Extend iboss Zero Trust SASE CASB with Microsoft Cloud App Security

Cloud Application Security Brokering, or CASB, has become an important aspect of cloud and SaaS migrations. Extend CASB features in iboss with Microsoft CAS for best of class application visibility and control.

Microsoft Cloud App Security with iboss Zero Trust SASE Overview

The iboss Zero Trust SASE includes extensive CASB controls for a vast amount of applications including LinkedIn, Facebook and Google. The iboss Zero Trust SASE CASB controls are easily extended to leverage Microsoft Cloud App Security which can be used for data at rest within Microsoft and other cloud applications. The integration is quickly and easily enabled and gives instantaneous access and protection from the Microsoft Cloud App Security suite. Combining iboss with Microsoft Cloud App security eliminates the need for log collectors and log forwarders. The iboss Zero Trust SASE connects user data to Microsoft to ensure CASB protection without configuration headaches.

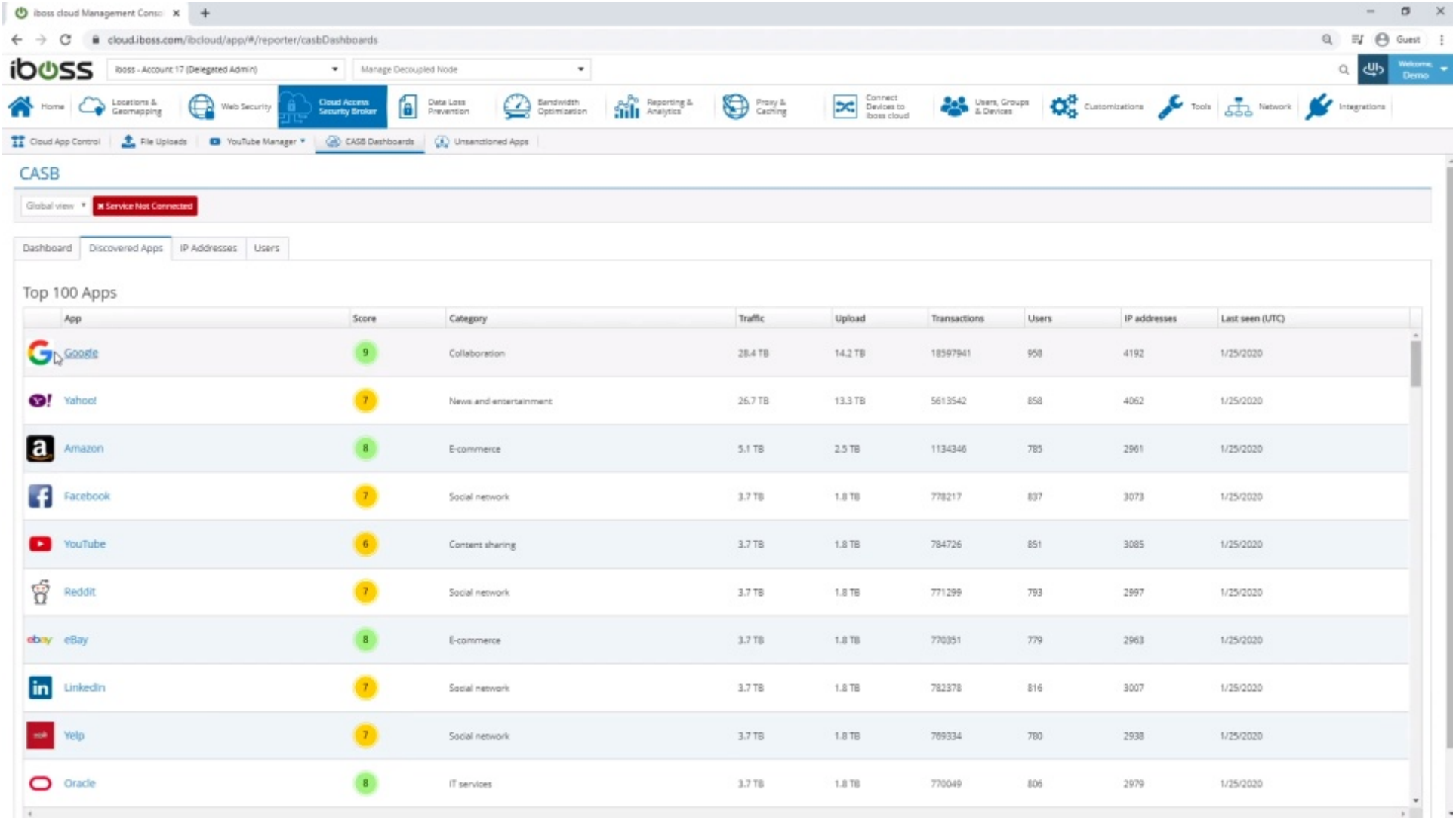
- The iboss Zero Trust SASE natively includes CASB to protect cloud application access by users from any location, including in and and out of the office
- Microsoft Cloud App Security CASB includes CASB controls for data resting within Azure, Office 365 suite and popular applications such as Box and DropBox
- By combining the power of iboss cloud CASB with Microsoft Cloud App Security, organizations can protect data as it moves to and from users and the cloud as well as for data as it rests within the cloud
- Eliminate the need for log storage servers and virtual machines used for forwarding traffic to Microsoft Cloud App Security. The iboss cloud automatically exchanges data and signatures with Microsoft Cloud App Security
- Gain visibility and risk insights for users as they work outside of the traditional network perimeter, including working on the road and at home
- iboss will prevent the use of unsanctioned cloud applications by automatically syncing policies and signatures from Microsoft Cloud App Security
- Create DLP policies that transcend Microsoft and automatically extend into iboss
- Easily view application risk profiles including compliance and certifications for GDPR and discover cloud application usage

Implementing Microsoft Cloud App Security Challenges

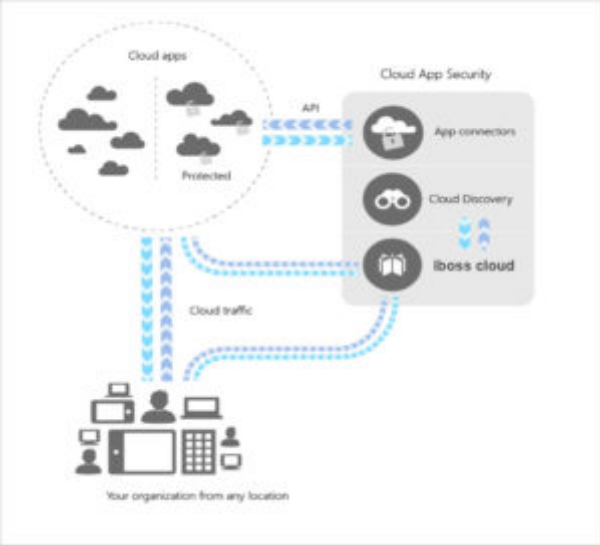
Microsoft Cloud App Security is a powerful CASB designed to protect data at rest within Microsoft and other popular cloud applications, such as DropBox and Box. When licensed, the iboss Zero Trust SASE includes CASB protection for data as it moves between users and the Internet. The combination of iboss Zero Trust Edge with Microsoft Cloud App Security provides the most powerful protection for both cloud data in motion and cloud data at rest. Implementing Microsoft Cloud App Security as a standalone product can be challenging. Those challenges include:

- The need to gather user Internet activity log data in order to forward this data to Microsoft Cloud App Security is the responsibility of IT staff. Since users are mobile and work from places beyond the traditional office, gathering the logs for Internet activity can be challenging so that consistent visibility is available in and and out of the office.
- The need to create logging servers that can send the data to Microsoft Cloud App Security for analysis. The need to create and manage these logging servers typically involves creating virtual appliances that then must be managed by IT staff which is against SaaS principles and increases costs.
- The need to synchronize Microsoft Cloud App Security policies and signatures to firewalls and gateways so the unsanctioned applications are controlled. This involves specialized technology integrations that must be implemented by overburdened IT staff and the results are typically limited to firewalls and on-prem gateways that can only protect users within the office.
- The need to manage multiple separate policies from different platforms to enforce CASB controls for data in motion and data at rest which increases operational overhead, increases costs and leads to poor end-user experience due to mismatching policies.

iboss cloud with Microsoft Cloud App Security



Architectural Overview



Gain Visibility Into Cloud Application Use Including Shadow IT

By combining the power of iboss cloud CASB controls and visibility with the power of Microsoft Cloud App Security (CAS), visibility and control of cloud application use is put back into the hands of the organization. The solution provides extensive visibility into cloud application use including volumes of transfers to reduce risk and ensure compliance.

Eliminate the Need to Implement, Host and Manage Log Forwarding Servers

Microsoft Cloud App Security is typically implemented with log-shipping servers designed to gather user Internet access logs and send them to Microsoft for processing. Implementing and managing virtual servers is not only costly, but requires valuable IT time for maintenance. Worst of all, managing infrastructure is contradictory to a SaaS strategy. The iboss cloud automatically synchronizes data with Microsoft CAS and abstracts this burden from IT staff which reduces time and costs.

Extend Microsoft Cloud App Security Beyond the Office to Users on the Road

The iboss cloud will automatically forward all of the necessary data to Microsoft Cloud App Security for all users regardless of location. Since users are always connected to iboss cloud, Microsoft Cloud App Security will always have visibility into user Internet access data in order to eliminate blind spots and identify risk behaviors and shadow IT.

Prevent Unsanctioned Cloud Application Access and Risky Cloud Activity

The iboss cloud automatically synchronizes data and signatures with Microsoft Cloud App Security so that unsanctioned and risky cloud applications are not accessed by organizational users. When an application is sanctioned within Microsoft Cloud App Security, the signatures are synchronized to iboss cloud which enforces those policies preventing data from traversing to and from those applications.

Gain Application Risk Profiles and Certification Standings

See application certifications and risk analysis directly within the iboss cloud administrative console. This includes cloud application standings for GDPR and ISO certifications. Use this information to uncover shadow IT and risk application use. Create policies to reduce risk while maintaining user productivity.

Apply Unsanctioned Application Policies to Users by Role

Unsanctioned applications can be restricted to users within specific roles within the organization. This includes applying application restrictions to users within an Organization Unit (OU) or Security Group. OUs and Security Groups are automatically mapped within the iboss cloud admin console.

Reduce Microsoft Cloud App Security Implementation Time

Implementing Microsoft CAS can be a daunting task which includes configuring scripts to block unwanted applications and configuring logging servers to forward data to Microsoft CAS. With iboss cloud, implementation time is completed within seconds and involves enabling the Microsoft CAS feature and entering basic configuration information. The iboss cloud handles all of the complexities automatically so that IT staff can benefit from the power of Microsoft CAS without the headaches and time involved in implementing it.

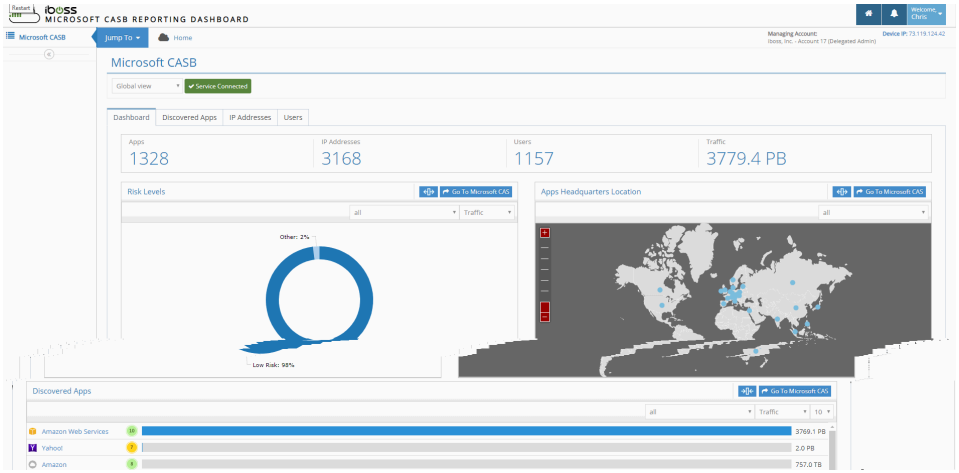
How It Works

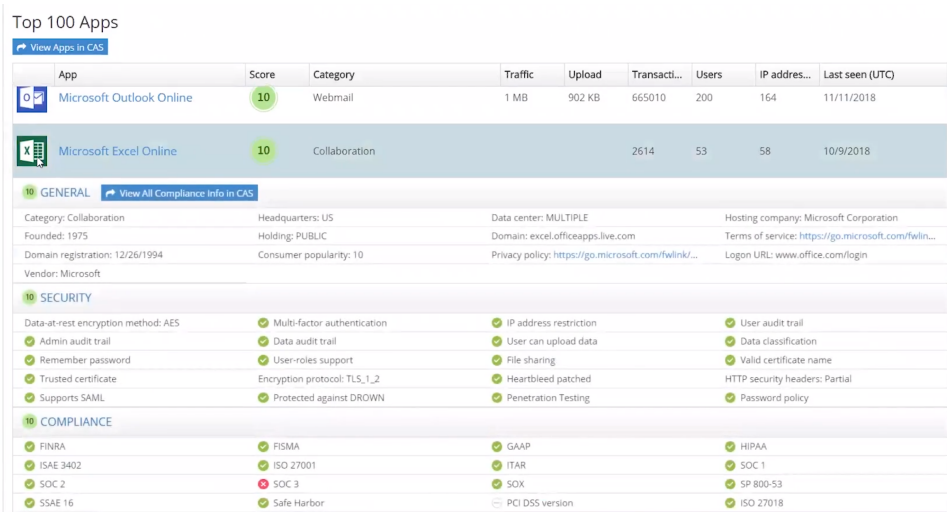
Taking advantage of Microsoft Cloud App security with iboss cloud is easy. To get started:

1. Get an active iboss cloud account.
2. Connect users to the iboss cloud using one of the many cloud connectors. This connects users to iboss cloud regardless of location.
3. Configure Microsoft Cloud App Security to connect with iboss cloud via the Microsoft instructions found at https://docs.microsoft.com/en-gb/cloud-app-security/iboss-integration.
4. Enter basic Microsoft Cloud App Security settings within the iboss cloud administrative interface which automatically configures all of the connections between Microsoft CAS and iboss cloud.
5. Microsoft Cloud App Security becomes instantly available within the iboss cloud single pane of glass admin interface, including detailed Microsoft Cloud App Security dashboards embedded natively within iboss cloud.

Feature Highlights

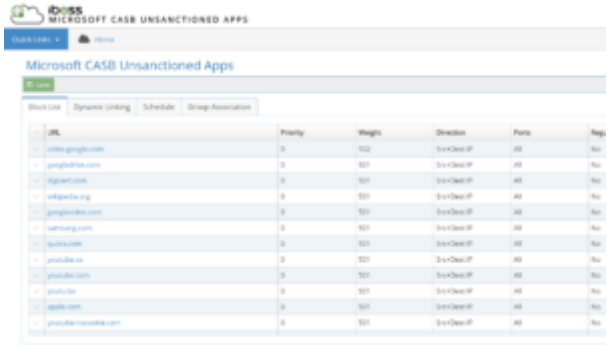
Microsoft Cloud App Security Dashboards Directly Inside iboss cloud





Combine the best of class logging and reporting available with iboss cloud with Microsoft Cloud App Security reporting for unsurpassed visibility into shadow IT and high risk user Internet activity. Data and signatures are automatically synchronized between iboss cloud and Microsoft Cloud App Security.

Automatically Restrict Unsanctioned Applications



When creating policies to prevent access to unsanctioned applications within Microsoft CAS, those policies automatically transfer to iboss cloud which enforces those policies on users. Since the iboss cloud protects users regardless of location, Microsoft CAS policies will be applied at all times which reduces risk and prevents unwanted shadow IT.

Pricing

Microsoft Cloud App Security Features	
Microsoft Cloud App Security integration is automatically included in all iboss Enterprise and Unlimited subscriptions. A Microsoft E5 Subscription Key or license to Microsoft CAS is required. This key is entered into iboss cloud to enable Microsoft CAS.	Contact Us

About iboss

iboss is a cloud security company that enables organizations to reduce cyber risk by delivering a Zero Trust service designed to protect resources and users in the modern distributed world. Applications, data and services have moved to the cloud and are located everywhere while users needing access to those resources are working from anywhere. Built on a containerized cloud architecture, iboss delivers security capabilities such as SWG, malware defense, browser isolation, CASB and data loss prevention to protect all resources, via the cloud, instantaneously and at scale. This shifts the focus from protecting buildings to protecting people and resources wherever they are located. Leveraging a purpose-built cloud architecture backed by 230+ issued and pending patents and more than 100 points of presence globally, iboss processes over 150 billion transactions daily, blocking 4 billion threats per day. More than 4,000 global enterprises trust the iboss Cloud Platform to support their modern workforces, including a large number of Fortune 50 companies.

To learn more, visit https://www.iboss.com