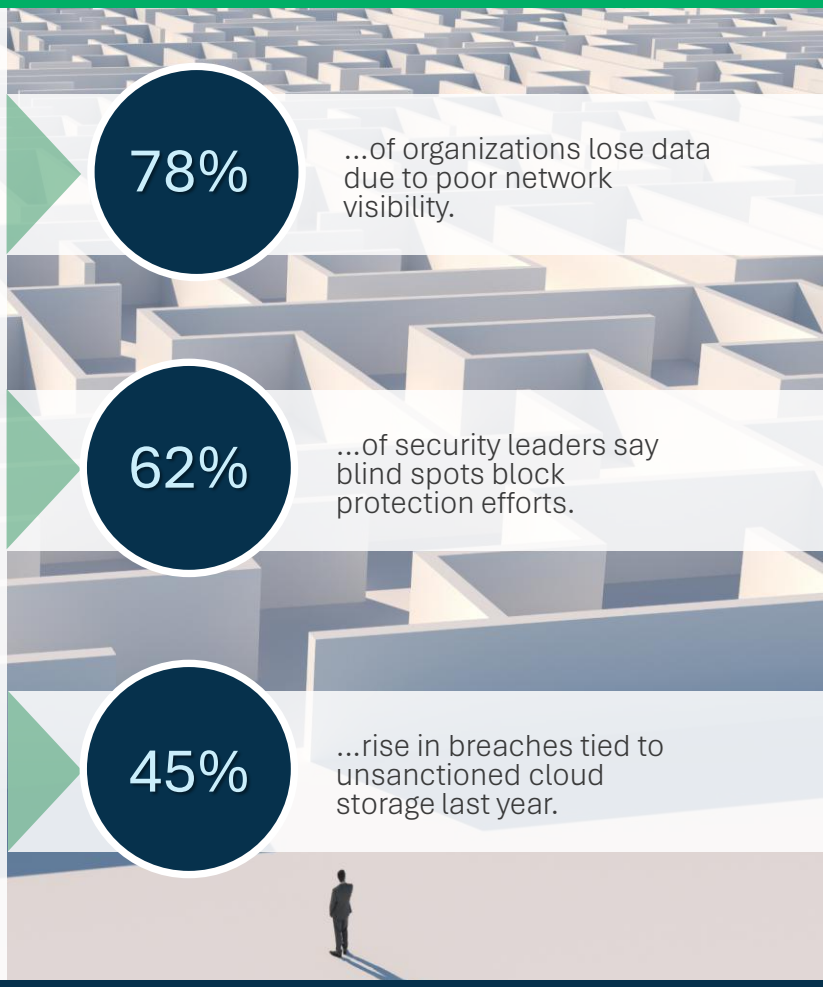
The Impact

Unmonitored network transfers weaken data protection efforts, creating serious risks for organizations.

Data Loss:
Sensitive data escapes to unsafe destinations, inviting breaches and fines.

No Visibility:
Teams cannot track data outside Microsoft, missing key threats.

Weak Controls:
Without instant blocking, risky transfers persist unchecked.



Solution Overview

The iboss Zero Trust SASE platform integrates with Microsoft Purview to address this gap. With the new Inline Data Discovery capability, iboss syncs Purview policies via API, bringing them into its inline inspection framework.

Sitting in the data path, iboss sees all transfers - whether to personal cloud storage, SaaS apps, or elsewhere - and applies real-time controls. iboss decrypts HTTPS traffic, inspects content,& extracts files or text matching Purview policies - It then submits this data to Purview for analysis, giving Microsoft visibility into transfers

Beyond visibility, iboss enforces native inline DLP policies in parallel to Microsoft Purview submissions, blocking risky transfers. This dual action - enriching Purview's insights while stopping leaks - sets iboss apart.

Key Capabilities

Policy Synchronization

Pulls Purview policies automatically for uniform network enforcement.

Real-Time DLP Controls

Blocks risky transfers instantly after inspecting all traffic using iboss built-in DLP Policies

Enhanced Visibility

Sends extracted data to Purview, revealing all transfer details.

Microsoft

CAPABILITY SOLUTION BRIEF

What We Solve	How We Solve It	Customer Benefits
Policy Synchronization	Organizations struggle to prevent sensitive data from being transferred to unauthorized locations in real-time, leading to potential breaches and compliance violations.	iboss syncs Purview policies and scans all traffic, sending matches to Purview for review.	Security teams see all data movements, spotting threats and ensuring compliance fast.
Real-Time DLP Controls	Sensitive data flows to unsafe destinations without real-time stops, raising risks.	iboss uses inline DLP to halt unauthorized transfers, decrypting traffic for inspection.	Data stays secure, cutting breach risks and compliance costs without manual effort.
Enhanced Visibility	Purview's limited scope skips network paths, leaving gaps in protection.	iboss extends Purview to the network, enforcing policies on all transfers consistently.	Unified protection simplifies security and boosts value from Microsoft tools.

Why Now?

Remote work and cloud growth push data across networks daily. Regulations tighten, and breach costs soar. Organizations must close visibility gaps now to protect data and avoid penalties.

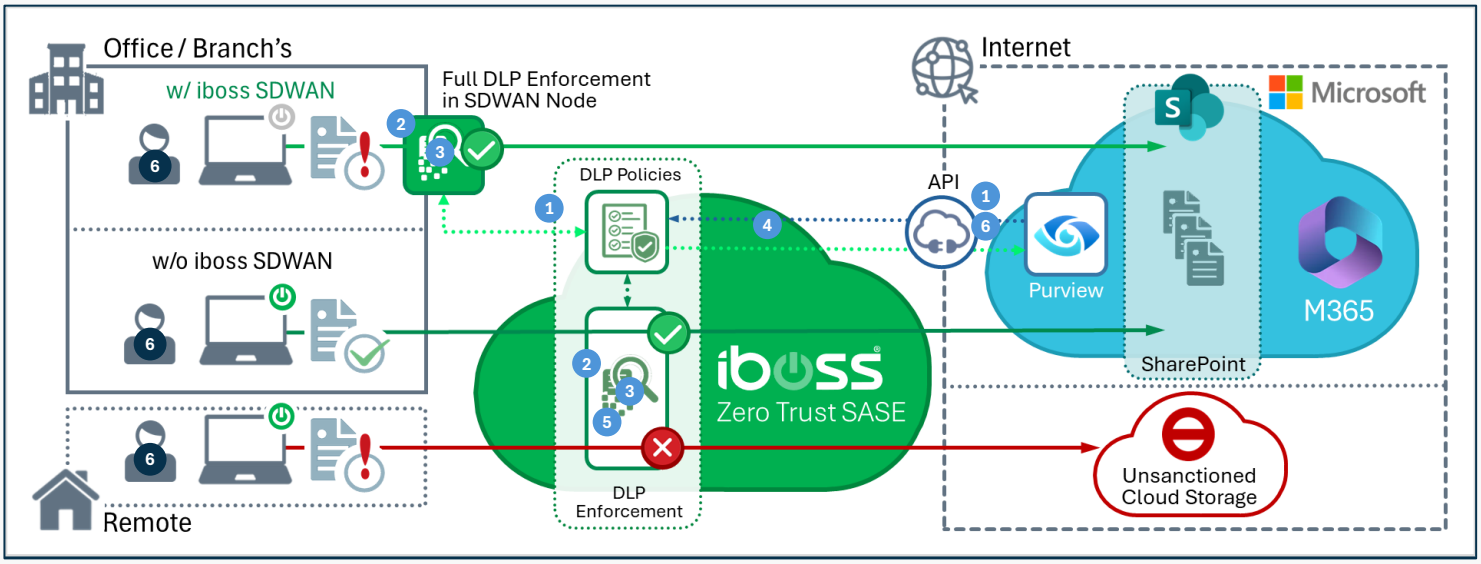
Additional Resources

Inline Data Discovery for Microsoft Purview Value Brief

Visit iboss.com/ for more information

Request a Demo Today

How It Works



1. **Policy Sync:**
   iboss links to Purview via API, syncing policies for network use.
2. **Traffic Decryption:**
   iboss decrypts HTTPS traffic to check for policy matches.
3. **Content Extraction:**
   iboss pulls files or text from matching transfers.
4. **Purview Submission:**
   Extracted content goes to Purview for analysis and logging.
5. **Instant Blocking:**
   iboss applies DLP rules to stop risky transfers on the spot.
6. **User Mapping:**
   iboss turns Azure GUIDs into readable names for clear reports.

Unified Controls

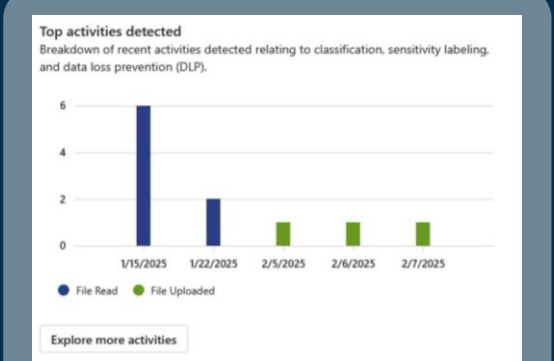
Ties into iboss policy engine for consistent rules across all traffic.

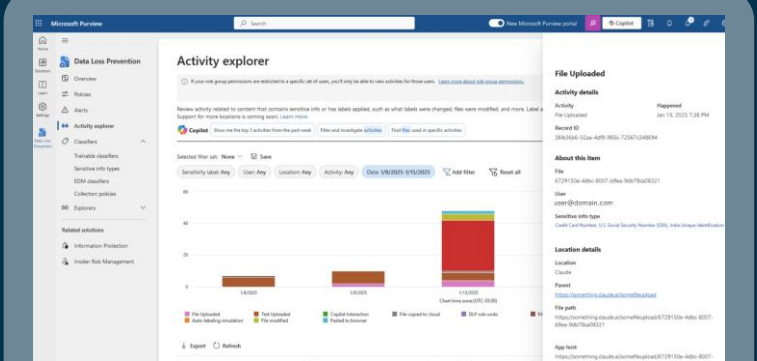
Unified Protection

Boosts Zero Trust by adding data transfer controls to access security.

Unified Visibility

Enhances iboss logs with deep insights into data and violations.



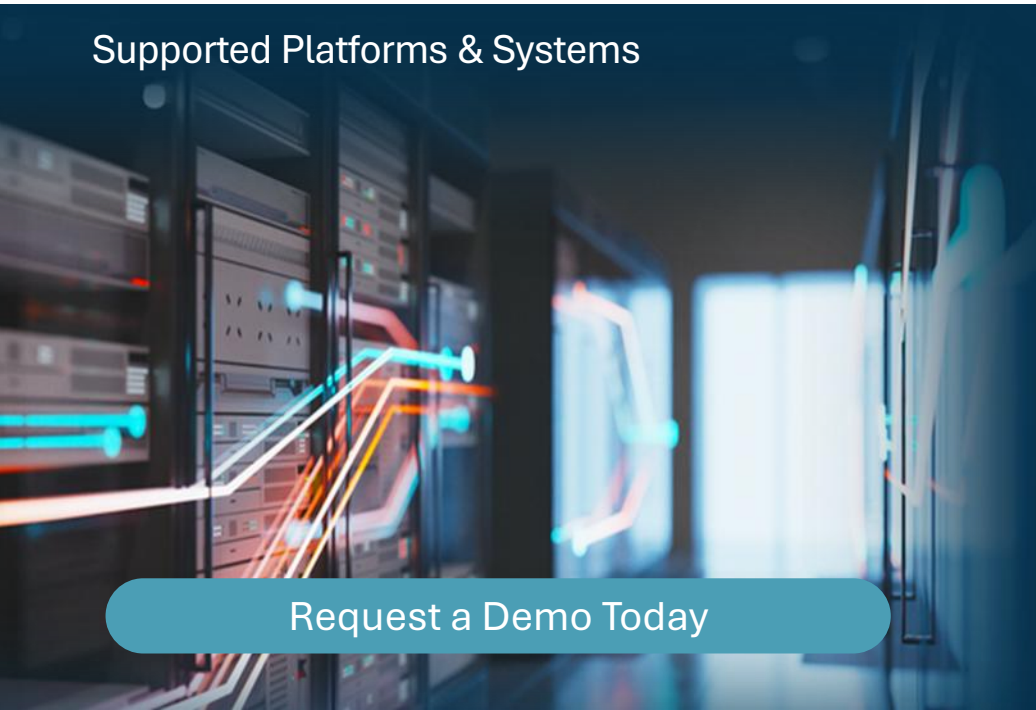


Microsoft

CAPABILITY SOLUTION BRIEF

Feature Details

Feature	Description
Policy Auto-Sync	Syncs Purview policies via API for seamless rules.
HTTPS Decryption	Checks encrypted traffic for sensitive data moves.
Content Extraction	Grabs files matching Purview policies for review.
Real-Time DLP	Stops unauthorized transfers with inline controls.
User Mapping	Turns Azure GUIDs into names for easy logs.
Label Detection	Spots and blocks sensitively labeled document transfers.
Inline CASB	Controls cloud apps beyond Microsoft with precision.
OCR Detection	Finds sensitive data in images and scanned files.
Global Scale	Uses iboss cloud for limitless traffic handling.
Single Console	Manages all security from one dashboard.



Supported Platforms & Systems

Endpoint Cloud Connector

- Windows
- macOS
- Linux
- ChromeOS
- iOS
- Android

Network Connector

- AWS
- Docker
- VMware OVF

Policy Enforcement Points

- iboss Global Cloud (100+ POPs)
- Azure
- Private Locations

Request a Demo Today

Microsoft

CAPABILITY SOLUTION BRIEF

Feature Details

iboss is a Zero Trust SASE platform that secures all connections through a single, cloud-based service. It replaces multiple point products such as VPN, Secure Web Gateway, SD-WAN, firewall, CASB, and Browser Isolation with one unified solution. This helps organizations control access, contain threats, and protect data across any network. By using identity-based ZTNA for private access, iboss reduces risks associated with legacy VPNs. Its cloud-delivered SWG inspects traffic, including HTTPS, and enforces advanced malware defenses and data loss prevention. Inline and out-of-band CASB features guard SaaS applications, while SD-WAN capabilities simplify office connectivity and reduce bandwidth costs. Through a single console, iboss lowers costs, unifies policies, and delivers consistent protection for all users, devices, and locations.

Fully, Unified, Full Distributed

Unified Controls

Implement a single policy framework across every location and user, eliminating the complexity of managing separate solutions.

Unified Protection

Apply consistent security controls for web, cloud, and private apps, reducing exposure and preventing threats everywhere.

Unified Visibility

Leverage a single console for real-time logging and reporting, enabling faster investigations and stronger oversight across the organization.

Contact Us:

sales@iboss.com 877-742-6832 iboss.com

Request a Demo Today