

iboss Cloud App Isolation

Data Loss Protection for cloud applications accessed from unmanaged devices

The Challenge

Most enterprises have employees or contractors using unmanaged devices to access cloud applications. As a result, enterprises are looking for a solution that secures unmanaged device access to public cloud apps. The option to solve this problem has been limited to reverse proxy. The reverse proxy solution is complex to setup and can have limited public cloud app support.

The Solution - iboss Cloud App Isolation

iboss Cloud App Isolation allows administrators to enforce the use of browser isolation for unmanaged device access to public cloud apps used by the enterprise. The iboss platform is configured to force users working from unmanaged devices to go through the Cloud App Isolation feature of the iboss platform in order to access public cloud apps. This helps prevent data loss by controlling unmanaged user access to content or files stored within designated public cloud applications.

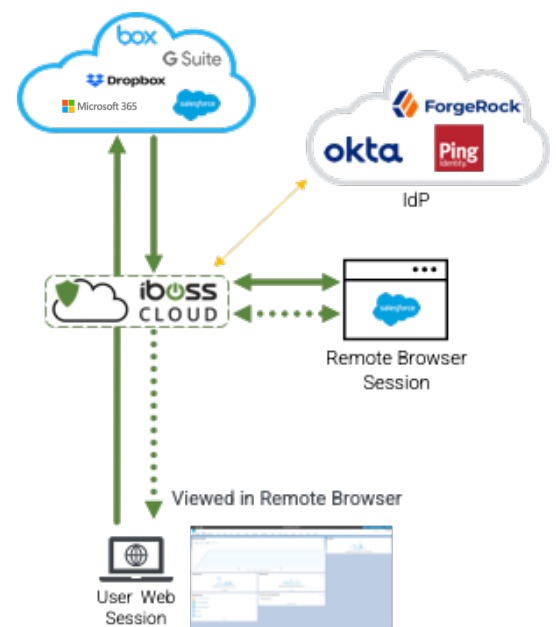
Using the iboss Cloud App Isolation feature, administrators can define policy based on users, groups, and any public cloud. The user or contractor is provided access to the public cloud app through the iboss platform in an isolated session. This allows the user or contractor to manipulate data in the public cloud service; however, any downloads to the local device is blocked. These download restrictions safeguard sensitive data and ensure that data stays in the cloud service.

How We Do It - Cloud App Isolation for Public Cloud Data Loss Protection

The Cloud App Isolation feature is enabled and controlled by the iboss Cloud administrator. Policies set within the iboss Cloud Platform determine which users, groups and public cloud apps are required to use the Cloud App Isolation feature. The iboss platform integrates with any IdP/SAML provider and works with any public cloud app. This allows the iboss admin to setup restrictions to enforce the use of Cloud App Isolation for any public cloud apps.

Tenant restrictions are enforced on the public cloud service so only users coming through the iboss platform are allowed access to the cloud apps. The user, using a standard web browser would be directed to the iboss cloud. The iboss cloud service then instantiates an isolated browser session, where the user is delivered access to read and modify the data stored in the cloud as shown in Figure 1.

Figure 1



The iboss Cloud App Isolation feature not only improves the level of security for data stored in public clouds, but it also increases compliance by ensuring that data is never downloaded onto devices that are not owned and managed by the enterprise.

iboss Cloud App Isolation Advantages

- Selectively deploy iboss Cloud App Isolation for specific unmanaged users, groups, and public cloud apps to protect sensitive data.
- Natively integrated with the iboss Cloud Platform, offering full content and malware inspection for the isolated application session.
- Provides comprehensive visibility and logging for all user activity for the isolated application session.
- Works with any public cloud app that supports SAML.
- Includes TLS/SSL decryption for unmanaged devices without requiring the installation of a root certificate for decryption.
- Increased security through containerized cloud gateways: iboss Cloud App Isolation sessions are tied to a specific organization, so traffic going through Cloud App Isolation feature is never mixed with other customers' traffic.

Conclusion

The iboss Cloud Platform allows enterprises to provide users with the fastest and most secure connection to applications from anywhere. Leveraging the iboss Cloud App Isolation feature, organizations can ensure that access to data stored in the public cloud remains secure for all users working from unmanaged devices. Since iboss Cloud App Isolation is natively integrated into the iboss Cloud Platform, comprehensive content, malware inspection and logging are provided. With iboss Cloud App Isolation enterprises can increase the data security for public cloud access without the complexities of alternative solutions.

For more information on the iboss Cloud Platform, visit <https://iboss.com/SASE/>

About iboss®

iboss is a cloud security company that enables the modern workforce to connect securely and directly to all applications from wherever they work. Built on a containerized cloud architecture, iboss delivers security capabilities such as SWG, malware defense, RBI, CASB and data loss prevention to all connections via the cloud, instantaneously and at scale. This eliminates the need for traditional network security appliances, such as VPNs, firewalls and web gateway proxies, which are ineffective at protecting a cloud-first and mobile world. 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 www.iboss.com



+1 877.742.6832

sales@iboss.com

101 Federal St
Boston, MA 02110

© 2021 iboss. All Rights Reserved.

Secure Connectivity from Anywhere.