Secure sensitive data by preventing data loss

The old network perimeter has eroded. The new edge is here to stay. Enterprises must adapt and protect their data in the modern 'work from anywhere' world.

Modern enterprise data is no longer protected by traditional on-prem DLP solutions. Now that "work from anywhere" is commonplace, the rise in the use of the cloud has created new blind spots for data loss protection. Some enterprises use VPNs as protection for remote users; however, split tunneling data to the internet leaves traffic unmonitored and not visible to on-prem DLP solutions. Today's enterprises must gain visibility into their data to identify and eliminate data loss incidents. With iboss, enterprises gain greater visibility and better control to help prevent data loss for all users working from anywhere.

Inspect and protect all of your content with iboss DLP

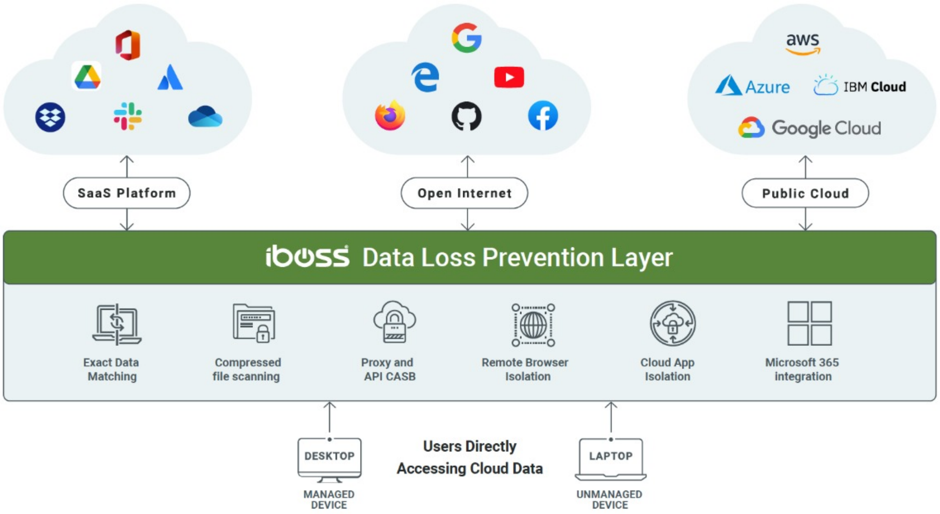
Predefined DLP policies make it fast and easy to deploy

API CASB for DLP Detection gives visibility and protection

Exact Data Match for Data Loss Prevention

Identify trends and eliminate blind spots

Inspect and protect all of your organization's most valuable data



As all users are connected to the iboss Cloud Platform from wherever they work, any data transfers get analyzed by the iboss service. This includes files or content stored in public and private clouds. The iboss service analyzes the data going through the service and looks for specific content and files identified through policies set by the cloud administrator.

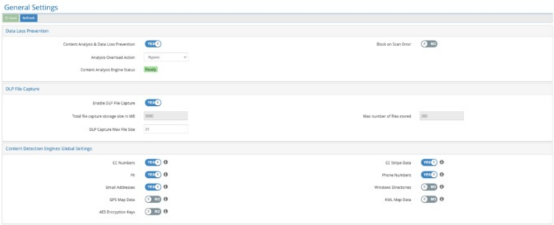
If there is an attempted download or upload of a file labeled internal or sensitive, it will be identified through the DLP engine and blocked if defined within the DLP policy.

The platform provides predefined rule-based expressions that stop common content like credit card numbers from being extracted. Additionally, Exact Data Matching can identify an exact match on content like PII, employee records or price lists. After an action is flagged in the platform, it is logged with all other incidents.

The iboss DLP feature provides organizations with a high-level of visibility into the movement of sensitive data and enables the enterprise to identify and act quickly before sensitive data moves to an unauthorized cloud location or device.

Predefined DLP policies make it fast and easy to deploy

The iboss built-in content detection and content analysis engines give the ability to search for sensitive content with minimal configuration. Find what you need faster. The desired content detection policies need only be toggled on by the cloud administrator. With a wide array of options to choose from, including the ability to monitor for credit card numbers, PII, GPS map data, email addresses, and more, iboss makes it easy to protect commonly misused data types. Gain traction on your compliance efforts.



General Settings

Data Loss Prevention

Content Analysis & Data Loss Prevention: YES
Block on Scan Error: NO
Analysis Overload Action: Bypass
Content Analysis Engine Status: Ready

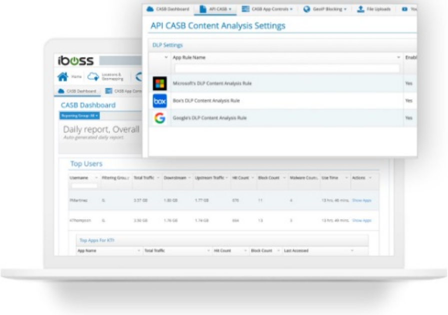
DLP File Capture

Enable DLP File Capture: YES
Total file capture storage size in MB: 5000
Max number of files stored: 200
DLP Capture Max File Size: 25

Content Detection Engines Global Settings

CC Numbers: YES
CC Stripe Data: YES
PII: YES
Phone Numbers: YES
Email Addresses: YES
Windows Directories: NO
GPS Map Data: NO
KML Map Data: NO
AES Encryption Keys: NO

The iboss content analysis engines can identify nearly any type of data in a transfer request, which is required information for detection engines to inspect content. Analysis engines can identify both decompressed files such as PDF and Microsoft Office files, along with compressed types such as ZIP and RAR types. Compressed files are identified by unpackaging and decompressing the data to it's original form. After inspection, if an engine is triggered by the detection of sensitive files or content, the administrator has the ability to set a block action. Each violation is logged and captured in the platform.



API CASB Content Analysis Settings

DLP Settings

App Rule Name	Enabl
Microsoft's DLP Content Analysis Rule	Yes
Box's DLP Content Analysis Rule	Yes
Google's DLP Content Analysis Rule	Yes

Top Users

Username	Filtering Grou...	Total Traffic	Downstream	Upstream Traffic	Hit Count	Block Count	Malware Coun...	Use Time	Actions
PMartinez	6	3.57 GB	1.80 GB	1.77 GB	676	11	4	13 hrs, 46 mins	Show Apps
KThompson	6	3.50 GB	1.76 GB	1.74 GB	664	13	3	13 hrs, 49 mins	Show Apps

Top Apps For KTh

App Name	Total Traffic	Hit Count	Block Count	Last Accessed

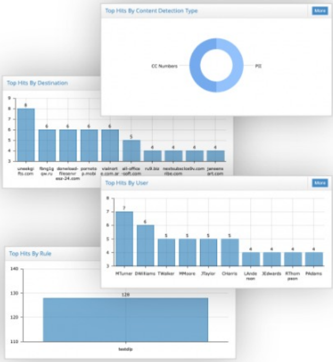
API CASB for DLP Detection allows user-centric visibility and data-centric protection

Using API CASB, the iboss service allows the organization to define DLP policies that can flag any sensitive data found in Box, Microsoft 365, and G Suite. As the enterprise continues to increase their usage of shared cloud environments for data storage, it is paramount that sensitive data is identified as being stored in authorized locations. This ensures data stored within Box, Microsoft 365 and Google cloud services is not transferred between enterprise and personal accounts and that enterprise data compliance is met.

Find precisely what you need with Exact Data Match for Data Loss Prevention

iboss Exact Data Match (EDM) for Data Loss Prevention (DLP) finds content in data being transferred that matches exact data records provided by the organization. The data records are indexed offline, hashed and the hash of the data is stored in the iboss cloud EDM service. The administrator would set policies to look for the exact data matches for the content provided to the iboss service from the enterprise.

The iboss Cloud Platform scans all traffic, looking for sensitive data in any transaction going through the iboss service. The use of EDM reduces false positives and increases detection accuracy for preventing data loss of sensitive content from the enterprise either accidentally or through misuse.



Identify trends and eliminate blind spots with DLP Event Log and Dashboard

When a DLP rule is triggered by a user's activity, an event is created in the Event Log dashboard. The details include the user event and details relating to the DLP analysis and the data it detected. This detailed DLP event log information can be used to audit user behavior or to better understand the behavior of the DLP rules defined by the enterprise. As data loss incidents are logged, the dashboard in the iboss' cloud displays the compiled events in an organized fashion. The dashboard is extremely beneficial in identifying trends with compliance concerns and helping eliminate those blind spots moving forward. Additionally, the platform can stream the DLP event log data to any SIEM for additional analysis.